

DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE  
LA EVIDENCIA DIGITAL DERIVADA DEL ANÁLISIS FORENSE, APLICADO EN  
EL LABORATORIO DE INFORMÁTICA FORENSE FISCALÍA GENERAL DE LA  
NACIÓN, SECCIONAL TOLIMA

ANDERSON RAYO PAMO  
MARTHA LUCÍA HERNÁNDEZ PERDOMO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
BOGOTÁ  
2018

DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE  
LA EVIDENCIA DIGITAL DERIVADA DEL ANÁLISIS FORENSE, APLICADO EN  
EL LABORATORIO DE INFORMÁTICA FORENSE FISCALÍA GENERAL DE LA  
NACIÓN, SECCIONAL TOLIMA

ANDERSON RAYO PAMO  
MARTHA LUCÍA HERNÁNDEZ PERDOMO

Proyecto de grado para optar el título de especialista en seguridad informática

Director de proyecto:  
SALOMÓN GONZÁLEZ GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
BOGOTÁ  
2018

Nota de aceptación

---

---

---

---

Firma del Director

---

Firma del Jurado

---

Firma del Jurado

Bogotá, Septiembre 2018

## CONTENIDO

	Pág.
INTRODUCCIÓN.....	10
1. TÍTULO.....	11
2. DESCRIPCIÓN DEL PROBLEMA .....	12
2.1. FORMULACIÓN DEL PROBLEMA .....	12
3. OBJETIVO GENERAL .....	13
3.1. OBJETIVOS ESPECÍFICOS.....	13
4. JUSTIFICACIÓN .....	14
5. ALCANCE Y DELIMITACIÓN DEL PROYECTO.....	16
6. METODOLOGÍA.....	17
6.1. METODOLOGÍA DE DESARROLLO .....	17
6.2. UNIVERSO Y MUESTRA .....	18
6.3. FUENTES DE RECOLECCIÓN DE INFORMACIÓN .....	19
7. MARCO DE REFERENCIA .....	21
7.1. MARCO DE ANTECEDENTES.....	22
7.2. MARCO DE CONTEXTO .....	23
7.3. MARCO TEÓRICO .....	24
7.4. MARCO CONCEPTUAL .....	31
7.5. MARCO LEGAL .....	32
8. DESARROLLO DE PROYECTO.....	34
8.1. HERRAMIENTAS ACTUALES DEL LABORATORIO DE INFORMÁTICA FORENSE DE LA FISCALÍA GENERAL SECCIONAL TOLIMA .....	34
8.1.1. Herramientas de software forense. ....	34
8.1.2. Herramientas de Hardware Forense .....	36
8.2. RECONOCIMIENTO DE NORMAS Y ESTÁNDARES .....	42
8.2.1. ISO/IEC 27037:2012 .....	43
8.2.2. NIST 8061 .....	466
9. IDENTIFICACIÓN DE COMUNIDADES TÉCNICO CIENTÍFICAS PARA EL MANEJO DE LA EVIDENCIA DIGITAL .....	48
9.1. ISO / IEC .....	48
9.2. NIST .....	48
9.3. SWGDE .....	49
10. ESTABLECER PROCESOS NECESARIOS PARA EL ASEGURAMIENTO, VALIDACIÓN Y CONSERVACIÓN DE LA EVIDENCIA DIGITAL .....	50

11.	DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE EVIDENCIA DIGITAL DERIVADA DE ANÁLISIS FORENSE INFORMÁTICOS .....	52
11.1.	OBJETIVO.....	52
11.2.	ALCANCE.....	52
11.3.	DESARROLLO .....	52
11.3.1.	Aseguramiento de evidencia digital.....	52
11.3.2.	Validación de evidencia digital derivada de análisis informáticos.....	73
12.	SOCIALIZACIÓN DEL PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE EVIDENCIA DIGITAL DERIVADA DE ANÁLISIS FORENSE INFORMÁTICO.....	75
13.	CONCLUSIONES .....	76
14.	RECOMENDACIONES.....	77
15.	DIVULGACIÓN .....	78
	BIBLIOGRAFÍA.....	79

## LISTA DE TABLAS

Pág.

Tabla 1. Recolección de información. ....	39
Tabla 2. Diagrama de Flujo del procedimiento para el aseguramiento de evidencia digital. ....	70
Tabla 3. Diagrama de flujo para almacenamiento en disco duro mediante la creación de imagen forense AD1 con herramienta de software forense FTK Imager. ....	71
Tabla 4. Diagrama de flujo para montaje de imagen forense AD1 a directorio o drive en modo protegido de solo lectura. ....	72

## LISTA DE FIGURAS

	Pág.
Figura 1. Proceso de cálculo de HASH .....	25
Figura 2. Grabación disco compacto.....	26
Figura 3. Rotulo de contenedor de evidencia.....	29
Figura 4. Cadena de custodia, cara anterior.....	30
Figura 5. Cadena de custodia, cara posterior.....	30
Figura 6. Impresión de pantalla software Encanse, en modo acquisition.....	34
Figura 7. Impresión de pantalla software AccessData Forensic Toolkit.....	35
Figura 8. Impresión de pantalla software UFED Physical Analyzer.....	36
Figura 9. Equipo UFED Ultimate Touch.....	36
Figura 10. Equipo FREDDIE Digital Intelligence.....	37
Figura 11. Servidor MicroSystem .....	37
Figura 12. Kit de bloqueadores Tableau e interfaces adaptadoras.....	38
Figura 13. Impresión de pantalla para directorio de reportes.....	53
Figura 14. Impresión de contenido de reporte FTK AccessData.....	53
Figura 15. Carga de directorio a herramienta FTK Imager.....	54
Figura 16. Selección de exportado de lista HASH.....	54
Figura 17. Pre visualizado de lista Hash de archivos inicial.....	55
Figura 18. Cálculo HASH para un solo archivo mediante FTK Imager.....	55
Figura 19. Pre visualizado de HASH calculado a LISTA HASH DE ARCHIVOS... ..	56
Figura 20. Grabado de datos a disco compacto mediante Software Nero.....	56
Figura 21. Selección de verificación posterior al grabado y desmarque de multi - Sección en software Nero para grabado de disco.....	57
Figura 22. Referencia para rotulado de disco compacto.....	57
Figura 23. Uso de cubierta sólida que permite la protección del disco compacto.....	58
Figura 24. Uso de bolsa anti estática.....	59
Figura 25. Ejemplo del contenido en rótulo.....	59
Figura 26. Ejemplo de contenido en cadena de custodia.....	60
Figura 27. Ejemplo de contenido en cadena de custodia.....	60
Figura 28. Imagen de referencia para embalado y rotulado final del elemento.....	61
Figura 29. Directorio de reporte de evidencia digital.....	62
Figura 30. Carga de directorio a herramienta FTK Imager.....	62
Figura 31. Selección de exportado de lista HASH de archivos.....	63
Figura 32. Pre visualizado de LISTA HASH DE ARCHIVOS INICIAL.....	63
Figura 33. Creación de paquete de imagen. FTK Imager formato AD1.....	64
Figura 34. Reporte creación imagen forense de directorio con herramienta FTK Imager.....	64
Figura 35. Paquetes de datos resultados de imagen AD1.....	65
Figura 36. Montaje de paquete de imagen AD1 con FTK Imager.....	65

Figura 37. Resultado de montaje de paquete AD1, en la unidad lógica F.....	66
Figura 38. Imagen de referencia para disco duro portable.....	66
Figura 39. Etiqueta de identificación de disco duro portable.....	66
Figura 40. Impresión de pantalla imagen de rotulo para disco duro portable.....	67
Figura 41. Impresión de pantalla de cadena de custodia para disco duro portable. .....	68
Figura 42. Impresión de pantalla complemento de cadena de custodia.....	68
Figura 43. Embalado y rotulado, bolsa anti estática burbuja.....	69
Figura 44. Diagrama de Flujo del procedimiento para el aseguramiento y validación de evidencia digital .....	70
Figura 45. Impresión de pantalla para control de asistencia. ....	75



## LISTA DE ANEXOS

	Pág.
Anexo A. Carta de aceptación de desarrollo de proyecto .....	83
Anexo B. Formato de recolección de datos - entrevista.....	84
Anexo C. Formato de recolección de datos - entrevista.....	87
Anexo D. Resumen analítico RAE .....	85

## INTRODUCCIÓN

La informática forense es la aplicación de técnicas y procedimientos dentro del área de conocimiento de las ciencias de la computación; tiene como objetivo de velar e interpretar hechos a partir de los resultados de procesos informáticos o peritajes, a petición de la víctima u organismos de control judicial; por tanto, los descubrimientos y obtención de la evidencia digital derivados se deben presentar con validez probatoria absoluta sobre el incidente informático objeto de investigación o hecho que relaciona la evidencia electrónica o digital.

Dada la finalidad de la informática forense es preciso indicar que los entes de investigación privada y del estado, en la actualidad no han desarrollado metodologías para el aseguramiento y validación de la evidencia digital derivada de los análisis informáticos; ya sea la evidencia producto de herramientas de software forense o procesos lógicos para el descubrimiento de un posible hecho de investigación de tipo penal o privada.

Para dar solución a esta problemática se plantea este proyecto de grado denominado Diseño de procedimiento para el aseguramiento y validación de la evidencia digital derivada del análisis forense, aplicado en el laboratorio de informática forense de la Fiscalía General De La Nación, Seccional Tolima; de lo cual se obtiene una posible solución real, con destino a entes de investigación y control judicial o relacionados con los servicios de informática forense a nivel particular.

## 1. TÍTULO

DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE LA EVIDENCIA DIGITAL DERIVADA DEL ANÁLISIS FORENSE, APLICADO EN EL LABORATORIO DE INFORMÁTICA FORENSE FISCALÍA GENERAL DE LA NACIÓN, SECCIONAL TOLIMA

## 2. DESCRIPCIÓN DEL PROBLEMA

Entre los retos de la investigación penal relacionados con actividades ilícitas como fraude electrónico, acceso abusivo a sistemas de información, daño informático, pornografía infantil, tráfico de estupefacientes, extorsión, hurto a través de medios informáticos, distribución de software malicioso; se halla la consecución de la prueba o evidencia digital, donde se identifica el medio y tecnologías de la información asociados para llevar a cabo una conducta ilegal. Es por tanto que la informática forense desempeña un papel de gran importancia para identificar y asegurar las pruebas necesarias dentro de las evidencias recolectadas.

Actualmente los entes de investigación del estado y el sector privado no cuentan con el desarrollo de procedimientos claros para el aseguramiento y validación de la evidencia digital derivada de procedimientos de informática forense; lo anterior se evidencia en la guía y procedimientos de informática Forense, así como el procedimiento de cadena de custodia de la FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA<sup>1</sup>, de igual forma se puede conocer el vacío en el documento: “Procedimiento De Evidencia Digital” en el cual se evidencia el poco cumplimiento de requisitos relacionados con la idoneidad tecnológica, procedimientos, ajuste a normas, estándares y protocolos, para el aseguramiento y validación de la evidencia digital (Ministerio de Tecnologías de la Información y Comunicaciones –MINTIC<sup>2</sup>-).

Así mismo los laboratorios de informática forense deben adaptar estándares de calidad y buenas prácticas para garantizar la integridad, disponibilidad y confidencialidad de la información digital obtenida a partir de un proceso de informática forense.

### 2.1. FORMULACIÓN DEL PROBLEMA

¿Cómo garantizar el aseguramiento y validación de la evidencia digital derivada de procesos de informática forense?

---

<sup>1</sup> FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA. Manual de procedimientos para cadena de custodia. {En línea}. {28 de septiembre de 2017}.

<sup>2</sup> MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Seguridad y Privacidad de la Información. Guía No. 13. Evidencia Digital. (28 de marzo de 2016).

### 3. OBJETIVO GENERAL

Diseñar un procedimiento estándar para el aseguramiento y validación de la evidencia digital, derivada de procesos de informática forense en el laboratorio de la Fiscalía general de la Nación Seccional Tolima encargado de dichas tareas.

#### 3.1. OBJETIVOS ESPECÍFICOS

- Diagnosticar las herramientas con las que cuenta actualmente el laboratorio de informática forense de la Fiscalía General Seccional Tolima, para el aseguramiento de evidencia digital.
- Identificar las diferentes normas y estándares para el aseguramiento de la información en Colombia.
- Caracterizar las comunidades de interés (stakeholders) en buenas prácticas para el manejo de la evidencia digital.
- Proponer nuevos procesos para el aseguramiento, validación y conservación de la evidencia digital deriva de procesos de informática forense.
- Socializar un nuevo procedimiento para el aseguramiento y validación de la evidencia digital derivada del análisis forense, en el laboratorio de informática forense Fiscalía General De La Nación, seccional Tolima.

## 4. JUSTIFICACIÓN

### Conveniencia institucional

Dado que la informática forense debe considerarse como eje transversal en la investigación para cualquier tipo de delito, sumado a que sus resultados generan carga probatoria o esclarecimiento de hechos sujetos a investigación penal o disciplinaria; se debe explorar la posible implementación de un procedimiento que permita validar la autenticidad de la evidencia digital a través del desarrollo de un proceso que garantice el aseguramiento y validación de la evidencia digital producto de un análisis forense, permitiendo evaluar el grado de autenticidad y aceptación de evidencia digital como un elemento material probatorio que permite evidenciar el esclarecimiento de algún hecho investigación.

¿Quién o cómo, se garantiza que la prueba se conserve en el tiempo en el mismo estado en el que fue hallada?; ¿Cómo se valida que la evidencia digital se halle íntegra y original, conservando su identidad frente a un proceso de investigación? Por lo anterior se requiere el desarrollo de un procedimiento ajustable para que asegure y valide la evidencia digital producto del análisis informático.

### Relevancia social:

Como aporte académico este proyecto busca propiciar la reflexión crítica frente a los modelos o sistemas de aseguramiento y validación de la evidencia digital en la institución y el departamento, como también el análisis entre los profesionales de diversas disciplinas interesados en el tema. También se busca servir de guía para la construcción de planes, programas y proyectos de seguridad informática.

En conclusión, el proyecto busca ser un marco referencial para futuras investigaciones, como también, un aporte académico a los estudios sobre seguridad digital. De la misma manera, el presente estudio se hace pertinente para la disciplina de ingeniería de sistemas, debido a la necesidad de brindar una herramienta de análisis crítico que involucre el desarrollo social y judicial, primeramente, y hacer de esto una dinámica y práctica activa, para mejorar el perfil ético en las entidades judiciales del Estado colombiano.

Lo anterior, se expone en base a que la situación requiere una atención tanto social como analítica y crítica para el fortalecimiento en aspectos como el académico, lexical, ético, moral, y comportamental en las entidades judiciales del departamento. De esta forma mejorar las relaciones intersectoriales con las personas que la rodean y que hacen parte del contexto jurídico.

Todo lo anterior conllevará a dichas instituciones a desarrollarse de manera óptima y adecuada en diferentes problemáticas que pueda generar la falta de ética en el

manejo y validación de evidencias digitales, esto a la vez, afronta los efectos de la globalización y procesos contemporáneos, debido a que dichos aspectos conforman un escenario en el que se hace necesario el uso de un buen sistema de aseguramiento y validación de la evidencia digital.

#### Implicaciones prácticas:

Al finalizar el proyecto, se pretende generar el proponer un modelo de aseguramiento y validación de la evidencia digital, para el laboratorio de informática forense Fiscalía General de la Nación, Seccional Tolima que servirá como guía "hoja de ruta" para las demás seccionales de la Fiscalía en el país, esto en caso de que deseen adoptar dicho proceso o modelo en el cual se pueden encontrar debilidades, oportunidades de mejora, como también amenazas y fortalezas según el direccionamiento que requiera la institución.

#### Valor teórico:

La investigación constituye un aporte conceptual al tema del manejo y validación de evidencias digitales, cargado con un valor semiótico y moral. El interés por el tema se asocia a la notable crisis de las entidades judiciales por lograr mantener su posicionamiento y buen nombre debido a la falta de estrategias y estructuras éticas. La investigación resalta el manejo y validación de evidencias digitales como ente principal en la formación y construcción de estrategias que permitan al público ser competitivo con sus entidades, en las cuales se escenifican roles, estrategias, e incluso problemas y soluciones ante las dificultades propias de las entidades jurídicas en cualquiera de sus tipologías. Por lo anterior, es de gran importancia identificar desde donde inicia la ética digital, como se desarrolla y desde allí se partirá para la creación y diseño de estrategias que permitan, modificar o mejorarla, así mismo, que sirva como base de modelo para futuras investigaciones del tema tratado.

#### Utilidad metodológica y viabilidad:

La presente propuesta se desarrolla partiendo que se tiene acceso a la información de la institución que serán objeto de estudio; en ese orden de ideas, el análisis de la información permitirá generar nuevas metodologías para la construcción de estrategias y modelos de manejo y validación de evidencias digitales como lo proponen varios autores en los antecedentes y el marco teórico, en sus diferentes estudios y escritos.

## 5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El desarrollo del proyecto toma como área de referencia a los laboratorios de informática forense de la Policía Judicial de la Fiscalía General de la Nación, los cuales no cuentan con procedimientos claros para el aseguramiento y validación de la evidencia digital producto del análisis informático. Por lo tanto, se busca producir un marco referencial para la aplicación de procedimientos que permitan preservar y generar indudablemente la admisibilidad de la evidencia digital obtenida en los laboratorios de informática forense.

De otra parte, los procesos establecidos en este proyecto buscan adaptarse a las necesidades por parte de los funcionarios que fungen en la actividad pericial en el Grupo de Delitos informáticos de la Fiscalía General de la Nación Seccional Tolima y a las restricciones presentadas en situaciones donde pueda poner en peligro real la evidencia objeto de aseguramiento, preservación y validación, promoviendo un mejor desempeño laboral bajo prácticas y normas de seguridad informática, obsérvese lo siguiente:

Alcance 1: La investigación permitirá proyectar a los profesionales de la informática en el departamento y la región, esto se logrará llevándolos a conocer los procedimientos de la seguridad informática y como se realizan los procesos de verificación al interior de las instituciones judiciales del país.

Alcance 2: La generación de nuevas tendencias en estudios sobre la seguridad informática permitirá generar una nueva tendencia en la región, puesto que la investigación permite observar el poco interés en el departamento por las investigaciones en este campo perteneciente a las ciencias de la computación.

Alcance 3: Adicionalmente la implementación de nuevos procesos que permitan a los profesionales de la oficina de delitos informáticos de la Fiscalía General de la Nación, procesar la información con la más alta seguridad y confiabilidad como también generar procesos de verificación que logren mostrar de forma creíble la información obtenida.



## 6. METODOLOGÍA

La presente investigación según SAMPIERI<sup>3</sup> es cualitativa porque extrae descripciones a partir de observaciones que adaptan la forma de entrevista, narraciones, diarios de campo, grabaciones, transcripciones de audio y video, registros escrito de todo tipo etc... Así mismo es analítica por que establecen cada una de las variables del problema planteado, a fin de analizar componentes y procesos; los cuales se identifican a través de entrevistas e inspección directa a sitio y procesos que conforman el sistema investigado o el problema plateado a resolver. Así mismo se verifican documentos, normas o estándares que se enmarcan en la seguridad de las tecnologías de la información para ser adaptados o referenciados dentro de la solución real que se pretende generar a partir del presente proyecto.

Además tiene un diseño no experimental, según HERNÁNDEZ, FERNÁNDEZ Y BAPTISTA<sup>4</sup>, el diseño no experimental como los estudios que se realizan sin la manipulación deliberada de variables y en los que solo se observan los fenómenos en su ambiente natural para después analizarlos. Esta investigación no tiene una manipulación de variables debido a que solo se observará y analizará el fenómeno de los canales de distribución para las empresas del departamento para así conocer la percepción que tiene la población del mismo.

Así mismo, es corte transaccional, de acuerdo a Hernández este tipo tiene por objetivo indagar la profundidad de la información en lo que se manifiesta una o más variables del enfoque cualitativo. El procedimiento refiere a la identificación de un grupo de individuos que se desarrollan en el contexto de situaciones específicas para la identificación de variable o conceptos cualitativos con el fin de conocer y valorar el estado del hecho objeto de análisis. Para el caso específico la verificación de información digital, esto se cuantifican mediante cumplimiento de metas, así mismo la generación, el manejo de diferentes archivos que permiten la descripción específica o procedimiento, es así como se cumple lo afirmado por (Hernández, Fernández y Baptista) En la investigación se realizará una descripción de una problemática determinada.

### 6.1. METODOLOGÍA DE DESARROLLO

Para el desarrollo del proyecto se realiza una investigación documental a través de medios electrónicos o impresos, a fin de identificar normas y estándares bajo los conceptos de seguridad de la información y medios tecnológicos, adaptables a

---

<sup>3</sup> SAMPIERI, Hernández, et al. Metodología de la Investigación, Tercera Edición, best séller Internacional. Editorial. Me Graw Hill. México DF Julio, 2002.

<sup>4</sup> HERNÁNDEZ SAMPIERI, Roberto; FERNÁNDEZ COLLADO, Carlos; BAPTISTA LUCIO, Pilar. Metodología de la investigación. México: McGraw-Hill, 2003.

laboratorios de informática forense; de lo cual se seleccionan los referentes más significativos para el diseño del procedimiento para el aseguramiento y validación de evidencia digital derivada análisis informáticos.

En ese sentido y con el objetivo de realizar una recolección de datos reales, se hace inspección al laboratorio de informática forense de la policía judicial de la Fiscalía General de la Nación Seccional Tolima; donde se desarrollan técnicas de documentación mediante la observación directa, registros fotográficos y entrevista a peritos en informática forense.

Adicionalmente realizada la recolección, se Identifican los procesos actuales para el aseguramiento, preservación y validación de la evidencia digital, obtenida de análisis de informática forense; de lo cual se establecen los protocolos, guías procesos y herramientas aplicadas.

Según lo dicho, una vez Identificados los procesos para el aseguramiento, preservación y validación de la evidencia digital derivada de procesos forenses; se establecen o relaciona la adaptación de normas, guías o documentos de buenas prácticas identificados en la investigación documental realizada.

## 6.2. UNIVERSO Y MUESTRA

La población objeto de estudio corresponde a todos los laboratorios de informática forense de la policía judicial de la Fiscalía General de la Nación, por lo cual se toma como muestra de estudio el Laboratorio de informática forense de la Sección de Policía judicial Seccional Tolima.

El laboratorio de informática forense se encuentra conformado por:

- Está compuesto por 5 integrantes; los cuales cuentan con un perfil de estudios relacionados con las tecnologías de la información y acreditación pericial de acuerdo al uso de herramientas forenses; uno de los integrantes desempeña el rol de coordinador y perito.
- Los procesos periciales corresponden al análisis de dispositivos electrónicos de almacenamiento de información como teléfonos celulares, computadores, dispositivos de almacenamiento de información digital.
- En cuanto a infraestructura tecnológica; el laboratorio de informática forense cuenta con hardware o equipos de cómputo especializado para la transferencia de información digital contenida en medios electrónicos o dispositivos enunciados previamente. De igual forma cuenta con software forense que

permite la recuperación y análisis de datos obtenido a través de hardware especializado.

### 6.3. FUENTES DE RECOLECCIÓN DE INFORMACIÓN

Revisión documental: Lo que se pretende realizar como primera medida, es la revisión de la documentación relacionada con el aseguramiento y validación de la evidencia digital derivada del análisis forense objeto de estudio. La revisión documental se hace importante y se justifica porque es de vital importancia identificar las acciones que han realizado las empresas frente al tema de la seguridad en la información, luego de ello se permite clasificar dichas estrategias y estudiarlas a profundidad y obtener datos objetivos durante la búsqueda que aporten datos de interés en la investigación.

Observación directa: Apoya la observación como técnica, refleja el pensamiento de los autores, al ir investigando y compartiendo los cambios encaminados a mejorar su sistema. Describe el trabajo, procesos y comportamiento de los autores, se utilizará en el presente estudio para observar los procedimientos utilizados por los ingenieros en la Fiscalía General de la Nación Seccional-Tolima de la ciudad de Ibagué seleccionadas para la investigación.

Tratamiento de la información: Para evitar el uso inadecuado de información y evitar la saturación de la misma, se utiliza el método de triangulación, obteniendo así, una recopilación de datos ordenada y sensata.

Para PÉREZ<sup>5</sup> “la triangulación implica reunir una variedad de datos y métodos referidos al mismo tema o problema. Implica también que los datos se recojan desde puntos de vista distintos y efectuando comparaciones múltiples de un fenómeno único, de un grupo, y en varios momentos, utilizando perspectivas diversas y múltiples procedimientos”

Se busca entonces una recolección de datos útil con ésta estrategia para el proyecto de investigación; tomando de referencia a COWMAN<sup>6</sup> entendemos que “La triangulación se define como la combinación de múltiples métodos en un estudio del mismo objeto o evento para abordar el fenómeno que se investiga.”

Se concluye que en este método se encuentran factores enlazados a empresas que hacen de la distribución de productos parte de su carga operativa, donde se debe

---

<sup>5</sup> PEREIRA PÉREZ, Zulay. Los diseños de método mixto en la investigación en educación: Una experiencia concreta. Revista Electrónica Educare, 2011, vol. 15, no 1.

<sup>6</sup> COWMAN, S. Triangulación: una media de reconciliación en la investigación en enfermería. Diario de Advanced Enfermería, 1993, vol. 18, p. 788-792.

identificar por qué lo hacen y qué variables se ven afectadas dentro del proceso de producción de la misma.

Debido a que la investigación se centra en el aseguramiento y validación de la evidencia digital derivada del análisis forense, la investigación presenta una triangulación de tipo secuencial, definida por MOGUEL<sup>7</sup> como el “uso de distintas perspectivas teóricas para analizar un mismo grupo de datos. A su vez, está orientada al contraste de hipótesis causales rivales. Es evidente que confrontar distintas teorías en un mismo grupo de datos permite una crítica eficiente coherente con el método científico.”

---

<sup>7</sup> MOGUEL, Ernesto A. Rodríguez. *Metodología de la Investigación*. Univ. J. Autónoma de Tabasco, 2005.

## 7. MARCO DE REFERENCIA

Dentro de la investigación documental previa sobre la informática forense no se hallaron procedimientos específicos para el aseguramiento y validación de la evidencia digital obtenida a partir de un análisis o procesos de informática forense. Aun así, se encontró evidencia en cuanto a creación de modelos, publicaciones, artículos y libros que hacen referencia al tratamiento de la evidencia digital, entre los cuales se destaca la informática forense, en la guía “Forensic Examination of Digital Evidence: A Guide for Law Enforcement”, en español “Examen forense de Evidencia Digital: Una guía para el cumplimiento de la ley”, la cual se constituye como referente de gran importancia para el desarrollo práctico de la informática forense en Colombia, U.S. DEPARTMENT OF JUSTICE<sup>8</sup>.

Por otro lado, se tienen las guías y modelos creados como “Guide to Integrating Forensic Techniques into Incident Response”, una publicación diseñada para ayudar a las organizaciones a investigar incidentes de seguridad informática y solucionar algunos problemas operativos de la tecnología de la información (TI) proporcionando una guía práctica sobre la realización de análisis forenses de computadoras y redes, GRANCE, CHEVALIER, KENT & DANG<sup>9</sup>.

Manuales desarrollados como el documento “Model Quality Assurance Manual for Digital Evidence Laboratories”, tienen el propósito de describir las mejores prácticas para recolectar, adquirir, analizar y documentar los datos encontrados en los exámenes forenses informáticos. (SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE SWGDE<sup>10</sup>.

La organización SWGDE también produjo la guía identificada como: “SWGDE Model Standard Operation Procedures for Computer Forensics”, la cual tiene como objeto crear un documento de muestra de trabajo que las organizaciones puedan utilizar como plantilla para producir su propio estándar documentado de procedimientos, SWGDE<sup>11</sup>.

El anterior modelo, va emparejado con el documento “SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence”, cuyo propósito

---

<sup>8</sup> U.S. DEPARTMENT OF JUSTICE. (Abril de 2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. *National Institute of Justice*. {En línea}. {02 de agosto de 2017}

<sup>9</sup> GRANCE. TIMOTHY. CHEVALIER. SUZANNE., KENT. KAREN. DANG. Hung. Guide to Integrating Forensic Techniques into Incident Response. {End line}. 01 de septiembre de 2006

<sup>10</sup> SWGDE. SWGDE Best Practices for Computer Forensics. {En línea}. 5 de septiembre de 2014. {02 de agosto de 2017}

<sup>11</sup> SWGDE. SWGDE Model Standard Operation Procedures for Computer Forensics. 13 de septiembre de 2012. {En línea}. {02 de agosto de 2017}

es proporcionar directrices y recomendaciones para ayudar a diseñar un programa formación adecuada SWGDE<sup>12</sup>.

Por su parte los documentos desarrollados por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional (ISO/IEC), entre los cuales se cuenta la norma “ISO/IEC 27001”, “Sistemas de gestión de la seguridad de la información”, R2013, la cual es la base para la adaptación de otras guías o normas; entre las cuales se tienen los puntos de control del “Código de prácticas para controles de seguridad de la información”, “ISO/IEC 27002”, que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información; Así mismo la “ISO/IEC 27037:2012<sup>13</sup>”, norma que define las directrices para la identificación, recolección, adquisición y preservación de la evidencia digital. Además, se tiene la guía “GTC-ISO/IEC 27035”, que brinda orientación sobre la gestión de incidentes de seguridad de la información para empresas grandes y medianas.

Por último se encuentra el Manual de Cadena de Custodia, actualizado y producido por la Fiscalía General de la Nación de Colombia en el 2016; donde se establecen procesos para el aseguramiento y preservación de la evidencia física o elementos materiales probatorios dentro del sistema penal; donde se hallan descritos algunos procedimientos que pueden ser análogos para el aseguramiento de la evidencia digital, así mismo describe de forma general el embalado, rotulado y registros de cadena de custodia. (Fiscalía General de la Nación de Colombia, 2016). Y el documento creado por MINTIC, titulado “Evidencia Digital”, el cual es una guía general para realizar el análisis informático a la evidencia digital.

## 7.1. MARCO DE ANTECEDENTES

Actualmente existen proyectos, guías y desarrollos relacionados con la gestión y administración de la evidencia digital, en donde se establecen procesos para la obtención de evidencia bajo los parámetros fundamentales de la seguridad de la información como la integridad, confidencialidad y la disponibilidad de la misma.

Dentro de los estudios identificados en los diferentes documentos no se observan procedimientos relacionados con el aseguramiento y validación de la evidencia digital obtenida a partir de análisis forenses; por tanto, que se trata de un proceso reverso para establecer la autenticidad de la evidencia digital. A continuación, se mencionan algunos documentos relacionados:

---

<sup>12</sup> Swgde. Swgde/swgit Guidelines & Recommendations for Training in Digital & Multimedia Evidence. {En línea}. 15 de enero de 2010. {02 de agosto de 2017}

<sup>13</sup> ISO/IEC 27037:2012. . {En línea}. 23 de octubre de 2012. {02 de septiembre de 2017}

Evidencia Digital, es un documento producido por MINTIC Colombia en el año 2016, en primera versión; en el cual se dan los lineamientos para realizar un proceso de informática forense, posterior a la gestión de un incidente informático donde se ha surtido los procesos de análisis, evaluación y decisión, determinando la necesidad de la recolección de evidencia digital para iniciar alguna acción de tipo legal o disciplinaria.

Investigaciones relacionadas con la Administración de la Evidencia Digital resaltan la admisibilidad y valor probatorio de la evidencia digital, lo cual se apalanca en proceso de auditoría y trazabilidad de la información digital a través de diferentes técnicas CANO<sup>14</sup>. También se realizan acercamientos al tratamiento de la evidencia digital como un soporte legal con capacidad probatoria de hechos ilícitos ante el sistema penal, MAMANI<sup>15</sup>.

## 7.2. MARCO DE CONTEXTO

La delimitación de la investigación del proyecto corresponde al diseño de un procedimiento para el aseguramiento y validación de la evidencia digital derivada del análisis forense informático, producida por el laboratorio de informática forense Fiscalía General De La Nación, Seccional Tolima; su objetivo final corresponde a la producción de un documento soportado en normas y estándares de seguridad de la información; que describe en forma detallada el aseguramiento de evidencia digital, así como el procedimiento y puntos de control para la validación de la evidencia.

Por lo anterior se requiere la identificación de normas, estándares y otros documentos que puedan ser usados como soporte técnico y procedimental, para el aseguramiento y validación de la evidencia digital. De igual forma se requiere conocer a través de inspecciones, entrevistas y observación, el estado del sistema objeto de investigación; a fin de comprender la situación actual frente al proceso relacionado con la generación y aseguramiento de la evidencia digital derivada de análisis informático.

El proyecto se desarrolla en un periodo de cuatro meses aproximadamente, en el cual se desarrolla el trabajo de campo e identificación de documentos que representan en el marco teórico para el desarrollo del procedimiento a implementar sobre el aseguramiento y validación de la evidencia digital derivada de análisis forense informático.

---

<sup>14</sup> CANO. Jeimy. Evidencia Digital Reflexiones Técnicas, Administrativas y Legales. {En línea}. {01 de mayo de 2017}

<sup>15</sup> MAMANI. Verónica. Método forense en redes de telecomunicación para la admisión de evidencia digital en la justicia boliviana. {En línea}. 28 de Junio de 2015. {13 de agosto de 2017}

### 7.3. MARCO TEÓRICO

Cuando se hace referencia a los procesos de aseguramiento y validación de la información, se hace indispensable definir los conceptos y nociones que posibilitan comprender de manera teórica las propuestas en este proyecto; en este orden de ideas, cuando se habla de los procedimientos en el contexto ya mencionado anteriormente es necesario entender que estos constituyen un conjunto de operaciones conectadas entre sí, organizadas de manera diacrónica y sincrónica, todo procedimiento involucra de acuerdo a su aplicación métodos y diarios de campo que permita cumplir la función determinada, S/A<sup>16</sup>. De acuerdo con lo anterior, dichos procesos van a generar un engranaje óptimo frente a el aseguramiento y validación de la información en la medida que se garanticen la veracidad y autenticidad de la información, dicho de esta manera la investigación del trabajo en curso toma relevancia, pues generará estrategias coherentes a las necesidades que puedan presentarse.

Como se puede evidenciar el aseguramiento y la validación de la información tiene elementos fundamentales los cuales indican la importancia de: “los métodos para generar claves o llaves que representan de manera unívoca un documento o conjunto de datos en cualquier extensión mediante una aplicación de una función matemática aplicada al conjunto de datos dando salida a la información por medio de una huella digital la cual siempre va a ser legible utilizando la función HASH”<sup>17</sup>.

El HASH MD5 (técnicamente llamado Message-Digest Algorithm), fue desarrollado por Ronald Rivest; es una función de HASH criptográfica cuyo objetivo principal es verificar que un archivo no ha sido alterado. El MD5 es una función usada generalmente para la verificación de archivos, de los cuales se obtienen un valor hexadecimal de 128 bits y normalmente se muestran en su equivalente hexadecimal de 32 dígitos. Aunque en la actualidad MD5 ha sido considerado una función insegura dentro de sistemas criptográficos, se observa una gran utilidad para la verificación de autenticidad de archivos a través de la suma de comprobación del valor hexadecimal inicialmente obtenido o suministrado en la fuente de la información digital, FISHER<sup>18</sup>.

El SHA-1 (abreviatura de Algoritmo de hash seguro) es una de varias funciones de hash criptográficas, desarrollada por la Agencia de Seguridad Nacional de Estados

---

<sup>16</sup> SIN AUTOR (S/A). Definición de procedimiento. {En línea}. {08 de mayo de 2017} disponible en (<http://www.definicion.org/procedimiento>).

<sup>17</sup> DE LUZ. Sergio. Criptografía: Algoritmos de autenticación (hash). {En línea}. 09 de noviembre de 2010. Disponible en: (<https://www.redeszone.net/2010/11/09/criptografia-algoritmos-de-autenticacion-hash/>).

<sup>18</sup> FISHER. Tim. What is md5? (md5 message-digest algorithm). (05 de octubre de 2016). {en línea}. {15 de septiembre de 2017}.

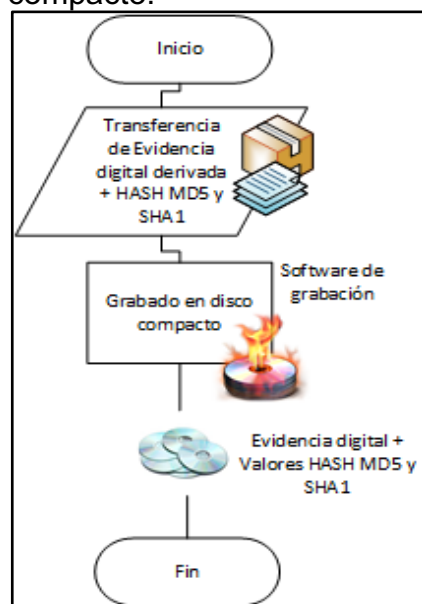




cual se logra con ayuda de una aplicación para realizar el cálculo o extracción de HASH en los algoritmos MD5, SHA1, SHA2 SHA3; procedimiento del cual se obtiene un archivo que relaciona el directorio, nombre de archivo y valores HASH calculados para cada uno de los archivos digitales identificados como evidencia digital; seguidamente se realiza el proceso de preservación transfiriendo los datos con la respectiva huella digital HASH a discos compactos considerados como dispositivos de almacenamiento óptico, lo cuales se deben finalizar con respecto a la actualización, modificación o eliminación de datos digital.

La evidencia digital derivada del análisis forense, tiene que ser individualizada a través de HASH y posteriormente se transfiere en lo posible a unidades de almacenamiento no modificables. En la actualidad se cuenta con los denominados discos compactos o unidades ópticas en diferentes presentaciones como CD R (700MB), DVD R (4,7 GB - 8,5 GB), y Blu-Ray (25 GB – 50 GB). Para cuando la evidencia digital derivada supera la capacidad máxima de almacenamiento de las unidades ópticas; se debe realizar transferencia en paquetes de datos de imágenes forenses digitales, con formatos que permitan realizar el montaje virtual para su respectivo análisis, garantizando que los datos son montados o cargados en modo de lectura únicamente.

Figura 2. Grabación disco compacto.



Fuente: Propia.

Los laboratorios de informática forense se encuentran a la vanguardia en tecnología mediante la implementación de nuevas tecnologías para el análisis de dispositivos electrónicos con almacenamiento de información digital; por tanto, las herramientas de software y hardware forense, son desarrolladas en la actualidad por compañías entre las cuales se destacan Cellebrite, AccessData, Guidance y Tableau.

Las herramientas desarrolladas por Cellebrite, corresponden a hardware y software forense para la extracción de información y análisis de la misma, a dispositivos móviles y otros medios de comunicación, las cuales cuentan con grandes bondades como el salto de sistemas de cifrado y seguridad por contraseña, aplicable en marcas y modelos reconocidas.

AccessData y Guidance desarrollan las herramientas de software forense FTK Tools y Encase respectivamente; las cuales tienen como objetivo realizar la adquisición de imágenes forenses a dispositivos de almacenamiento de información digital. Una vez obtenida los duplicados a través de las imágenes forenses digitales se ejecutan procesos automatizados a fin de identificar, recuperar, seleccionar y administrar el contenido o evidencia digital de cada uno de los dispositivos de almacenamiento procesados. Posteriormente se realizan informes de presentación el cual transfiere un duplicado idéntico de la evidencia incluyendo metadatos y huellas digitales HASH.

Por último, se tienen los bloqueadores de escritura, los cuales pueden ser de hardware o software; los más reconocidos por su efectividad y compatibilidad es la marca Tableau. La marca Tableau dispone de múltiples interfaces de conectividad entre las que se destacan los formatos SATA, SAS, IDE y USB; las cuales son las más estándar o adaptables a otras interfaces personalizadas por algunas marcas de dispositivos de almacenamiento.

De esta manera, al analizar detenidamente la evidencia digital a través de los protocolos y procedimientos, se facilitan y garantizan resultados eficaces; no obstante, se debe contextualizar lo que se comprende por evidencia digital, para no tener ambigüedades y poder categorizar la información de acuerdo a la situación que lo prevé. De acuerdo al sitio web INFORMÁTICA FORENSE COLOMBIA<sup>21</sup> la evidencia digital o prueba electrónica, 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; de acuerdo a lo anterior es importante que la información recolectada sea tratada con la rigurosidad que se debe, debido a que es el referente para los procesos judiciales y penales en la normativa colombiana, aclarando de ante mano que se debe verificar los procesos de recuperación, almacenamiento y análisis bajo las debidas técnicas de auditoría y posible recreación del proceso forense a fin de obtener el mismo resultado.

De este modo las técnicas y herramientas especializadas para el análisis de elementos materiales probatorios como equipos electrónicos o dispositivos de almacenamiento de información digital, deben contemplar los procesos relacionados con las fases para la identificación, preservación, análisis, obtención

---

<sup>21</sup> INFORMÁTICA FORENSE COLOMBIA. (12 de marzo de 2017). *Informática forense Colombia. La evidencia digital*. {en línea}. {02 de agosto de 2017}

de pruebas y la presentación de datos o información con una ilustración contextual de los hechos descubiertos para que sean válidos dentro de un proceso legal. En este sentido la Fiscalía General de la Nación como órgano estatal encargado de velar y perseguir la investigación penal dentro del sistema judicial, debe brindar a los ciudadanos medios de investigación eficaz para la determinación y administración de la justicia, evitando fraudes y elementos viciados para emitir un juicio más acertado de los hechos en Colombia.

Según SARAVI<sup>22</sup> un término fundamental en esta investigación es la comprobación de la autenticidad de la información digital obtenida, que se identifica como evidencia digital derivada encontrada en la escena del acontecimiento o medios tecnológicos comprometidos dentro de una investigación. Por otro lado HERNANDEZ<sup>23</sup> indica que se tiene la confiabilidad de la información, si es de una fuente verificable y creíble, que no esté presta a malas lecturas del contexto, sí esto llegase a ocurrir se puede generar acciones antijurídicas y delitos informáticos, al no tratar la información con la rigurosidad que se requiera.

La autenticidad de la evidencia digital de acuerdo al Manual de cadena de custodia de la FISCALÍA GENERAL DE COLOMBIA<sup>24</sup> depende de la preservación de la misma; por lo cual una vez realizado un examen forense y obtenido la evidencia digital en su respectiva unidad de almacenamiento; se debe gestionar el aseguramiento de la evidencia a través de la documentación por medio de imágenes que referencian el elemento físico. Luego de la documentación se realiza el embalado en un contenedor adecuado para su protección, el cual debe estar completamente sellado con su respectivo rotulo donde se identifica el número de caso de investigación, lugar de hallazgo o procedencia, fecha y hora de la recolección, identificación de la persona que realiza la recolección y descripción del elemento contenido, FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA<sup>25</sup>.

Para la protección de dispositivos electrónicos de almacenamiento de información digital como discos duros, equipos de cómputo, memorias USB, GPS, teléfonos celulares y otros similares, se debe realizar embalado en contenedores adecuados como bolsas burbuja antiestática o cajas de material adecuado que protejan de descargas de electricidad estática golpes y deformaciones por presión de otros

---

<sup>22</sup> SARAVI, V. M. 20 de Junio de 2015. Método Forense en Redes de Telecomunicaciones para la Admisión de Evidencia Digital en la Justicia Boliviana. La Paz.

<sup>23</sup> HERNANDEZ, S. 23 de Abril de 2017. Delitos Informáticos?. Machetá. [Folleto en línea] Obtenido de [https://issuu.com/sergiohernandessalcedo/docs/delitos\\_1\\_](https://issuu.com/sergiohernandessalcedo/docs/delitos_1_)

<sup>24</sup> FISCALIA GENERAL DE LA NACIÓN. julio de 2017. manual de procedimientos para cadena de custodia.

<sup>25</sup> FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA. Glosario Grupo *Delitos Informáticos. Versión 01*. Subproceso Policía Judicial. (2014). *Proyecto Guía Delitos Informáticos*. Bogotá: Procesos de normalización

elementos contundentes. Adicional a lo anterior se deben realizar rótulos que identifiquen prevención de no exponer a fuentes de radiación electromagnética.

Figura 3. Rotulo de contenedor de evidencia.

**RÓTULO ELEMENTOS MATERIALES DE PRUEBA Y EVIDENCIA FÍSICA**  
Versión 3 - Revisión 2016

**I. NÚMERO ÚNICO DE CASO**

EP 01	RECOLECCIÓN	TIPO DE CASO	TIPO DE DELITO	FECHA	HORA	LOCALIDAD
-------	-------------	--------------	----------------	-------	------	-----------

**II. FECHA Y HORA DE RECOLECCIÓN**

AA	MM	DD	HH	MM	SS
----	----	----	----	----	----

**III. HALLAZGO**

**IV. LUGAR DE HALLAZGO DEL ELEMENTO MATERIAL DE PRUEBA Y EVIDENCIA FÍSICA**

**DIRECCIÓN:**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**UBICACIÓN:**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**V. NOMBRE Y APELLIDOS DE LA PERSONA A QUIEN SE LE ENCONTRÓ EL EMP Y EP**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**VI. CONTENIDO DEL ELEMENTO MATERIAL DE PRUEBA Y EVIDENCIA FÍSICA**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**VII. RÓTULO ELABORADO POR:**

NOMBRE Y APELLIDOS	FECHA DE ELABORACIÓN	ESTADO	CÓDIGO	TIPO
--------------------	----------------------	--------	--------	------

Fuente: Manual de cadena de custodia FGN-2016.

Además del embalado y rotulado se debe considerar de vital importancia la cadena de custodia la cual corresponde a una bitácora que registra la tenencia o custodia del elemento; donde se identifica la fecha, hora, identificación de la persona, calidad en la que actúa el custodio, observaciones y anotaciones de importancia.



#### 7.4. MARCO CONCEPTUAL

**DELITO INFORMÁTICO:** Conducta ilícita realizada con el fin de alterar, dañar, borrar, transmitir o utilizar datos electrónicos para ejecutar un esquema de fraude, engaño, extorsión u obtención de dinero, propiedades o datos, mediante el uso de la tecnología sin autorización o con ella, interrumpiéndolos, asistiendo a otros en el acceso ilegal a sistemas de cómputo o introduciendo lenguaje de programación y/o código fuente dañino en un sistema informático.

**DISCO DURO:** Disco de metal cubierto con una superficie de grabación magnética. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.<sup>26</sup>

**ENCASE:** Herramienta de software para el procesamiento forense de evidencia digital, Desarrollada por Guidance Software, es una de las mejores aplicaciones existentes en la actualidad que permite realizar un completo análisis forense de diversos sistemas operativos, permitiendo crear una Imagen exacta Bit a Bit del Disco original.

**ESTACIÓN FORENSE:** En informática forense se refiere a un equipo de cómputo dotado con una configuración avanzada tanto de software como de hardware, que permite realizar desde la adquisición de la imagen forense hasta el examen de la información contenida en ellas.

**EVIDENCIA DIGITAL:** Es todo dato digital que compone el resultado de un proceso de informática forense, donde se resalta la documentación e individualización a través de la extracción de HASH para cada uno de los archivos obtenidos.

**FORENSIC TOOLKIT (FTK):** Herramienta de software para el procesamiento forense de evidencia digital, desarrollada por Access Data, permite obtener resultados rápidos y eficientes.

**HARDWARE:** Maquinaria. Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).

**HASH:** Es un valor alfanumérico calculado a través de algoritmos especializados a partir del contenido de un archivo lo que permite garantizar su integridad. Es para los archivos las veces de Huella Digital. Cualquier modificación a un archivo, hace que el valor HASH cambie y por tal motivo se considera alterado o diferente al cálculo inicial.

---

<sup>26</sup> [www.internetglosario.com/753/Discoduro](http://www.internetglosario.com/753/Discoduro)

INFORMÁTICA FORENSE: es la aplicación de técnicas científicas y analíticas especializadas e infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.<sup>27</sup>

UFED TOUCH ULTIMATE: Hardware y software forense que permite la extracción, decodificación, análisis y generación de informes de datos móviles más tecnológicamente avanzada. Realiza la extracción física, lógica, del sistema de archivos y contraseñas de todos los datos (aunque hayan sido eliminados) del más amplio rango de dispositivos, que incluye teléfonos antiguos y comunes, teléfonos inteligentes, dispositivos GPS portátiles, tabletas y teléfonos con chipsets de manufactura china.<sup>28</sup>

## 7.5. MARCO LEGAL

LEY 1273 de 2009<sup>29</sup>, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones:

CAPITULO. I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

CAPITULO. II. De los atentados informáticos y otras infracciones.

LEY 527 DE 1999<sup>30</sup> (18 de agosto) Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones (CONGRESO DE LA REPUBLICA, 1999).

---

<sup>27</sup> INFORMÁTICA FORENSE COLOMBIA. (12 de Marzo de 2017). INFORMÁTICA FORENSE COLOMBIA. La evidencia Digital. {En línea}. {02 de agosto de 2017} Disponible en: <<http://www.informaticaforense.com.co/la-evidencia-digital/>><sup>27</sup>

<sup>28</sup> CELLEBRITE. Definición de Ufed Touch Ultimate. {En línea}. {09 de septiembre de 2017} disponible en: <<https://www.cellebrite.com/es/products/ufed-ultimate-es/>>

<sup>29</sup> CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. Bogotá. Diario oficial 47.223, 2009.

<sup>30</sup> CONGRESO DE LA REPÚBLICA. ley 527 de 1999. *ley 527 de 1999*. Bogotá. diario oficial 43.673, 1999.



Código de Procedimiento Penal LEY 906 de 2004<sup>31</sup>

Artículo 260 CPP. El perito que reciba el contenedor dejará constancia del estado en que se encuentra y procederá a las investigaciones y análisis del elemento material probatorio y evidencia física, a la menor brevedad posible, de modo que su informe pericial pueda ser oportunamente remitido al fiscal correspondiente.

Artículo 270 CPP. Recibida la solicitud y los elementos mencionados en los artículos anteriores, el perito los examinará. Si encontrare que el contenedor, tiene señales de haber sido o intentado ser abierto, o que la solicitud no reúne las mencionadas condiciones lo devolverá al solicitante. Lo mismo hará en caso de que encontrare alterado el elemento por examinar. Si todo lo hallare aceptable, procederá a la investigación y análisis que corresponda y a la elaboración del informe pericial. El informe pericial se entregará bajo recibo al solicitante y se conservará un ejemplar de aquel y de este en el Instituto.

Artículo 228 CPP. Terminada la diligencia de registro y allanamiento, dentro del término de la distancia, sin sobrepasar las doce (12) horas siguientes, la policía judicial informará al fiscal que expidió la orden los pormenores del operativo y, en caso de haber ocupado o incautado objetos, en el mismo término le remitirá el inventario correspondiente, pero será de aquella la custodia de los bienes incautados u ocupados, congreso de la república.

En caso de haber realizado capturas durante el registro y allanamiento, concluida la diligencia, la policía judicial pondrá inmediatamente al capturado a órdenes del fiscal, junto con el respectivo informe.

Artículo 257 CPP. Inicio de la cadena de custodia: El servidor público que, en actuación de indagación o investigación policial, hubiere embalado y rotulado el elemento material probatorio y evidencia física, lo custodiará, Congreso de la república.

---

<sup>31</sup> CONGRESO DE LA REPÚBLICA. actuación del perito. *código de procedimiento penal ley 906 de 2004*. Bogotá: diario oficial no. 45.658, 2004.

## 8. DESARROLLO DE PROYECTO.

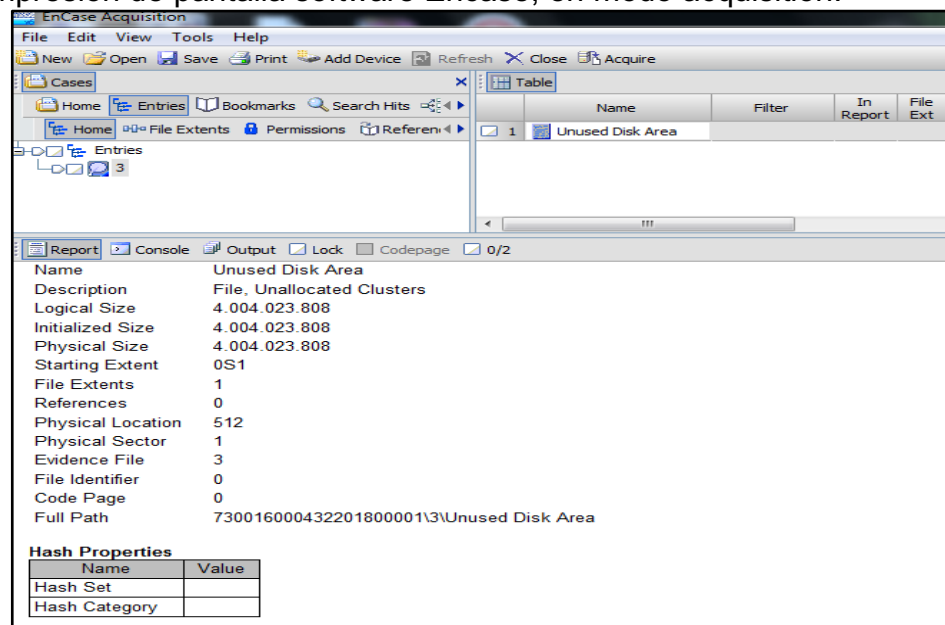
### 8.1. HERRAMIENTAS ACTUALES DEL LABORATORIO DE INFORMÁTICA FORENSE DE LA FISCALÍA GENERAL SECCIONAL TOLIMA

De acuerdo a labores de campo, documentadas en el anexo B, Identificación de procesos de informática forense, donde se recolecta o produce evidencia digital; se establece que el laboratorio de informática forense de la Fiscalía General Seccional Tolima cuenta con las siguientes herramientas:

#### 8.1.1. Herramientas de software forense.

##### 8.1.1.1. Encase Forensic – Guidance.

Figura 6. Impresión de pantalla software Encase, en modo acquisition.



Fuente: Propia.

Herramienta de software forense, producido por la empresa Guidance con el objetivo de realizar procesamientos automatizados para la adquisición de imágenes forenses digital, el análisis de datos digitales contenidos en dispositivos de almacenamiento de información de tipo electrónico como discos duros, memorias USB, dispositivos de comunicación celular y entre otros.

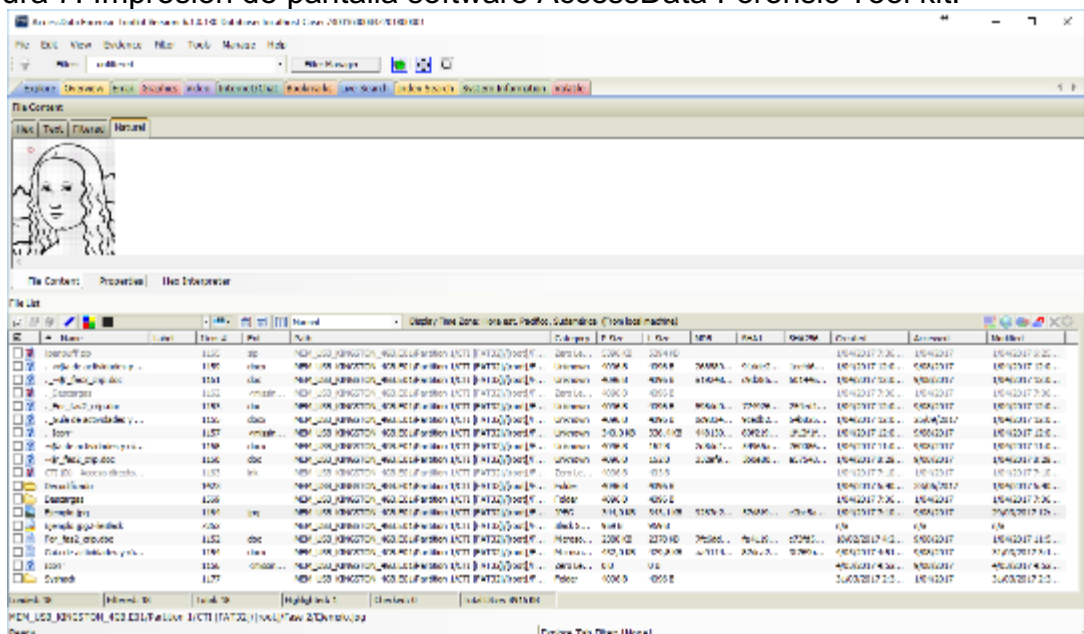
Su funcionamiento es sencillo ya que procesa sobre bases de datos dinámicas integradas a cada uno de los casos de procesos; por tal motivo no depende de un

motor de bases de datos y puede ser portado de forma libre para ser ejecutado en cualquier máquina donde se halle instalado el software Encase.

El procesamiento de Encase recupera, identifica y asegura la evidencia mediante el cálculo HASH en diferentes formatos; lo anterior de acuerdo a procesos configurados que pueden ser ejecutados por separado para una mayor eficiencia y rendimiento en los procesos de análisis. De igual forma permite realizar búsquedas de palabras claves o parámetros mediante el arreglo de expresiones regulares tipo grep, que identifica patrones de caracteres de acuerdo a la estructura de la expresión regular.

### 8.1.1.2. Forensic Tool Kit (FTK) – AccessData.

Figura 7. Impresión de pantalla software AccessData Forensic Tool kit.



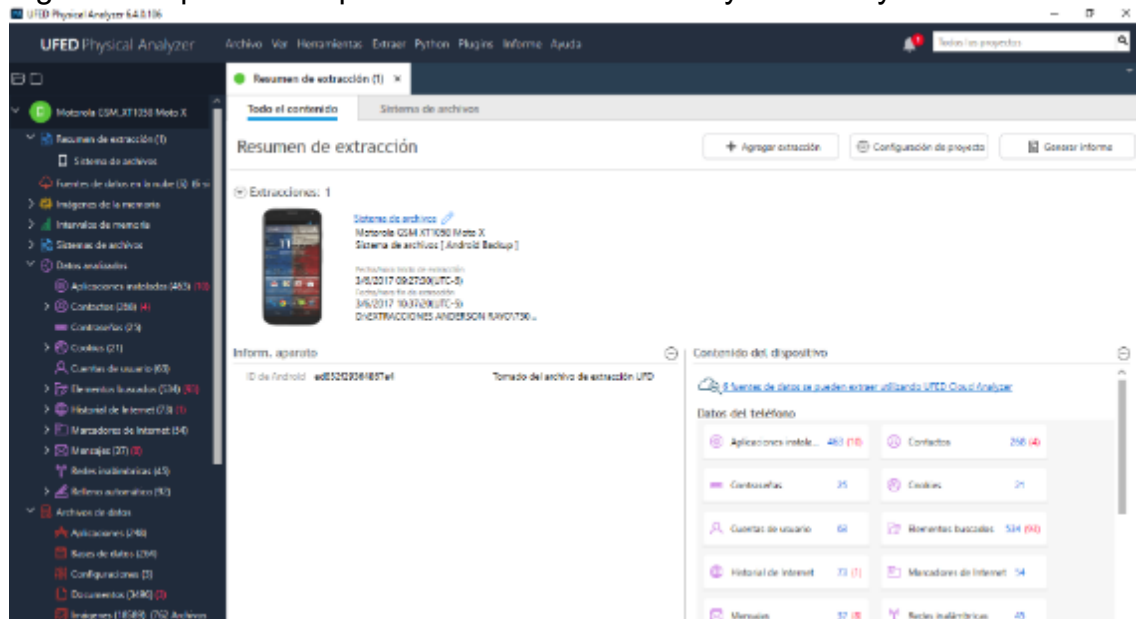
Fuente: Propia.

Los procesos y objetivos de análisis realizan los mismos procedimientos automatizados descritos para la herramienta Encase, excepto por su funcionamiento ya que depende del gestor de bases de datos PostgreSQL. Por tal motivo no es posible realizar la portabilidad de caso de forma sencilla, por lo cual se debe realizar un back up a fin de restaurarlo en otra máquina.

Entre sus ventajas se destacan herramientas de gran utilidad como OCR (Reconocimiento de Caracteres sobre imágenes), reconocimiento de imágenes explícitas, detección de software malicioso y entre otros; con lo cual supera por gran ventaja a otras herramientas de software similares.

### 8.1.1.3. Physical Analyzer

Figura 8. Impresión de pantalla software UFED Physical Analyzer.



Fuente: Propia.

Herramienta de software forense desarrollada por la empresa Cellebrite, utilizada para la gestión y análisis de paquetes de datos extraídos de teléfonos celulares a través de la herramienta de hardware forense UFED Ultimate – Cellebrite.

### 8.1.2. Herramientas de Hardware Forense

#### 8.1.2.1. UFED Ultimate Touch – Cellebrite

Figura 9. Equipo UFED Ultimate Touch.



Fuente: Propia.

Herramienta de hardware forense desarrollada por la empresa Cellebrite, la cual cuenta con múltiples interfaces de conexión con el objetivo de realizar extracción de información a dispositivos de comunicación móvil como teléfonos celulares, GPS, Radios de comunicación y entre otros.

#### 8.1.2.2. Servidores de alto rendimiento Digital Intelligence

Figura 10. Equipo FREDDIE Digital Intelligence.



Fuente: Propia.

Equipos de cómputo diseñados y creados por la empresa Digital Intelligence, con el fin de realizar adquisición de imágenes forenses mediante interfaces de conexión habilitadas únicamente para la lectura de datos, no se permite la modificación o eliminación.

#### 8.1.2.3. Servidores de alto rendimiento MicroSystem con Kit de bloqueadores contra escrituras.

Figura 11. Servidor MicroSystem



Fuente: Propia.

Equipos de cómputo de alto rendimiento a fin de agilizar el procesamiento de datos a través de las herramientas de software forense.

#### 8.1.2.4. Kit de bloqueadores Tableau.

Figura 12. Kit de bloqueadores Tableau e interfaces adaptadoras.



Fuente: Propia.

Hardware especializado con el fin de intermediar en la interfaz de conexión, únicamente permite la lectura de datos, más no la eliminación y modificación de los mismos.

#### 8.1.2.5. Equipos de apoyo

- Equipos de cómputo.
- Discos Duros Portables de Alta capacidad.
- Discos duros internos Sata de alta capacidad.
- Cámaras fotográficas.
- Testigos métricos.
- Discos compactos tipo CD-R, DVD-R y Blu-Ray-R.

De acuerdo a lo anterior, se observa que el laboratorio de informática forense cuenta con herramientas de hardware y software forense diseñado para la protección, recuperación y análisis de información digital contenida en dispositivos de almacenamiento electrónicos, magnéticos y ópticos. Las herramientas son capaces de generar reportes digitales para el análisis de contexto de la información obtenida. De igual forma se aprecian equipos de apoyo que permiten realizar actividades complementarias como la documentación, fijación y almacenamiento de la evidencia digital derivada de los procesos forenses.

De acuerdo a entrevista expuesta en el Anexo D. (J. B. Ávila), acorde a la inspección, se establecen los procesos realizados en el laboratorio de informática forense donde se obtiene evidencia digital derivada. Los procesos corresponden a dos tipos de procedimientos, en el primer tipo de procedimiento se obtiene evidencia derivada de procesos netamente forenses mediante la aplicación de herramientas sobre elementos electrónicos, magnéticos y ópticos, que contienen información digital. La segunda categoría corresponde a procedimientos de documentación y recolección de información en ambientes virtuales como sitios web, bases de datos u otros sistemas de información; que deben ser inspeccionados directamente a fin de obtener la evidencia digital derivada que permite probar un hecho ocurrido. A continuación, se relacionan los procedimientos identificados; así:

Tabla 1. Recolección de información.

Procedimiento	Elementos examinados	Herramientas.
Extracción de información digital a dispositivos de almacenamiento electrónico masivos y similares	<ul style="list-style-type: none"> <li>● Discos duros</li> <li>● Memorias USB y MSD</li> <li>● Discos Compactos tipo CD, DVD y Blu-ray.</li> <li>● Dispositivos electrónicos con almacenamiento de información incorporada como Grabadoras, Cámaras fotográficas y otros</li> </ul>	<ul style="list-style-type: none"> <li>● Encase – Guidance.</li> <li>● Forensic Tool Kit (FTK) – Access Data.</li> <li>● Herramientas de protección contra escritura o modificación de datos.</li> </ul>
Extracción de información a dispositivos de comunicación inalámbrica y similar.	<ul style="list-style-type: none"> <li>● Teléfonos Celulares</li> <li>● Teléfonos Inalámbricos de largo alcance</li> <li>● Teléfonos Satelitales</li> <li>● GPS</li> </ul>	<ul style="list-style-type: none"> <li>● Universal Forensic Evidence Device – Cellebrite.</li> <li>● Herramientas de protección sobre escritura o modificación de datos.</li> </ul>
Inspección a páginas web, con fines de documentación y recolección de evidencia digital.	<ul style="list-style-type: none"> <li>● Páginas web con contenido público injurioso o inapropiado.</li> <li>● Mensajería web en redes sociales.</li> <li>● Mensajes de correo electrónico en cuentas aportadas por las víctimas.</li> </ul>	<ul style="list-style-type: none"> <li>● Captura de pantalla.</li> <li>● Descarga directa de explorador web.</li> <li>● Impresión a formatos digitales como PDF.</li> <li>● Extracción de HASH con FTK Imager.</li> </ul>

Tabla 1. Recolección de información. (Continuación)

Procedimiento	Elementos examinados	Herramientas.
Identificación de administración ISP para IP Publica, dominios o hosting web.	<ul style="list-style-type: none"> <li>• Dominios web maliciosos.</li> <li>• Páginas de pornografía.</li> <li>• Publicaciones inapropiadas.</li> </ul>	<ul style="list-style-type: none"> <li>• Medios abiertos sobre Internet de registros de dominios como Lacnic, Arin, DomainTools y otros.</li> </ul>
Detección y análisis de Malware	Equipos de cómputos comprometidos, aportados por la víctima.	<p>Herramientas de protección sobre escritura o modificación de datos.</p> <p>Herramientas de protección sobre escritura o modificación de datos.</p>
Obtención de registros y auditorias.	<p>Sistemas de información.</p> <p>Bases de datos.</p>	Inspección directa en el sistema de información bajo el acompañamiento de administradores del mismo; documentación a través de impresiones de pantalla y extracción de HASH para la evidencia obtenida.
Extracción de HASH	Evidencia derivada.	Extracción de HASH con FTK Imager.
Grabado (Duplicado) de evidencia digital derivada	Evidencia digital	Equipo de cómputo y grabadores de discos compactos.

Autor: propio

Identificados los anteriores procedimientos, se observa un método de individualización e identificación de la evidencia digital derivada, mediante la extracción o cálculo de huella digital HASH MD5 Y SHA1, posteriormente se realiza grabado o duplicado de la evidencia junto con el respectivo cálculo HASH en un disco compacto u otro contenedor de información digital adecuado para el aseguramiento de evidencia digital.



De igual forma se conoce a través de las entrevistas realizadas el procedimiento general mediante herramientas hardware y software forense para la extracción de información a dispositivos de almacenamiento de información digital, de comunicación móvil y similar; así:

- Descripción de la evidencia objeto de análisis.
- Documentación fotográfica de la evidencia objeto de análisis.
- Preparación de herramientas de hardware y software forense necesarias.
- Aplicación de herramientas forenses, de acuerdo a guías propias de manejo indicadas en las herramientas de hardware y software forense, para realizar extracción de imagen forense bit a bit o volcado de información en paquetes de datos en formato propio de las herramientas forenses.
- Análisis, gestión y reportes con herramientas de análisis, aplicadas a la extracción de imagen forense bit a bit o volcado de información en paquetes de datos. En el cual se identifican atributos y calculo HASH, para cada uno de los archivos obtenidos. El reporte por lo general es un esquema de presentación digital en formatos HTML, PDF, Excel e incluso visores propios de la misma herramienta de análisis, donde se relaciona la evidencia digital exportada a directorios vinculados al reporte.
- En el reporte con la herramienta de software forense de análisis y gestión se obtienen metadatos o atributos de la evidencia digital obtenida, así como el cálculo HASH para cada uno de los archivos, donde se observa que los archivos propios del reporte no contienen calculo HASH. Por tal motivo se aplica cálculo HASH a todos los archivos que componen el reporte de evidencia digital derivada, lo anterior permite documentar la integridad general de todos los archivos que componen la nueva evidencia digital derivada, incluyendo la identificación de archivos que componen la estructura del reporte de la herramienta de software forense.
- El cálculo de HASH para cada uno de los archivos, por lo general corresponde a un gran listado de información donde se relaciona la ruta de directorio, nombre de archivo, HASH MD5 y SHA1, de lo cual se generan gran cantidad de registros que al ser impresos ocuparían gran cantidad de páginas. Por lo anterior se procede a calcular HASH al listado general que contiene la lista HASH de archivos, obteniendo como resultado un sólo registro HASH que permite realizar una verificación en cadena con respecto a la evidencia digital derivada del análisis forense realizado. Este último registro HASH se relaciona en el respectivo informe de laboratorio, garantizando la verificación de la información obtenida en el proceso forense.

- Obtenidos los reportes que vinculan la evidencia digital, junto con la extracción de HASH, se procede a realizar almacenamiento o grabación de información en contenedor adecuado sin sobre escritura como CDR, DVDR, BLU RAY R. Para las evidencias que superan la capacidad de almacenamiento de los contenedores antes descritos no se tiene procedimiento claro puesto que los contenedores corresponden a dispositivos de almacenamientos susceptibles de modificación e incluso eliminación de la evidencia digital cuando sea examinada por los analistas de información o investigadores de caso.
- Obtenidos los discos compactos o unidades de almacenamiento (contenedores de evidencia digital), se procede a realizar documentación fotográfica del elemento, embalado y rotulado. Se utiliza un embalado previo que proteja el contenedor físico de golpes o deformaciones, para lo cual se utilizan estuches de pasta o cubiertas de cartón. El embalado es una protección sellada y se tiene en cuenta en la descripción del rótulo el último recubrimiento externo. En cuanto al rótulo corresponde a un formato normalizado en el manual de cadena de custodia de la Fiscalía General de la Nación. Adicional al embalado y rotulado se tiene el anexo de cadena de custodia, el cual corresponde a un formato normalizado por la Fiscalía, en donde se relaciona el registro de custodios o portadores de la evidencia, objeto y observaciones.
- Como último proceso se tiene la disposición final de la evidencia derivada la cual debe ser referenciada en el informe, es decir mencionar el destino de la evidencia, el cual puede ser el almacén de evidencias, análisis de contexto para la información o custodia por parte del investigador que solicita el análisis forense.

## 8.2. RECONOCIMIENTO DE NORMAS Y ESTÁNDARES

Una vez reconocida la norma y estándares relacionadas en el marco de referencia y marco teórico, se tiene como referencia internacional la norma ISO/IEC 27037:2012, propuesta por la ISO (Organización Internacional de Normalización) y la IEC (Comisión Electrotécnica Internacional), la cual proporciona procesos específicos para el manejo de evidencia digital; estos procesos corresponden a la identificación, recolección, adquisición y preservación de evidencia digital.

Los procesos indicados en la norma ISO/IEC 27037:2012, se requieren dentro de una investigación de informática forense para mantener la integridad de la evidencia digital; por ende, se considera una metodología aceptable y clara para la admisibilidad de pruebas dentro de un proceso penal o disciplinario. De igual forma

se identifica la norma NIST 8061-r2 (Guía de manejo de incidentes de seguridad informática), donde se referencia el procedimiento para la atención, manejo y toma de decisiones ante un incidente informático.

#### 8.2.1. ISO/IEC 27037:2012

La Norma ISO/IEC 27037:2012, proporciona las directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales. Igualmente, esta norma es la guía para referenciar procesos en la gestión de pruebas digitales, con el único fin de resguardar la integridad del origen y la obtención de evidencia digital derivada, donde se contemplan los siguientes principios básicos para el manejo de evidencia digital:

- Minimizar el manejo del dispositivo digital original o evidencia digital potencial.
- Tomar en cuenta cualquier cambio y documentar las acciones tomadas (en la medida en que un experto valore sobre la fiabilidad).
- Cumplir con las reglas locales para el manejo de evidencia.
- Los expertos forenses que atienden el incidente y analizan la evidencia posterior, no deben tomar acciones más allá de su competencia.

Los procesos indicados en la norma ISO/IEC 27037:2012, se encuentran vigentes y globalizan los procesos para el manejo y obtención de evidencia digital, y por tanto es un referente de gran importancia para el desarrollo de la informática forense. A continuación, se describen los procesos sugeridos en la norma ISO/IEC 27037:2012.

##### 8.2.1.1. Identificación

La evidencia digital por lo general siempre estará contenida en algún medio o dispositivo de almacenamiento de información, sin dejar de lado los medios de propagación electromagnéticos, por tanto, se deben identificar adecuadamente los medios físicos que contengan la evidencia digital potencial o probatoria de un hecho de investigación. El proceso de identificación implica la búsqueda, reconocimiento y documentación de evidencia digital potencial, sin dejar atrás la documentación de la fuente u origen de donde se obtiene. La etapa de identificación debe ser un proceso priorizado cuando exista la posibilidad de la pérdida o eliminación de los datos dependiendo el medio de contención y la volatilidad del mismo.

#### 8.2.1.2. Recolección

Una vez identificados los dispositivos electrónicos o dispositivos de almacenamiento que contienen información digital o las potenciales evidencias digitales, los especialistas deben decidir si recolectan o extraen los contenedores o medios de almacenamiento de la evidencia digital de acuerdo a las circunstancias o hechos de investigación con el fin de aislar y proteger la posible evidencia digital.

La recolección es un procedimiento dentro del manejo de evidencia digital con el fin de apartar el medio contenedor de la información de la ubicación original para ser trasladada con la debida protección y reserva a un laboratorio u otro ambiente controlado para el posterior adquisición y análisis de los datos digitales de acuerdo a los requerimientos de la investigación o hipótesis de los hechos. Los dispositivos de almacenamiento contenedores de evidencia digital pueden presentar los estados como activos o desactivados, es decir, si el equipo objeto de análisis se encuentra encendido o apagado; por tal motivo se requieren diferentes metodologías, procedimientos y herramientas, para la recolección de la evidencia digital.

De acuerdo a la metodología a desarrollar, se debe realizar una documentación adecuada donde se referencian las técnicas y herramientas para la adquisición o copias de los datos digitales. Por tal motivo es de gran importancia documentar información adicional que rodea la evidencia digital o la escena donde se encuentra ubicado el dispositivo contenedor de la misma, como por ejemplo notas de contraseñas, bases de datos, arquitectura de sistemas de información, e información relacionada con los hechos a investigar, lo anterior con el fin de aplicar la metodología más adecuada y razonable para la preservación de los datos digitales.

#### 8.2.1.3. Adquisición

El procedimiento de adquirir una evidencia o dato digital, implica producir una copia exacta verificable, la cual depende del medio de almacenamiento y estado de conservación, como por ejemplo discos duros, particiones, directorios y selección de archivos; por tal motivo es recomendable realizar una documentación sobre los métodos, herramientas aplicadas y actividades desarrolladas durante el procedimiento.

El procedimiento utilizado para obtener evidencias digitales, debe estar claramente documentado, para ser reproducible o verificable por un investigador de la defensa o contraparte del sujeto indiciado; al adquirir las posibles evidencias digitales se debe realizar la menor manipulación o intrusión que implique cambios en la evidencia digital, por tal motivo se deben utilizar herramientas adecuadas que permitan garantizar la integridad de los datos. Si en el resultado del proceso se tiene

una alteración inevitable de los datos digitales, se debe realizar la respectiva documentación.

El procedimiento de adquisición de evidencia digital producirá una copia de la evidencia digital o del dispositivo de almacenamiento, para lo cual se deben aplicar métodos de verificación con cálculos HASH tanto de la fuente original como para la copia, observando correspondencia univoca de los códigos HASH, donde la fuente original y cada copia de la evidencia digital deben producir la misma salida de códigos de la función de verificación HASH.

En circunstancias en las que el proceso de verificación no puede realizarse producto de errores de lectura propios del dispositivo de almacenamiento de información, o período de tiempo de adquisición es limitado; se debe aplicar el mejor método posible y disponible, para ser justificado y defender la postura o selección del método. Si la adquisición o imagen forense no puede ser verificada, se debe realizar la respectiva documentación y justificación.

#### 8.2.1.4. Preservación

La preservación de la evidencia digital asegura su utilidad y eficacia mediante la valoración como un elemento material probatorio dentro de la investigación; por tal motivo es importante proteger la integridad de la evidencia digital mediante el aseguramiento y conservación a lo largo de los procesos de verificación y manejo de las evidencias digitales, a partir de la identificación de los dispositivos de almacenamiento de información digital que contienen la copia o evidencia digital adquirida.

El estado ideal de las evidencias digitales no debe presentar duda de los datos que la conforman o cualquier metadato asociado con la misma como son la fecha y hora de creación, modificación, último acceso y entre otros atributos o metadatos; por lo cual el investigador deberá poder demostrar que las evidencias digitales no han sido modificadas desde el procedimiento de recolección o adquisición, de haber cambios en la información se debe proporcionar la justificación documentada sobre los cambios inevitables para la obtención de alguna evidencia digital.

La confidencialidad es uno de los requisitos más aplicados para la protección y conservación de las evidencias digitales, lo cual se presenta en el ambiente comercial y legal; por tanto, la preservación debe estar sujeta a la confidencialidad de la evidencia digital para que únicamente sea usada por las personas únicamente involucradas en el proceso, así como la utilización de las mismas en los escenarios exclusivos de la investigación desarrollada.

### 8.2.2. NIST 800-61 R2

La guía de incidentes de seguridad informática dentro de las infraestructuras tecnológicas producida por las NIST, se ha convertido en un referente de gran importancia para la gestión y tratamiento eficaz de los incidentes mediante la planificación y disposición de recursos.

A su vez permite establecer la capacidad de respuesta potencial por parte de una organización ante un incidente informático, proporcionando directrices para el manejo de incidentes particularmente para analizar los datos relacionados y determinar la respuesta apropiada, independientemente las plataformas de hardware, sistemas operativos, protocolos o aplicaciones involucradas.

De acuerdo al objeto de estudio en el presente proyecto; se observa contenido referente en el capítulo 3, ítems 3.3.2 Reunión y manejo de pruebas, e ítems 3.4.3 Retención de pruebas.

Reunión y manejo de pruebas:

- Documentar claramente las pruebas
- La evidencia debe cumplir con las leyes y regulaciones.
- Las pruebas son válidas, siempre que se demuestre la cadena de custodia relacionada en formularios u otros, donde se cierra cada registro con firma autógrafa.
- Se debe mantener un registro detallado de todas las pruebas, incluyendo las siguientes:
  - Identificar información.
  - Nombre, título y número de teléfono de cada persona que recogió o manejó la evidencia durante la investigación.
  - Fecha y hora (incluida la zona horaria) de cada caso de manejo de la evidencia.
  - Lugares donde se almacenaron las pruebas.

Retención de pruebas:

Las organizaciones deben establecer una política de cuánto tiempo se debe retener la evidencia de un incidente. Por lo cual se debe establecer el seguimiento de los factores que deben ser considerados durante la creación de la política:

- En la investigación penal. Si es posible que el atacante sea procesado, es posible que sea necesario retener pruebas hasta que se hayan completado todas las acciones legales. En algunos casos, esto puede llevar varios años, además, pruebas que parecen insignificantes ahora pueden llegar a ser más importantes en el futuro. Por ejemplo, si un atacante es capaz de utilizar el conocimiento que aplicó en un primer ataque, y a posterior realizar un segundo ataque más grave; la evidencia del primer ataque puede ser clave para explicar cómo se realizó el segundo ataque.
- Retención de datos. Las organizaciones tienen políticas de retención de datos, lo cual regula el tiempo que deben ser preservados.

## 9. IDENTIFICACIÓN DE COMUNIDADES TÉCNICO CIENTÍFICAS PARA EL MANEJO DE LA EVIDENCIA DIGITAL

Se establecen organizaciones que han desarrollado importantes documentos referentes a normas de estandarización, guías y buenas prácticas dentro del campo de la informática forense, las cuales se identifican como ISO (Organización Internacional de Normalización), la IEC (Comisión Electrotécnica Internacional), NIST (Instituto Nacional de Estándares y Tecnología) y el SWGDE (Grupo de Trabajo Científico sobre Pruebas Digitales). A continuación, se describe una breve reseña de cada una de estas organizaciones:

### 9.1. ISO / IEC

La Organización Internacional de Normalización (ISO) es un organismo internacional para el establecimiento de normas y estándares, compuesto por representantes de diversas organizaciones internacionales para la normalización. La IEC (Comisión Electrotécnica Internacional), es un organismo sin fines de lucro, no gubernamental, se reconoce como una organización que prepara y publica normas internacionales dentro de los campos eléctricos, tecnologías electrónicas y servicios conexos conocidos colectivamente como "electrotecnia". (International Organization for Standardization, 2016)

La Organización Internacional de Normalización tiene su sede principal en Suiza, desde donde viene trabajando en diferentes sectores para el desarrollo sistemas de gestión y normalización de productos y servicios, abarcando los procesos de calidad, medio ambiente, riesgos y seguridad y responsabilidad social.

Las normas ISO son documentos que especifican requerimientos para la producción de servicios y productos, avanzando sobre un sistema de gestión normalizado, garantizando calidad en los procesos operativos de las organizaciones para lograr sus objetivos.

### 9.2. NIST

El Instituto Nacional de Estándares y Tecnología (en español) fue fundado en 1901 y ahora es parte del Departamento de Comercio de los Estados Unidos. NIST es uno de los laboratorios de ciencia física más antiguos de los Estados Unidos. El Congreso estableció la agencia NIST para eliminar un gran desafío en la competitividad industrial de los Estados Unidos (THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2015).

La organización NIST trabaja sobre el desarrollo de estándares y normalización en diferentes áreas como la industrial, construcción, tecnologías de la información, telecomunicaciones, ciber-seguridad, ciencias forenses, seguridad pública y entre



otros. Se destaca de NIST que es una organización líder para la acreditación y certificación de laboratorios del sector industrial, sin dejar atrás el desarrollo de guías y procedimientos en el área de las tecnologías de la información, como por ejemplo la Guía de manejo de incidentes de seguridad informática; la cual ha sido tomada como referente por diferentes organizaciones gubernamentales para la gestión de los incidentes informáticos.

### 9.3. SWGDE

El Grupo de Trabajo Científico sobre Pruebas Digitales (en español) reúne a organizaciones activamente involucradas en el campo de la evidencia digital y multimedia para fomentar la comunicación y la cooperación, así como asegurar la calidad y consistencia dentro de la comunidad forense. (Scientific Working Group on Digital Evidence, 2015)

La organización SWGDE, se destaca por el desarrollo de guías y procedimientos para dentro del campo de la informática forense, donde se adoptan diferentes estándares desarrollados por entidades como NIST e ISO. Dentro de sus guías se hallan procedimientos definidos para cada tipo de evidencia electrónica, con el objetivo de realizar la extracción de la evidencia digital prioritaria o potencial.

## 10. ESTABLECER PROCESOS NECESARIOS PARA EL ASEGURAMIENTO, VALIDACIÓN Y CONSERVACIÓN DE LA EVIDENCIA DIGITAL

Es preciso resaltar que el objetivo del presente diseño aplica únicamente sobre el aseguramiento, validación y conservación de la evidencia digital derivada de análisis forenses informáticos. Por tal motivo se da por entendido que hace referencia a la evidencia digital derivada descubierta a través de una metodología de investigación de informática forense, el cual debe cumplir con requisitos propios del proceso, incluyendo procesos de verificación y auditoría que permitan realizar una recreación del procedimiento aplicado.

Establecido el objetivo del presente proyecto, se propone como referencia la norma ISO/IEC 27037:2012<sup>32</sup> la cual establece los procesos de identificación, recolección, adquisición y preservación, los cuales son adaptables en la obtención de la evidencia digital derivada bajo los lineamientos de la seguridad de la información, donde se establecen los siguientes procesos:

- **Identificación:** Es la forma en la cual se reconoce un objeto o persona según el sistema o producto tecnológico del cual se haga uso. Es el reconocimiento de la evidencia digital, la cual debe ser debidamente identificada mediante la documentación y referencia de metadatos. Por lo general las herramientas de software forense generan una documentación conocida como reportes automatizados que identifican los hallazgos y resultados. De lo contrario, al no contar con herramientas aplicables a un proceso de obtención de evidencia digital, se debe realizar la respectiva documentación que legitima el resultado obtenido.
- **Recolección:** Se percibe como la actividad que permite obtener de manera veraz y rápida información física o digital según la búsqueda que se está realizando. Con respecto a la recolección, se debe realizar analogía con el proceso de adquisición, pues corresponde a etapas de la obtención de la evidencia derivada de un proceso de informática forense. En el presente proceso se realiza la obtención de evidencia derivada del objeto de análisis bajo procedimientos de informática forense o similar donde se obtienen los datos que corresponden a la evidencia digital.
- **Preservación:** En este proceso la evidencia debe ser preservada para garantizar su utilidad y su originalidad, para la conformación de evidencia o elemento material probatorio dentro de una investigación, la cual puede ser verificada mediante la comprobación de pasos o secuencia para su

---

<sup>32</sup> ISO/IEC. Octubre de 2012. Guía para la identificación, recopilación, adquisición y preservación de pruebas digitales. {En línea} Disponible en: <https://www.iso.org/standard/44381.html>

obtención. Una vez realizado el procedimiento de obtención de evidencia derivada, se debe asegurar la integridad de la evidencia digital mediante la extracción o cálculo de la función HASH para cada uno de los archivos que componen el reporte o evidencia digital derivada. Cuando se tratan de múltiples registros HASH, se sugiere realizar el cálculo HASH al archivo que contienen el cálculo HASH general de los archivos, el cual debe ser referenciado en el informe de la actividad, con lo cual se asegura un procedimiento de verificación en cadena.

- **Transferencia:** obtenido el HASH, se debe realizar grabado de la evidencia digital derivada junto con los respectivos HASH en un contenedor adecuado como CD-R, DVD-R o BLU-RAY, no modificables. Si la evidencia digital derivada supera la capacidad del contenedor óptico, se deben crear estrategias como imágenes forenses de reportes dentro de contenedores susceptibles de modificación como discos duros o memorias USB.
- **Embalado y Cadena de custodia:** Se adopta el procedimiento de cadena de custodia descrito por el manual de cadena de custodia de la Fiscalía General de la Nación.

## 11. DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE EVIDENCIA DIGITAL DERIVADA DE ANÁLISIS FORENSE INFORMÁTICOS

### 11.1. OBJETIVO

Describir el procedimiento general para el aseguramiento y validación de evidencia digital obtenida de procedimientos de informática forense, el cual debe ser aplicado en los laboratorios de informática forense de la Fiscalía General de la Nación.

### 11.2. ALCANCE

Aplica a servidores de la Fiscalía General de la Nación, cuerpo técnico de investigación, grupo delitos informáticos o a quienes transitoriamente les sea asignada la función pericial para realizar procedimientos de informática forense mediante la aplicación de técnicas, herramientas de hardware y software para la obtención de evidencia digital derivada.

### 11.3. DESARROLLO

#### 11.3.1. Aseguramiento de evidencia digital

Obtenida la evidencia digital derivada del análisis forense informático, sea de dispositivos de almacenamiento de información, teléfonos celulares, información contenida en páginas web, detección y análisis de Malware, obtención de registros y auditorías; la cual por lo general corresponde a un reporte en archivos con diferentes formatos como HTML, Excel, PDF y entre otros, donde se relacionan atributos específicos para cada uno de los archivos digitales que conforman la evidencia digital hallada, junto con la transferencia o duplicado idéntico de la misma, se sugiere desarrollar el siguiente procedimiento:

- Herramientas.
  - Herramienta de software para realizar calculo HASH en algoritmos SHA1, SHA2 o MD5. Se recomienda la herramienta de software forense FTK Imager de la empresa Access Data.
  - Equipo de cómputo de alto rendimiento con sistema operativo compatible y unidades de grabación para discos ópticos para la transferencia de datos.

- Software para grabación de datos a disco óptico (CD, DVD, Blu Ray) que permita verificación posterior a la grabación.
- Unidades de almacenamiento de información tipo discos ópticos (CD, DVD, Blu Ray).
- Unidades de almacenamiento de información tipo discos duros.

11.3.1.1. Procedimiento para cuando es posible realizar grabación de datos en unidades de almacenamiento de información tipo discos ópticos (CD R, DVD R, Blu Ray R).

- Ubicar directorio de reporte.

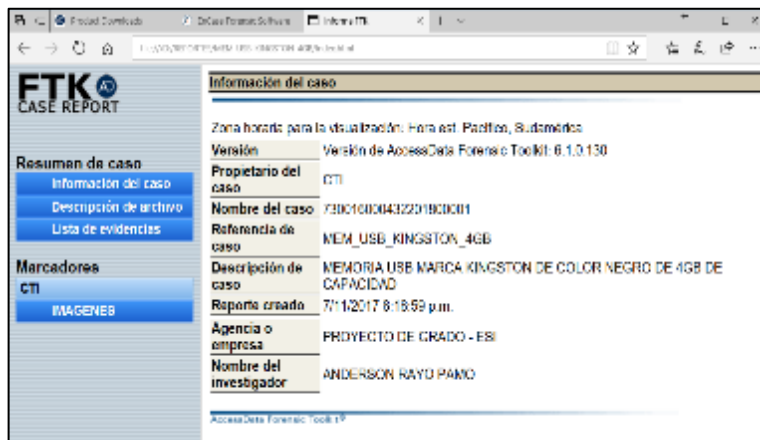
Ubicación reporte de herramienta forense en directorio (equipo de cómputo) donde se ha realizado la transferencia inicial.

Figura 13. Impresión de pantalla para directorio de reportes.



Fuente: Propia.

Figura 14. Impresión de contenido de reporte FTK AccessData.

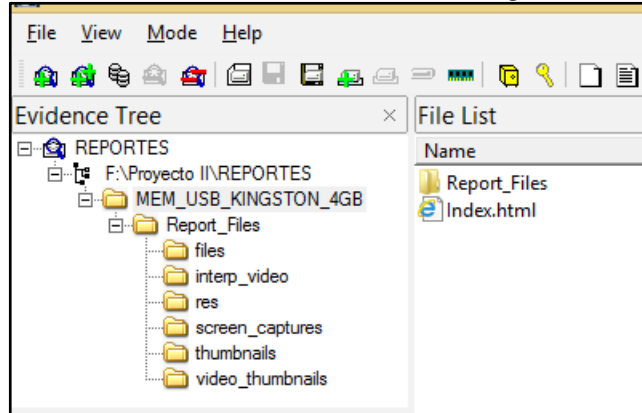


Fuente: Propia.

- Carga de directorio.

El directorio es cargado en modo contenido de carpeta a herramienta de software forense FTK Imager.

Figura 15. Carga de directorio a herramienta FTK Imager.

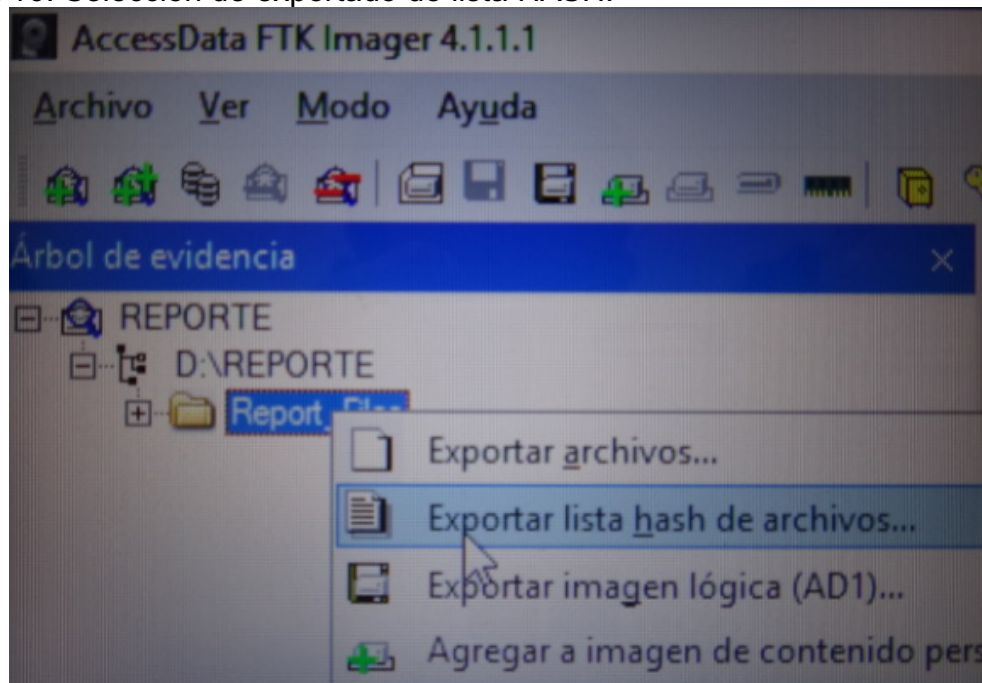


Fuente: Propia.

- Extracción de la lista HASH.

En el directorio raíz cargado en la herramienta de software forense FTK Imager y proceder a realizar extracción de lista HASH de archivos para todo el contenido del directorio.

Figura 16. Selección de exportado de lista HASH.

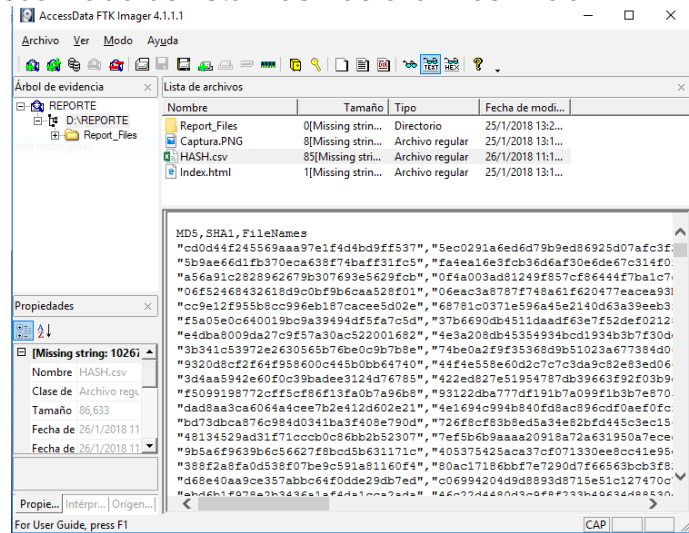


Fuente: Propia

- Cargar la ubicación o directorio de la lista HASH de archivo obtenida.

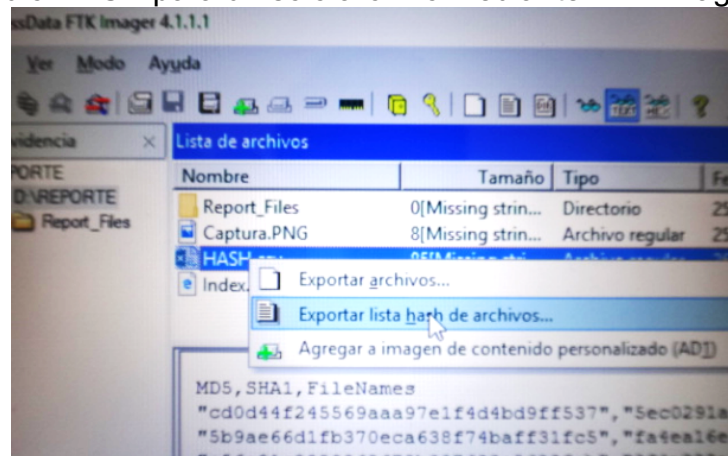
Si el resultado en la lista HASH de archivos contiene gran cantidad de registros imposibles de imprimir o referenciar en informe pericial, se procede a cargar la ubicación o directorio de la lista HASH de archivo obtenida en el proceso previo y se realiza cálculo HASH para el mencionado archivo, de lo cual se obtiene un solo registro de cálculo HASH que puede ser relacionado en el informe pericial garantizando una cadena de verificación y validación.

Figura 17. Pre visualizado de lista Hash de archivos inicial.



Fuente: Propia.

Figura 18. Cálculo HASH para un solo archivo mediante FTK Imager.



Fuente: Propia.

Figura 19. Pre visualizado de HASH calculado a LISTA HASH DE ARCHIVOS.

Nombre	Tamaño	Tipo	Fecha de modi...
Report_Files	0[Missing strin...	Directorio	25/1/2018 13:2...
Captura.PNG	8[Missing strin...	Archivo regular	25/1/2018 13:1...
HASH DE HASH.csv	1[Missing strin...	Archivo regular	27/3/2018 16:4...
HASH.csv	85[Missing stri...	Archivo regular	26/1/2018 11:1...
Index.html	1[Missing strin...	Archivo regular	25/1/2018 13:1...

MDS, SHA1, Nombres de archivos  
 "6749db714cd8a844852d30c6f7f29e5f", "04e98855427b598cf89d0b37a22fcd452c77076", "REPORTE\I

Fuente: Propia.

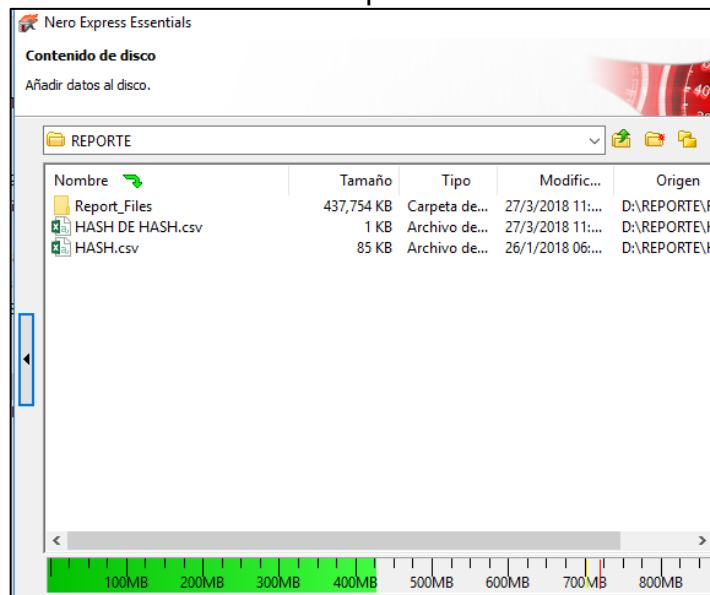
De acuerdo a la figura 19; a continuación, se relaciona en forma de ejemplo el cálculo HASH para el archivo identificado como LISTA HASH DE ARCHIVOS; el cual corresponde a los siguientes valores hexadecimales en algoritmo MD5 y SHA1, así:

MD5, SHA1, Nombres de archivos  
 "6749db714cd8a844852d30c6f7f29e5f", "04e98855427b598cf89d0b37a22fcd452c77076", "REPORTE\D:\REPORTE\HASH.csv"

- Grabación a disco compacto óptico.

Obtenidos los reportes con los respectivos cálculos HASH, se procede a realizar grabación a disco compacto óptico (CD R, DVD R, Blu Ray R), mediante software que permita la verificación posterior, asegurando la transferencia de datos y cierre de disco sin permiso de grabación de más datos o multi-sección.

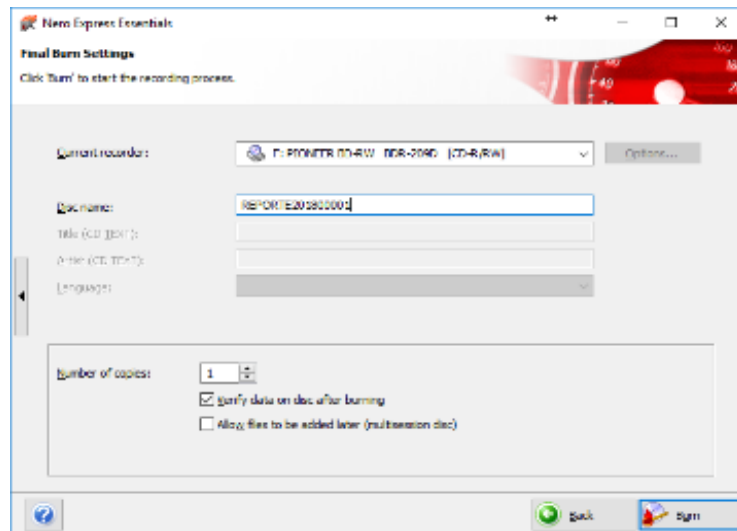
Figura 20. Grabado de datos a disco compacto mediante Software Nero.



Fuente: Propia.



Figura 21. Selección de verificación posterior al grabado y desmarque de multi - Sección en software Nero para grabado de disco.



Fuente: Propia.

- Rotulado de disco compacto.

Proceso en el cual se coloca una identificación que permite referenciar el origen de la evidencia digital derivada.

Figura 22. Referencia para rotulado de disco compacto.



Fuente: Propia.

- Documentación del disco compacto.

Realizar la documentación del disco compacto previo al embalado en contenedor adecuado mediante imagen fotográfica la cual debe ser referenciada en informe pericial.

A continuación, se relaciona descripción realizada en el rótulo para el ejemplo que se viene documentando en el presente trabajo, el cual corresponde a: “UN DISCO COMPACTO TIPO DC R MARCA IMATION COLOR BLANCO CON NUMERO SERIAL EN ANILLO 99QWERTY01, ROTULADO COMO 730016000432201800001 REPORTE FTK MEM\_USB\_KINGSTON\_4GB. ELEMENTO EMBALADO EN BOLSA ANTI ESTÁTICA Y RÓTULADO; AL CUAL SE LE DA INICIO DE CADENA DE CUSTODIA.”

- Embalado y rotulado.

De acuerdo a procedimiento de cadena de custodia de la Fiscalía General para los discos compactos el contenedor o contenedores deben garantizar la protección a golpes, humedad y resistencia a deformaciones por presión de otros elementos sólidos. Aunque los discos compactos no son susceptibles a descargas eléctricas o electromagnéticas se sugiere usar como contenedor final bolsa anti estática.

Figura 23. Uso de cubierta sólida que permite la protección del disco compacto.



Fuente: Propia.

Figura 24. Uso de bolsa anti estática.



Fuente: Propia

- Documentación posterior del embalado y rotulado.

Realizada mediante imagen fotográfica, la cual debe ser referenciada en informe pericial. En el rotulo se debe describir la cantidad de elementos, marca, número serial, color, y entre otros que permitan individualizar el elemento; además se debe relacionar el contenedor final.

Figura 25. Ejemplo del contenido en rótulo.

ROTULO DE ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FÍSICA - FPJ-07.																														
Versión3 - Resolución 0-2369 DE Julio 11 de 2016																														
1. CODIGO UNICO DE CASO					2. FECHA Y HORA DE RECOLECCION																									
7	3	0	0	1	6	0	0	0	4	3	2	2	0	1	8	0	0	0	0	1	1	8	0	1	0	1	1	2	0	0
DPTO		MUNICIPIO		ENTIDAD		UNIDAD		AÑO		CONSECUTIVO																				
3. HALLAZGO										4. SITIO O LUGAR DE HALLAZGO DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FÍSICA																				
NUMERO DEL EMP Y EF		DIRECCION:		Transversal 1 sur No. 47 02, Ibagué. Fiscalía General de la Nación. Grupo Delitos informáticos.										NOMBRES Y APELLIDOS DE LA PERSONA A QUIEN SE LE ENCONTRO EL EMP O EF																
1														NA																
CANTIDAD		UBICACION:		REPORTE FTK A MEMORIA USB MARCA KINGSTON DE 4 GB SERIAL NO. 0000001.										NA																
1														NA																
5. DESCRIPCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FÍSICA																														
UN DISCO COMPACTO TIPO DC R MARCA IMATION COLOR BLANCO CON NUMERO SERIAL EN ANILLO 99QWERTY01, ROTULADO COMO 730016000432201800001 REPORTE FTK MEM_USB_KINGSTON_4GB. ELEMENTO EMBALADO EN BOLSA ANTI ESTÁTICA Y ROTULADO; AL CUAL SE LE DA INICIO DE CADENA DE CUSTODIA.																														
6. ROTULO DILIGENCIADO POR:																														
NOMBRES Y APELLIDOS					CEDULA DE CIUDADANIA					ENTIDAD					CARGO					FIRMA										
ANDERSON RAYO PAMO					79111111					FISCALIA GENERAL DE LA NACION					TECNICO INVESTIGADOR I															

Fuente: Propia.

Figura 26. Ejemplo de contenido en cadena de custodia.

H		R		E		NOMBRES Y APELLIDOS		CEDULA DE CIUDADANIA		ENTIDAD		FIRMA	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				ANDERSON RAYO PAMO		79111111		FISCALIA GENERAL DE LA NACION			

A	A	M	M	D	D	HORA	NOMBRES Y APELLIDOS DE QUIEN RECIBE EL EMP Y EF	CEDULA DE CIUDADANIA	ENTIDAD	CALIDAD EN LA QUE ACTUA C (custodio) P (perito)	PROPOSITO DEL TRASLADO (Almacenamiento, Análisis, Presentación Audiencia, Consulta, Disposición)	ESTADO EN QUE SE RECIBE EL EMBALAJE O CONTENEDOR DEL EMP Y EF	FIRMA
1	8	0	1	0	1	12:15	ANDERSON RAYO PA	79111111	FGN-CTI	X	ALMACENAMIENTO	BOLSA ANTESTÁTICA SELLADA	

6. PARA SER DILIGENCIADO POR EL TECNICO EN PRUEBA DE IDENTIFICACIÓN PRELIMINAR HOMOLOGADA "RIPH"	
¿ PRACTICO PRUEBA PRELIMINAR ?	
SI	NO
CANTIDAD DE MUESTRAS TOMADAS	
Número del Rótulo(s)	

7) OBSERVACIONES (\*)

---



---



---



---

Fuente: Propia.

Figura 27. Ejemplo de contenido en cadena de custodia.

**REGISTRO DE CADENA DE CUSTODIA**  
Versión 3 - Resolución 0-2389 DE Julio 11 de 2018

1. CODIGO UNICO DE CASO 2. HISTORIA CLINICA (\*)

7 3 0 0 1 6 0 0 0 4 3 2 2 0 1 8 0 0 0 0 1	
<small>DPTO MUNICIPIO ENTIDAD UNIDAD AÑO CONSECUTIVO</small>	

3. DOCUMENTACIÓN DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

H	R	E	NOMBRES Y APELLIDOS	CEDULA DE CIUDADANIA	ENTIDAD	FIRMA
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ANDERSON RAYO PAMO	79111111	FISCALIA GENERAL DE LA NACION	

4. DESCRIPCIÓN DEL ELEMENTO(S) MATERIAL(ES) DE PRUEBA Y EVIDENCIA FISICA

UN DISCO COMPACTO TIPO DC R MARCA IMATION COLOR BLANCO CON NUMERO SERIAL EN ANILLO 99QWERTY01, ROTULADO COMO 730016000432201800001 REPORTE FTK MEM\_USB\_KINGSTON\_4GB. ELEMENTO EMBALADO EN BOLSA ANTI ESTÁTICA Y ROTULADO; AL CUAL SE LE DA INICIO DE CADENA DE CUSTODIA.

(\*) Para ser diligenciado exclusivamente por la Bodega General de evidencias de la Fiscalía General de la Nación con la posición que le correspondió a la evidencia al interior de la bodega.  
H Marque con una X si corresponde a quien HALLÓ el elemento materia de prueba o evidencia física.  
R Marque con una X si corresponde a quien RECOLECTO el elemento materia de prueba o evidencia física.  
E Marque con una X si corresponde a quien EMBALÓ el elemento materia de prueba o evidencia física.  
Se puede marcar una o varias opciones para un mismo nombre, según sea el caso

CONVENCIONES

Fuente: Propia.

Figura 28. Imagen de referencia para embalado y rotulado final del elemento.



Fuente: Propia.

- Disposición del elemento.

Finalizados los procedimientos de documentación y recolección de elementos, se deben iniciar registros en cadena de custodia, donde se detalla la disposición o traslado del elemento con destino al almacén o unidad de análisis de información.

#### 11.3.1.2. Procedimiento para discos duros.

Es el procedimiento para cuando no es posible realizar grabación de datos en disco compacto por capacidad de almacenamiento superada para dichos dispositivos; se sugiere almacenar evidencia digital en discos duros a través de imagen forense en paquetes de datos reconocidos por herramientas de software forense; para el caso aplicado se sugiere la herramienta de software FTK Imager del paquete de herramientas de FTK Access Data; a continuación, se describe el procedimiento.

- Ubicación de directorio.

Ubicar reporte de herramienta forense en directorio donde se ha realizado la transferencia inicial.

Figura 29. Directorio de reporte de evidencia digital.

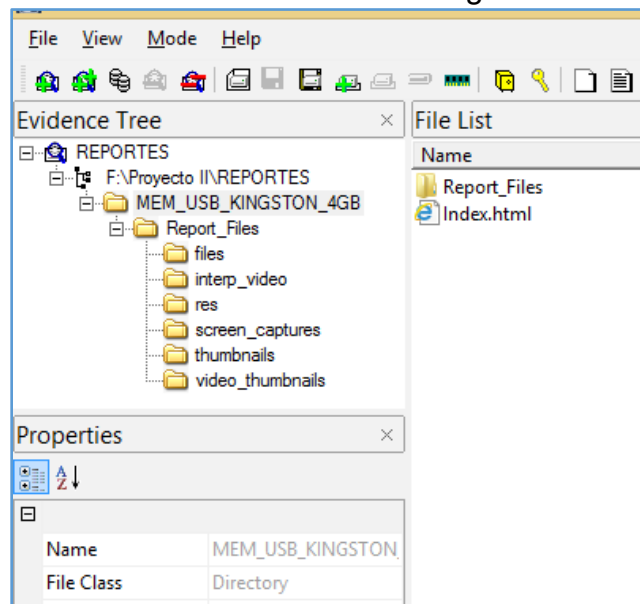


Fuente: Propia.

- Carga de directorio a herramienta.

Una vez ubicado el directorio, se realiza carga de directorio en modo contenido de carpeta a herramienta de software forense FTK Imager.

Figura 30. Carga de directorio a herramienta FTK Imager.



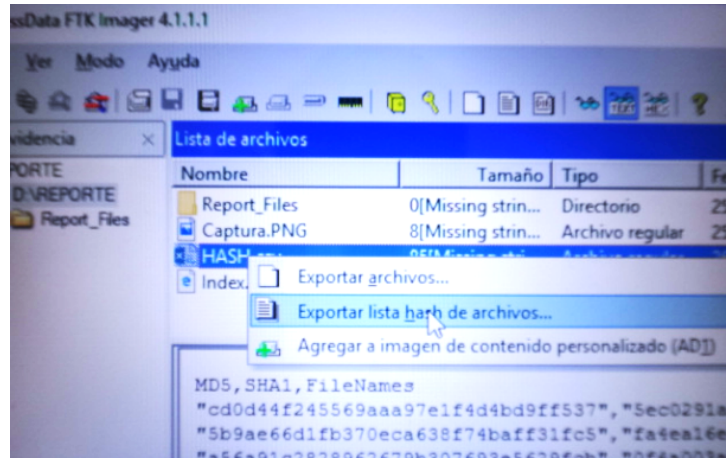
Fuente: Propia.

- Exportado de Lista HASH de directorio.

En el directorio raíz cargado en la herramienta de software forense FTK Imager, proceder a realizar extracción de lista HASH de archivos para todo el contenido del directorio.



Figura 31. Selección de exportado de lista HASH de archivos.

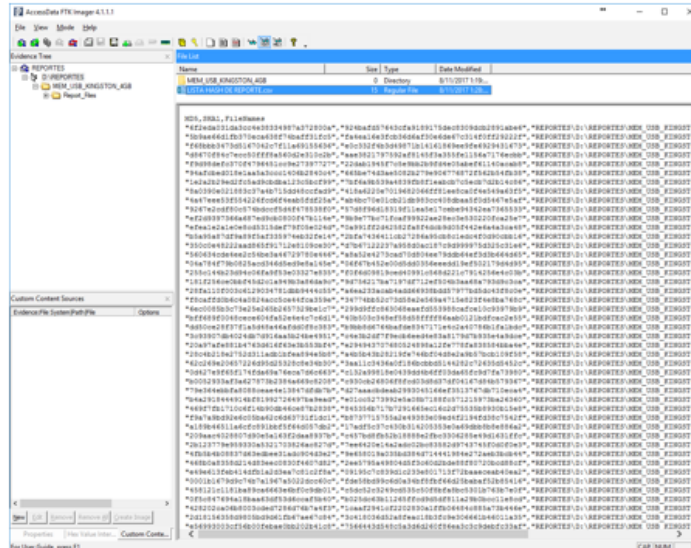


Fuente: Propia.

- Cálculo HASH de lista HAHS inicial.

Si el resultado en la lista HASH de archivos contiene gran cantidad de registros imposibles de imprimir o referenciar en informe pericial; se procede a cargar la ubicación o directorio de la lista HASH de archivos obtenida en el proceso previo y se realiza cálculo HASH para el mencionado archivo; de lo cual se obtiene un solo registro de cálculo HASH que puede ser relacionado en el informe pericial garantizando una cadena de verificación y validación.

Figura 32. Pre visualizado de LISTA HASH DE ARCHIVOS INICIAL.

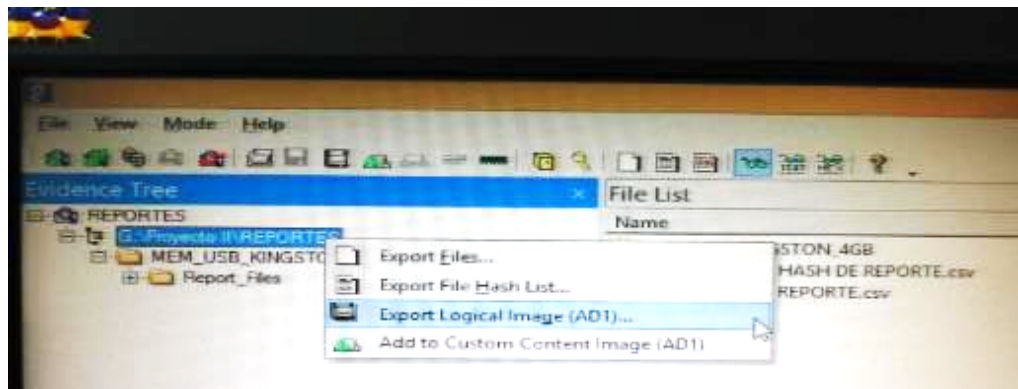


Fuente: Propia.

- Creación de imagen forense para los datos obtenidos.

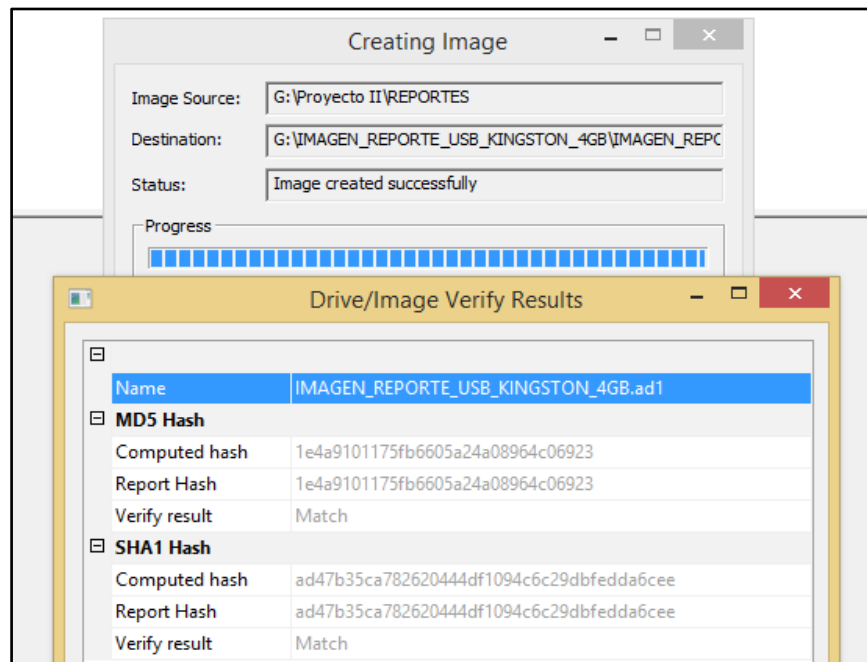
Obtenidos los reportes con los respectivos cálculos HASH, se ubican en un solo directorio contenedor y se procede a realizar carga del directorio a la herramienta de software forense FTK Imager; donde se procede a realizar imagen forense bit a bit del directorio, obteniendo una imagen forense en formato AD1, con la respectiva verificación o comprobación de HASH, el cual debe ser referenciado en el informe pericial.

Figura 33. Creación de paquete de imagen. FTK Imager formato AD1.



Fuente: Propia.

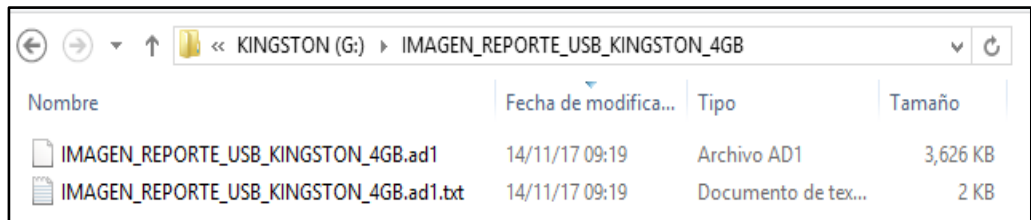
Figura 34. Reporte creación imagen forense de directorio con herramienta FTK Imager.



Fuente: Propia



Figura 35. Paquetes de datos resultados de imagen AD1.

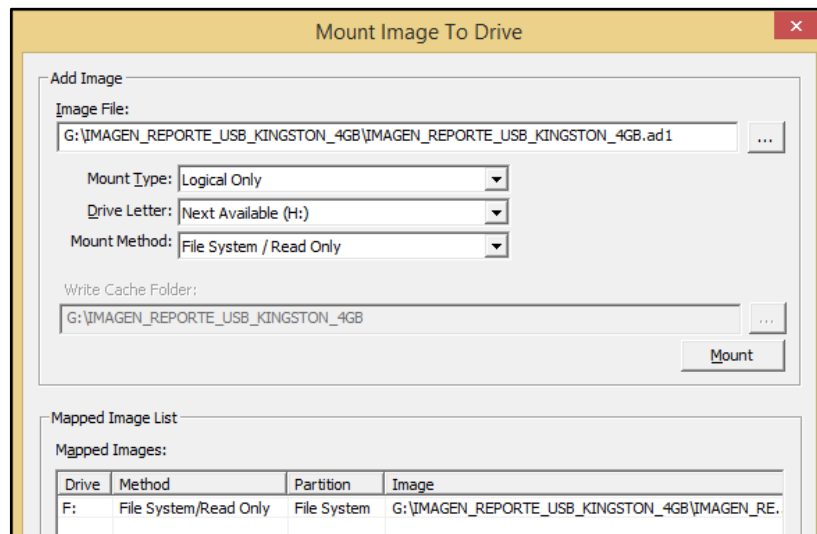


Fuente: Propia.

- Transferencia de imagen a disco duro.

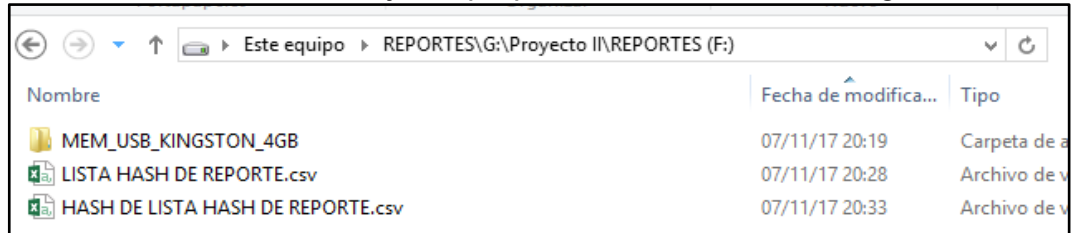
Una vez obtenida la imagen forense en formato AD1, se realiza transferencia a disco duro contenedor de evidencia digital derivada final, mediante la misma herramienta FTK Imager, usando la función exportado o creación de imagen forense a partir de un archivo de imagen. Adicional a lo anterior se realiza transferencia de la herramienta de software forense FTK Imager en versión portable a fin facilitar el cargue o emulación de la imagen forense para el respectivo análisis de la información de contexto, lo cual protege de modificaciones o eliminación de información por parte de los analistas de información. Se recomienda como buena práctica durante el análisis de la información, realizar copia de trabajo a fin de no trabajar directamente en la evidencia digital obtenida.

Figura 36. Montaje de paquete de imagen AD1 con FTK Imager.



Fuente: Propia.

Figura 37. Resultado de montaje de paquete AD1, en la unidad lógica F.



Fuente: Propia.

- Identificación de disco duro.

La identificación del dispositivo de almacenamiento se debe realizar de acuerdo a etiquetas propias de fábrica; como se evidencia en las siguientes imágenes de referencia.

Figura 38. Imagen de referencia para disco duro portable.



Fuente: Propia.

Figura 39. Etiqueta de identificación de disco duro portable.



Fuente: Propia.

- Documentación previa a embalada de disco.

Documentación del disco duro previo del embalado en contenedor adecuado, mediante imagen fotográfica la cual debe ser referenciada en informe pericial. La documentación del disco duro debe describir la cantidad de elementos, marca, número serial, capacidad y entre otros; que permitan individualizar los elementos. Además, se debe relacionar el contenedor final.

A continuación, se relaciona descripción realizada en el rótulo para el ejemplo que se viene documentando en el presente trabajo, el cual corresponde a: “UN DISCO DURO PORTABLE MARCA SEAGATE, SERIAL NA4C7TP4 DE 1.5 TB, CONTIENE IMAGEN FORENSE AD1, DE REPORTE FTK PARA LA MEMORIA USB MARCA KINGSTON DE 4 GB SERIAL NO. 0000001. ELEMENTO EMBALADO EN BOLSA ANTI ESTÁTICA BURBUJA, ROTULADO; AL CUAL SE LE DA INICIO DE CADENA DE CUSTODIA.”

- Embalado y rotulado.

El Embalado y rotulado para discos duros, se realiza de acuerdo a procedimiento de cadena de custodia. Se recomienda usar contenedor adecuado que proteja de golpes, deformaciones y descargas eléctricas. A continuación, se relacionan imágenes de referencia para el contenido de los campos del rótulo y cadena de custodia.

Figura 40. Impresión de pantalla imagen de rotulo para disco duro portable

ROTULO DE ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA - FPJ-07.																																		
Versión3 - Resolución 0-2369 DE Julio 11 de 2016																																		
1. CODIGO UNICO DE CASO										2. FECHA Y HORA DE RECOLECCION																								
7	3	0	0	1	6	0	0	0	4	3	2	2	0	1	8	0	0	0	0	1	1	8	0	1	0	1	1	2	0	0				
DPTO		MUNICIPIO		ENTIDAD		UNIDAD				AÑO		CONSECUTIVO																						
3. HALLAZGO													4. SITIO O LUGAR DE HALLAZGO DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA																					
NUMERO DEL EMP Y EF		DIRECCION: <b>Transversal 1 sur No. 47 02, Ibagué. Fiscalía General de la Nación. Grupo Delitos informáticos.</b>											NOMBRES Y APELLIDOS DE LA PERSONA A QUIEN SE LE ENCONTRÓ EL EMP O EF																					
2													NA																					
CANTIDAD		UBICACION: <b>REPORTE FTK A MEMORIA USB MARCA KINGSTON DE 4 GB SERIAL NO. 0000001.</b>											NA																					
1													NA																					
5. DESCRIPCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA																																		
<b>UN DISCO DURO PORTABLE MARCA SEAGATE, SERIAL NA4C7TP4 DE 1.5 TB, CONTIENE IMAGEN FORENSE AD1, DE REPORTE FTK PARA LA MEMORIA USB MARCA KINGSTON DE 4 GB SERIAL NO. 0000001. ELEMENTO EMBALADO EN BOLSA ANTI ESTÁTICA BURBUJA, ROTULADO; AL CUAL SE LE DA INICIO DE CADENA DE CUSTODIA.</b>																																		
6. ROTULO DILIGENCIADO POR:																																		
NOMBRES Y APELLIDOS							CEDULA DE CIUDADANIA							ENTIDAD							CARGO							FIRMA						
ANDERSON RAYO PAMO							79111111							FISCALIA GENERAL DE LA NACION							TECNICO INVESTIGADOR I													

Fuente: Propia.

Figura 41. Impresión de pantalla de cadena de custodia para disco duro portable.

H		R		E		NOMBRES Y APELLIDOS		CEDULA DE CIUDADANIA		ENTIDAD		FIRMA	
X	X	X	X	X	X	ANDERSON RAYO PAMO		79111111		FISCALIA GENERAL DE LA NACION			

3. DOCUMENTACIÓN DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

4. DESCRIPCIÓN DEL ELEMENTO(S) MATERIAL(ES) DE PRUEBA Y EVIDENCIA FISICA

UN DISCO DURO PORTABLE MARCA SEAGATE, SERIAL NA4C7TP4 DE 1.5 TB, CONTIENE IMAGEN FORENSE AD1, DE REPORTE FTK PARA LA MEMORIA USB MARCA KINGSTON DE 4 GB SERIAL NO. 0000001. ELEMENTO EMBALADO EN BOLSA ANTI ESTÁTICA BURBUJA, ROTULADO; AL CUAL SE LE DA INICIO DE CADENA DE CUSTODIA.

CONVENIONES

(\*) Para ser diligenciado exclusivamente por la Bodega General de evidencias de la Fiscalía General de la Nación con la posición que le correspondió a la evidencia al interior de la bodega.  
 H Marque con una X si corresponde a quien HALLO el elemento materia de prueba o evidencia física.  
 R Marque con una X si corresponde a quien RECOLECTO el elemento materia de prueba o evidencia física.  
 E Marque con una X si corresponde a quien EMBALÓ el elemento materia de prueba o evidencia física.  
 Se puede marcar una o varias opciones para un mismo nombre, según sea el caso.

Fuente: Propia.

Figura 42. Impresión de pantalla complemento de cadena de custodia.

FECHA		HORA	NOMBRES Y APELLIDOS DE QUIEN RECIBE EL EMPLEO	CEDULA DE CIUDADANIA	ENTIDAD	CALIDAD EN LA QUE ACTUA		PROPÓSITO DEL TRASLADO (Almacenamiento, Análisis, Fijación, Audición, Contesta, Disposición)	CIUDADANÍA DE LA FISCALIA GENERAL O COORDINADOR DEL MAFPP	FIRMA			
A	B					M	D				D	H	M
1	8	3	1	0	2	00	ANDERSON RAYO PAMO	79111111	FCN-CT	X	AL ALMACENAMIENTO	FCN-CT	

5. PARA SER DILIGENCIADO POR EL EMPLEO DEL EMPLEO DE IDENTIFICACIÓN PRELIMINAR (MONITOREO DE LA CADENA DE CUSTODIA)

¿PRÁCTICO PRELIMINAR POR BURBUJA?

SI NO

CONTENIDO DE LAS PRUEBAS TOMADAS

(Número de Hojas)

NOTAS:

- 1) SIEMPRE ENTREGAR AL MENSAJERO LA CADENA DE CUSTODIA.
- 2) EL REGISTRO DE CADENA DE CUSTODIA SIEMPRE DEBE ACOMPAÑAR AL ELEMENTO MATERIAL DE PRUEBA Y EVIDENCIA FISICA.
- 3) SI ESTA HOJA NO ALCANZA PARA DILIGENCIAR LOS REGISTROS DE CONTINUIDAD DE CADENA DE CUSTODIA, SE PUEDEN UTILIZAR TANTAS HOJAS ADICIONALES SEAN NECESARIAS.
- 4) CUANDO SE RECIBEN OBSERVACIONES DE CÓMO OCORRIÓ EL MONITORIO, SE DEBE REGISTRAR EL NOMBRE DE QUIEN LA REALIZA Y LA FECHA.

Fuente: Propia.

- Documentación posterior del embalado y rotulado.

Se realiza documentación mediante imagen fotográfica, la cual debe ser referenciada en informe pericial; con lo cual se permite referenciar el estado del elemento cuando se finalizan los procesos y documentación forense.

Figura 43. Embalado y rotulado, bolsa anti estática burbuja.



Fuente: Propia.

- Disposición final del elemento.

La disposición del elemento debe ser registrada en la cadena de custodia, donde se referencia el lugar de traslado, ya sea con destino al almacén de evidencias o unidad de análisis de información.

Tabla 2. Diagrama de Flujo del procedimiento para el aseguramiento de evidencia digital.


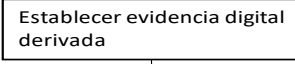
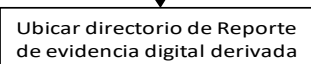

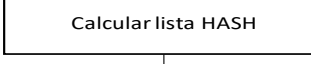
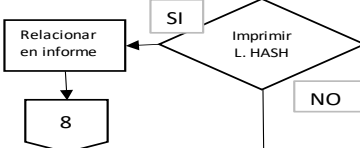
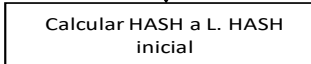
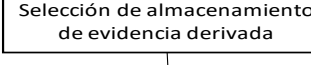
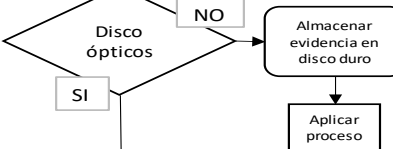
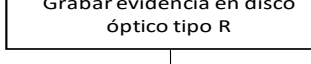
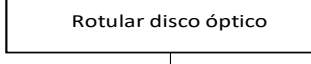
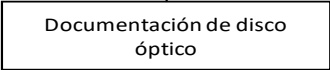
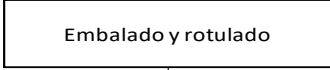
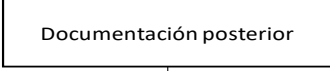
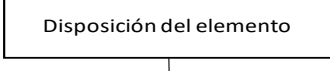

No.	ACTIVIDAD	RESPONSABLE	OBSERVACIONES
1			El proceso de aseguramiento de evidencia se inicia con la identificación y transferencia de evidencia digital, a partir de un proceso forense.
2		Perito forense	Se establece la evidencia derivada mediante procedimientos y herramientas forenses, la cual es generada mediante reportes o duplicado.
3		Perito forense	Establecer ubicación de reporte de evidencia derivada.
4		Perito forense	Aplicación de herramienta de software forense para el cálculo de evidencia digital.
5		Perito forense	Se inicia proceso de cálculo HASH, mediante la opción EXTRAER LISTA HASH.
6		Perito forense	La lista HASH de archivos contiene el cálculo HASH, nombre y ruta de cada uno de los archivos que componen la evidencia digital derivada.
7		Perito forense	Calcular el HASH a la lista HASH inicial es un proceso de verificación en cadena para el aseguramiento de integridad de archivos digitales
8		Perito forense	Los dispositivos de gran capacidad de almacenamiento objeto de análisis generan diferentes tamaños lógicos de información.
9		Perito forense	La preservación de la evidencia digital se recomienda en discos ópticos tipo R. Si la capacidad es superada necesariamente se debe realizar en discos duros, Procedimiento relacionado en el siguiente diagrama.
10		Perito forense	Transferencia de la evidencia digital con el respectivo cálculo HASH.
11		Perito forense	Identificación del contenedor de evidencia digital.

Tabla2. Diagrama de Flujo del procedimiento para el aseguramiento de evidencia digital. (Continuación)

12		Perito forense	Establecer las características e individualización del medio de almacenamiento para referencia en informe.
13		Perito forense	Contenedor final para el aseguramiento del medio de almacenamiento
14		Perito forense	Información de referencia para relacionar en el informe.
15		Perito forense	Información de referencia para indicar el destino de la evidencia.
16			

Autor: propio

Tabla 3. Diagrama de flujo para almacenamiento en disco duro mediante la creación de imagen forense AD1, con herramienta de software forense FTK Imager.


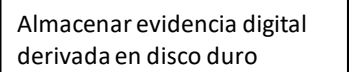
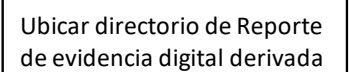

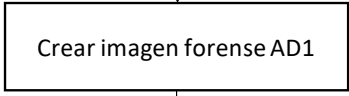
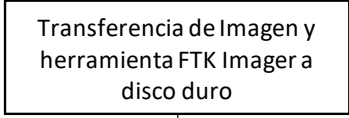
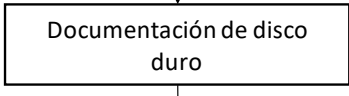
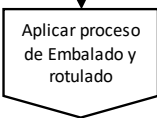
No.	ACTIVIDAD	RESPONSABLE	OBSERVACIONES
1			
2			Es la opción disponible cuando no es posible resguardar la evidencia digital en discos ópticos.
3		Perito forense	Establecer ubicación de reporte de evidencia derivada

Tabla 3. Diagrama de flujo para almacenamiento en disco duro mediante la creación de imagen forense AD1, con herramienta de software forense FTK Imager. (Continuación)

4		Perito forense	Aplicación de herramienta de software forense FTK Imager
5		Perito forense	Ejecución de creación de imagen forense del directorio donde se ubica la evidencia derivada mediante FTK Imager.
6		Perito forense	Se indica como transferencia puesto que lo mas recomendable es aplicar la opción de exportado mediante FTK Imager.
7		Perito forense	Establecer las características e individualización del medio de almacenamiento para referencia en informe.
8			

Autor: propio

Tabla 4. Diagrama de flujo para montaje de imagen forense AD1 a directorio o drive en modo protegido de solo lectura.


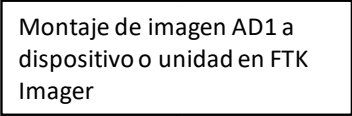
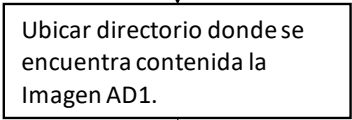
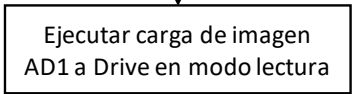
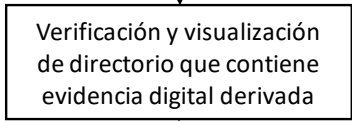
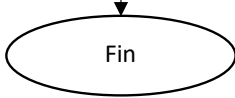
No.	ACTIVIDAD	RESPONSABLE	OBSERVACIONES
1			
2		Perito forense	Una vez ejecutado FTK Imager, seleccionamos "Mount Image to drive".



Tabla 4. Diagrama de flujo para montaje de imagen forense AD1 a directorio o drive en modo protegido de solo lectura. (Continuación)

3		Perito forense	Selección de imagen forense AD1, para la ejecución Mount Image.
4		Perito forense	Ejecución de Mount Image con protección para evitar la modificación de la información digital.
5		Perito forense	Acceso a la información de reporte o evidencia digital derivada en modo protegido.
6		Perito forense	Se indica como transferencia puesto que lo mas recomendable es aplicar la opción de exportado mediante FTK Imager.

Autor: propio

### 11.3.2. Validación de evidencia digital derivada de análisis informáticos.

Para el siguiente procedimiento se hace referencia a que la evidencia digital producto de análisis forense ha surtido el proceso de aseguramiento de evidencia digital previamente descrito. Por tal motivo el proceso de validación corresponde a la verificación de puntos de control, a fin de identificar si se guarda la respectiva integridad de la información digital, a la cual deben estar sujetos los correspondientes reportes de herramientas de software forense, junto con la evidencia digital transferida; por tanto, se sugiere realizar los siguientes puntos de control (P. C.):

- P. C. 1. Establecer si elemento cuenta con el respectivo embalaje, rotulo y cadena de custodia, de acuerdo a lo relacionado en el respectivo informe pericial; de no haber correspondencia se debe identificar trazabilidad mediante cadena de custodia en la cual se registran los cambios para el elemento.
- P. C. 2. El dispositivo de almacenamiento, sea disco compacto o disco duro, debe corresponder a la identificación en rótulo o etiquetas de identificación.

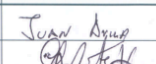


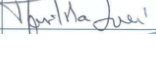


- P. C. 3. El dispositivo de almacenamiento de información se encuentra en correcto estado de funcionamiento y es accesible la información contenida de acuerdo informe pericial.
- P. C. 4. Como proceso de validación se sugiere realizar verificaciones HASH, los cuales deben coincidir exactamente para cada uno de los archivos digitales contenidos como evidencia digital transferida, así como para los archivos que conforman el reporte de la herramienta de software forense.
- P. C. 5. De hallarse un cálculo HASH para una lista HASH de archivos, se debe realizar verificación mediante la comprobación HASH para la lista HASH de archivos, con respecto a los códigos HASH de archivos relacionados en el informe pericial. Se realiza este procedimiento ya que la lista HASH de archivos es el registro que contiene el cálculo HASH para todos los archivos contenidos en el reporte de la herramienta de software forense. De ser necesario realizar comprobación o cálculo HASH para cada uno de los archivos y compararla con la lista HASH de archivos actual.

## 12. SOCIALIZACIÓN DEL PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE EVIDENCIA DIGITAL DERIVADA DE ANÁLISIS FORENSE INFORMÁTICO.

Las socializaciones de los resultados son comunicados constantemente durante el diseño del procedimiento al Coordinador del Grupo Delitos Informáticos de la policía judicial de la Fiscalía General de la Nación seccional Tolima, Ingeniero Juan Bautista Ávila Flórez, quien toma parte activa sobre la orientación relacionada con las herramientas de hardware y software forense.

Además de lo anterior se procedió a realizar exposición y práctica del procedimiento diseñado en la fecha 21 de marzo de 2018, en las instalaciones de las oficinas del Grupo Delitos Informáticos de la Seccional Tolima, donde el auditorio receptor son los peritos de informática forense que integran el personal de la mencionada oficina; de lo cual se tuvo una percepción positiva, puesto que se enriquecía el conocimiento con algunas técnicas o procedimientos desconocidos por parte de los investigadores de informática forense. De lo anterior se tiene como evidencia el acta de asistencia para la reunión de socialización de la cual se relaciona a continuación impresión de pantalla, así:

Figura 45. Impresión de pantalla para control de asistencia.

FISCALÍA GENERAL DE LA NACIÓN		PROCESO GESTIÓN INTEGRAL				FORMATO CONTROL DE ASISTENCIA		<small>Código: FISC-14.3-F-05</small> <small>Versión: 02</small> <small>Página: 1 de 1</small>		
NOMBRE DEL EVENTO: SOCIALIZACION DE PROYECTO DE GRADO APLICADO POR SERVIDOR Y PARTICULAR EXTERNO			DEPENDENCIA: DELITOS INFORMATICOS	PROGRAMA: N/A	CIUDAD: IBAGUE	FECHA : 27/03/2018				
SERVIDOR RESPONSABLE: JUAN BAUTISTA AVILA FLOREZ			LUGAR: OFICINA GRUPO DELITOS INFORMATICOS	HORA INICIO: 08:00	HORA FINALIZACIÓN: 09:30					
ACTIVIDADES DESARROLLADAS										
SOCIALIZACION DE DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE LA EVIDENCIA DIGITAL DERIVADA DEL ANÁLISIS FORENSE, APLICADO EN EL LABORATORIO DE INFORMÁTICA FORENSE FISCALÍA GENERAL DE LA NACIÓN, SECCIONAL TOLIMA										
No.	NOMBRES Y APELLIDOS	DOCUMENTO DE IDENTIDAD	CARGO	ÁREA			DEPENDENCIA / ENTIDAD	TELÉFONO / EXTENSIÓN	CORREO ELECTRÓNICO O DIRECCIÓN	FIRMA
				FISCALÍA	POLICIA	OTRO				
1	JUAN BAUTISTA AVILA FLOREZ	93374075	PROFESIONAL INVESTIGADOR III - COORDINADOR	X			DELITOS INFORMATICOS / CTI	2708102 / 231	juan.avila@fiscalia.gov.co	
2	GERMAN ALBERTO FORERO VARON	93376520	TECNICO INVESTIGADOR II	X			DELITOS INFORMATICOS / CTI	2708102 / 231	german.forer@fiscalia.gov.co	
3	BRIGITTE MAYERLY ÑUSTES OCAMPO	39571301	TECNICO INVESTIGADOR II	X			DELITOS INFORMATICOS / CTI	2708102 / 231	brigitte.nuste@fiscalia.gov.co	
4	TEDDY ALLENS DE LUQUE GOMEZ	17957475	TECNICO INVESTIGADOR II	X			DELITOS INFORMATICOS / CTI	2708102 / 231	teddy.deluque@fiscalia.gov.co	
5	ANDERSON RAYO PAMO	79995575	INGENIERO DE SISTEMAS - EXPOSITOR	X			UNAD - FGN / CTI	2708102 / 231	anderson.rayo@fiscalia.gov.co	
6	MARTHA LUCÍA HERNÁNDEZ PERDOMO	39548007	INGENIERA DE SISTEMAS - EXPOSITORA	X			UNAD		martina-2068@hotmail.com	

Fuente: Propia.

### 13. CONCLUSIONES

El aseguramiento y validación de la evidencia digital depende de los pilares fundamentales de la seguridad de la información, los cuales corresponden a la integridad, disponibilidad y confidencialidad; lográndose mediante la aplicación de técnicas y procedimientos dependientes de la seguridad informática.

La integridad de los datos digitales se logra mediante el cálculo HASH inicial, el cual debe perdurar en el tiempo para dar la autenticidad del dato digital considerado como evidencia dentro de un resultado de análisis forense informático.

La implementación o adopción de normas, estándares y guías relacionadas con la seguridad informática y seguridad de la información, permite generar un referente válido para el aseguramiento y validación de la evidencia digital producto de análisis de informática forense.

El presente proyecto permite identificar claramente la necesidad de un modelo o guía que permita el desarrollo de manera sistemática de los procesos de verificación de la evidencia digital, en el caso específico La Fiscalía General de la Nacional Seccional Ibagué; donde se debe realizar una socialización para dar a conocer el procedimiento y de esta manera aplicarlo en la entidad, de esta manera se estaría cumpliendo con el principal objetivo de crear un procedimiento para el mejoramiento de la calidad de los procesos o servicio relacionados con la informática forense.

Con el análisis realizado se ha evidenciado el poco estudio sobre el tema relacionado con el aseguramiento y validación de la evidencia digital, producto del análisis forense, debido a que no se hallaron investigaciones específicas en el área, lo que le permite a la presente investigación ser una guía para los futuros especialistas, y así generar nuevas fases al proyecto, logrando realizar varios enfoques, dentro de ellos el análisis forense a evidencias electrónicas, donde se requieren otros procedimientos y se observaría, como un estudio complementario al presente.

El presente estudio es una fuente de conocimientos para la especialización de seguridad informática, fortalece la presentación de resultados de análisis forenses informáticos dentro del campo pericial al servicio de la ley y permite a los nuevos egresados de las instituciones de educación superior perfilarse para tomar la especialización en seguridad informática con profundización en la informática forense, de esta manera el conocimiento no es dominio exclusivo de un sector o número determinado de personas, sino que existan más ingenieros especialistas en este campo que se orienta a generar y evaluar la seguridad tecnológica en las organizaciones de tipo privado como también gubernamentales.

## 14. RECOMENDACIONES

Para el tratamiento, conservación y custodia de la evidencia digital por parte de cualquier institución, se recomienda implementar el sistema de gestión de seguridad de la información, con el fin de respaldar y validar la conservación de la evidencia digital. Con lo cual se propende por la adecuada administración y gestión de la información de evidencia digital conservada a través de diferentes medios de almacenamiento ya sea de tipo electrónico o físico, lo que permite garantizar la trazabilidad y custodia de evidencias digitales dentro de los depósitos o almacenes de evidencia hasta su eficaz uso o aplicación como medio probatorio dentro de una investigación disciplinaria o de carácter legal.

A fin de resguardar la integridad de las evidencias digitales, se recomienda realizar una segunda fase de la presente investigación en donde se analice los procesos para el tratamiento y análisis informático de la evidencias inicial, de la cual se obtiene la evidencia digital derivada; de otra parte también se puede replicar el modelo con diferentes mejoras que arrojen investigaciones posteriores, en las cuales se pueda complementar un diseño de procedimientos para el análisis forense informático.

Se hace relevante mostrar los resultados de la presente investigación en diferentes medios, canales y mecanismos de publicación propios de la Universidad Nacional Abierta y Distancia; por lo cual resultaría importante involucrarlo en eventos relacionados con la seguridad informática, con el fin de enriquecer con este proceso a los ingenieros que se dedican a la labor pericial e informática forense, así como también orientar a los versados profesionales de la carrera de Derecho y relacionados con la Jurídica, Leyes, Normas y Procedimiento Penal.

Es conveniente realizar una mesa técnica integrada por peritos en informática forense de la Fiscalía General de la Nación de las diferentes seccionales, a fin de validar e impulsar la normalización y adaptación del producto obtenido en el presente proyecto, como una guía para el aseguramiento y validación de la evidencia digital derivada del análisis forense.

## 15. DIVULGACIÓN

En primera instancia la publicación del “DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE LA EVIDENCIA DIGITAL DERIVADA DEL ANÁLISIS FORENSE, APLICADO EN EL LABORATORIO DE INFORMÁTICA FORENSE FISCALÍA GENERAL DE LA NACIÓN, SECCIONAL TOLIMA” se realiza a través de la presentación del presente proyecto ante el comité evaluador; mediante lo cual se busca la anuencia y aceptación del mismo, como un proyecto acorde para optar por el título de Especialista en Seguridad Informática.

Una vez aprobado el presente proyecto de grado se sugiere la socialización ilustrativa del nuevo procedimiento para el aseguramiento y validación de la evidencia digital producto de análisis forenses informáticos al coordinador del Grupo de delitos informáticos e Informática forense de la policía judicial, junto con el comité de control y calidad de la Seccional Tolima Fiscalía General de la Nación, adicionando petición formal para la evaluación del proceso para ser implementado dentro de las guías, manuales o procedimientos de la Fiscalía General, de acuerdo a los conductos regulares de dicha institución.

Por último se tienen las opciones de presentación en los canales institucionales de la Universidad Abierta y a Distancia, como biblioteca o repositorios de documentos; adicional se tienen los diferentes eventos académicos donde se exponen estudios y avances de investigación relacionados con las tecnologías de la información, donde se puede incluir la presentación del presente diseño como una opción para el aseguramiento y validación de la evidencia digital producto de análisis forenses informáticos.

## BIBLIOGRAFÍA

CANO. Jeimy. Evidencia Digital Reflexiones Técnicas, Administrativas y Legales. {En línea}. {01 de mayo de 2017} disponible en: <<http://www.urru.org/papers/rrfraude/drjeimycano.pdf>>.

CELLEBRITE. Definición de Ufed Touch Ultimate. {En línea}. {09 de septiembre de 2017} disponible en: <<https://www.cellebrite.com/es/products/ufed-ultimate-es/>>

CONGRESO DE LA REPÚBLICA. Actuación del perito. Código de procedimiento penal LEY 906 de 2004. Bogotá: Diario Oficial No. 45.658, 2004.

CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. Bogotá. Diario Oficial 47.223, 2009.

CONGRESO DE LA REPÚBLICA. Ley 527 de 1999. Ley 527 de 1999. Bogotá. Diario Oficial 43.673, 1999.

COWMAN, S. Triangulación: una media de reconciliación en la investigación en enfermería. Diario de Advanced Enfermería, 1993, vol. 18, p. 788-792.

DE LUZ. Sergio. Criptografía: Algoritmos de autenticación (HASH). {En línea}. 09 de noviembre de 2010. {09 de septiembre de 2017} disponible en: <<https://www.redeszone.net/2010/11/09/criptografia-algoritmos-de-autenticacion-hash/>>

FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA. Glosario Grupo Delitos Informáticos. Versión 01. Subproceso Policía Judicial. (2014). Proyecto Guía Delitos Informáticos. Bogotá: Procesos de normalización.

FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA. Manual de procedimientos para cadena de custodia. {En línea}. {28 de septiembre de 2017} disponible en: <<http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf>>

FISHER. Tim. What is MD5? (MD5 Message-Digest Algorithm). (05 de octubre de 2016). {En línea}. {15 de septiembre de 2017} disponible en: <<https://www.lifewire.com/what-is-md5-2625937>>

FISHER. Tim. What is MD5? (MD5 Message-Digest Algorithm). {En línea}. 13 de Octubre de 2016. {13 de octubre de 2017} disponible en: <<https://www.lifewire.com/what-is-md5-2625937>>

FISHER. Tim. What is SHA-1?. {En línea}. 30 de Octubre de 2017. {30 de septiembre de 2017} disponible en: <<https://www.lifewire.com/what-is-sha-1-2626011>>

GLOSARIO DE INFORMÁTICA E INTERNET. Definición de Disco Duro. {En línea} 23 de Junio de 2017. {13 de agosto de 2017} disponible en: <<https://www.internetglosario.com/letra-d.html>>

GRANCE. Timothy, CHEVALIER. Suzanne., KENT. Karen, DANG. Hung. Guide to Integrating Forensic Techniques into Incident Response. {En línea}. 01 de septiembre de 2006. {15 de septiembre de 2016} disponible en: <<https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response>>

HERNÁNDEZ SAMPIERI, Roberto; FERNÁNDEZ COLLADO, Carlos; BAPTISTA LUCIO, Pilar. Metodología de la investigación. México: McGraw-Hill, 2003.

HERNANDEZ. Sergio. DELITOS informáticos?. {En línea}. 23 de abril de 2017. {10 de agosto de 2017} disponible en: <[https://issuu.com/sergiohernandessalcedo/docs/delitos\\_1\\_](https://issuu.com/sergiohernandessalcedo/docs/delitos_1_)>

INFORMÁTICA FORENSE COLOMBIA. (12 de Marzo de 2017). INFORMÁTICA FORENSE COLOMBIA. La evidencia Digital. {En línea}. {02 de agosto de 2017} Disponible en: <<http://www.informaticaforense.com.co/la-evidencia-digital/>>

INSTITUTO UNIVERSITARIO TECNOLÓGICO DE ANTIOQUIA. Cuaderno Activa. No. 9. Medellín: Darío E. Soto Duran, 2017.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (15 de Enero de 2016). About ISO. {En línea}. {02 de octubre de 2017} disponible en: <<https://www.iso.org/about-us.html>>

ISO/IEC 27037:2012. {En línea}. 23 de octubre de 2012. {02 de septiembre de 2017} disponible en: <<https://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/>>

MAMANI. Verónica. MÉTODO FORENSE EN REDES DE TELECOMUNICACIÓN PARA LA ADMISIÓN DE EVIDENCIA DIGITAL EN LA JUSTICIA BOLIVIANA. {En línea}. 28 de Junio de 2015. {13 de agosto de 2017} disponible en: <<https://es.slideshare.net/veronicadestelloazul/metodo-informatico-forense>>

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía No. 13. Evidencia Digital. {En línea}. Bogotá, Colombia. 28 de Marzo de 2016. {15 de septiembre de 2017} Disponible en: <[https://www.mintic.gov.co/gestionti/615/articles-5482\\_G13\\_Evidencia\\_Digital.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf)>



MOGUEL, Ernesto A. Rodríguez. Metodología de la Investigación. Univ. J. Autónoma de Tabasco, 2005.

NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY. Computer Security Incident Handling Guide Revision 2. U. S. Agosto, 2012.

PEREIRA PÉREZ, Zulay. Los diseños de método mixto en la investigación en educación: Una experiencia concreta. Revista Electrónica Educare, 2011, vol. 15, no 1.

RONDEROS. Juan. LA PRUEBA DIGITAL EN EL CONTEXTO JURÍDICO ACTUAL. {En línea}. 11 de noviembre de 2015. {15 de septiembre de 2017} disponible en: ([https://www.deceval.com.co/portal/page/portal/Home/Marco\\_Legal/Eventos/Presentacion\\_Deceval\\_JGRFINAL.pdf](https://www.deceval.com.co/portal/page/portal/Home/Marco_Legal/Eventos/Presentacion_Deceval_JGRFINAL.pdf))

SAMPIERI, Hernández, et al. Metodología de la Investigación, Tercera Edición, best séller Internacional. Editorial. Mc Graw Hill. México DF Julio, 2002.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE). SWGDE Misión. {En línea}. {02 de agosto de 2017} disponible en: <[https://www.swgde.org/about\\_us](https://www.swgde.org/about_us)>

DEFINICION.ORG. Definición de procedimiento. {En línea}. {08 de mayo de 2017} disponible en <<http://www.definicion.org/procedimiento>>

SWGDE. SWGDE Best Practices for Computer Forensics. {En línea}. 5 de septiembre de 2014. {02 de agosto de 2017} disponible en: <<https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics>>

SWGDE. SWGDE Model Standard Operation Procedures for Computer Forensics. 13 de septiembre de 2012. {En línea}. {02 de agosto de 2017} disponible en: <<https://www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/SWGDE%20Model%20SOP%20for%20Computer%20Forensics>>

SWGDE. SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence. {En línea}. 15 de enero de 2010. {02 de agosto de 2017} disponible en: <<https://www.swgde.org/pdf/Current%20Documents/1e17485a-df78-380d-9aa4-b649a05ebf47.pdf>>

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. About NIST. {En línea}. 5 de junio de 2015. {15 de agosto de 2017} disponible en: <<https://www.nist.gov/about-nist>>

U.S. Department of Justice. (Abril de 2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. National Institute of Justice. {En línea}. {02 de agosto de 2017} disponible en: <<https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>>

WIKIPEDIA. Definición Cómputo forense. {En línea}. {28 de septiembre de 2017} disponible en: <[https://es.wikipedia.org/wiki/C%C3%B3mputo\\_forense](https://es.wikipedia.org/wiki/C%C3%B3mputo_forense)>

## Anexo A. Carta de aceptación de desarrollo de proyecto



Ibagué; 28 De agosto de 2017.

Señores:


Universidad Nacional Abierta y a Distancia.  
Programa de Especialización en Seguridad Informática.  
CEAD IBAGUE.  
La ciudad.

Asunto: Aceptación de desarrollo de proyecto de grado.

Por medio del presente me permito informar que una vez conocido e ilustrado el proyecto de grado en Especialización De Seguridad Informática de los ingenieros ANDERSON RAYO PAMO y MARTHA LUCIA HERNÁNDEZ; el cual tiene como título "DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE LA EVIDENCIA DIGITAL DERIVADA DEL ANÁLISIS FORENSE, APLICADO EN EL LABORATORIO DE INFORMÁTICA FORENSE FISCALÍA GENERAL DE LA NACIÓN, SECCIONAL TOLIMA"; se tiene aceptación total y disponibilidad de los recursos necesarios para el desarrollo de dicha actividad.

De igual forma se observa que los recursos requeridos no violan la reserva documental, puesto que se trabajará sobre el desarrollo de procesos y herramientas forenses aplicadas en el Grupo Delitos Informáticos, del Cuerpo técnico de Investigación de la Fiscalía General De la Nación Seccional Tolima.

Atentamente,

  
JUAN BAUTISTA AVILA FLOREZ  
Profesional Investigador III  
Coordinador Grupo Delitos Informáticos.

SUBDIRECCIÓN DE POLICIA JUDICIAL TOLIMA - CUERPO TÉCNICO DE  
INVESTIGACIÓN  
TRANSVERSAL 1 SUR NO. 47-02 ZONA INDUSTRIAL EL PAPAYO  
CONMUTADOR 2708102 EXT. 256 FISCATEL 8201-8202  
[www.fiscalia.gov.co](http://www.fiscalia.gov.co)

Scanned by CamScanner

## Anexo B. Formato de recolección de datos - entrevista.

Fecha: septiembre 20 de 2017

Hora: 05:00 p.m.

Empresa: Cuerpo Técnico de investigación, Fiscalía General de la Nación – Seccional Ibagué.

Entrevistado: Ingeniero German Forero Varón.

Responsabilidad: Análisis y extracción de información a teléfonos móviles, satelitales, GPS y entre otros.

Actualmente llevo más de diez años realizando labores forenses relacionadas con la extracción de información a dispositivos de comunicación móvil y similar, cuento con certificación para el manejo de herramientas forenses como UFED Cellebrite, herramienta para la extracción de información de dispositivos de comunicación y similares.

El proceso de extracción de la información se realiza de acuerdo a la guía de manejo de la herramienta forense, puesto que se requieren instrucciones precisas las cuales son indicadas por la herramienta UFED. Una vez realizada la extracción de la información del dispositivo electrónico se procede a realizar análisis y reportes con herramienta de software forense para el análisis y generación de reportes; a continuación, me permito indicar el paso a paso para la obtención de la evidencia derivada producto de análisis forenses a dispositivos de comunicaciones móviles y similares:

1. Descripción objeto de la evidencia objeto de análisis.
2. Documentación fotográfica de la evidencia objeto de análisis.
3. Preparación de herramientas de hardware y software forense necesarias.
4. Aplicación de herramientas forenses de acuerdo a guías propias de manejo indicadas en las herramientas de hardware y software forense, para realizar extracción de imagen forense bit a bit o volcado de información en paquetes de datos en formato propio de las herramientas forenses.

5. Análisis, gestión y reportes con herramientas de análisis aplicada a la extracción de imagen forense bit a bit o volcado de información en paquetes de datos. En el cual se identifican atributos y calculo HASH MD5 y SHA1 para cada uno de los archivos obtenidos. El reporte por lo general es un esquema de presentación digital en formatos HTML, PDF, Excel e incluso visores propios de la misma herramienta de análisis, donde se relaciona la evidencia digital exportada a directorios vinculados al reporte.
6. Una vez obtenido el reporte con la herramienta de análisis y gestión. Aunque en los reportes se obtienen metadatos o atributos de la evidencia digital obtenida, así como el cálculo HASH para cada uno de los archivos. Se observa que los archivos propios del reporte no contienen calculo HASH, por tal motivo se aplica cálculo HASH a todos los archivos que componen el reporte de evidencia digital derivada, lo anterior permite documentar la integridad general de todos los archivos que componen la nueva evidencia digital derivada.
7. El cálculo de HASH para cada uno de los archivos, por lo general corresponde a un gran listado de información donde se relaciona la ruta de directorio, nombre de archivo y HASH MD5 y SHA1, de lo cual se generan gran cantidad de registros que al ser impresos ocuparían gran cantidad de páginas. Por lo anterior se procede a calcular HASH al listado general que contiene la lista HASH de archivos, obteniendo como resultado un solo registro HASH que permite realizar una verificación en cadena con respecto a la evidencia digital derivada del análisis forense realizado. Este último registro HASH se relaciona en el respectivo informe de laboratorio garantizando, con lo cual se garantiza posterior la verificación de la información obtenida en el proceso forense.
8. Obtenidos los reportes que vinculan la evidencia digital, junto con la extracción de HASH. Se procede a realizar almacenamiento o grabación de información en contenedor adecuado sin sobre escritura como CDR, DVDR, BLURAY R. Para las evidencias que superan la capacidad de almacenamiento de los contenedores antes descritos, no se tiene procedimiento claro puesto que los contenedores corresponden a dispositivos de almacenamientos susceptibles de modificación e incluso eliminación de la evidencia digital cuando sea examinada por los analistas de información o investigadores de caso.
9. Obtenidos los discos compactos o unidades de almacenamiento (contenedores de evidencia digital), se procede a realizar documentación fotográfica del elemento, embalado y rotulado. Se utiliza un embalado previo

que proteja el contenedor físico de golpes o deformaciones, para lo cual se utilizan caratulas o cubiertas de cartón pasta. El embalado es una protección sellada y se tiene en cuenta en la descripción del rótulo el último recubrimiento externo. En cuanto al rótulo corresponde a un formato normalizado en el manual de cadena de custodia de la Fiscalía General de la Nación. Adicional al embalado y rotulado se tiene el anexo de cadena de custodia, el cual corresponde a un formato normalizado por la Fiscalía, en donde se relaciona el registro de custodios o portadores de la evidencia, objeto y observaciones.

10. Como último proceso se tiene la disposición final de la evidencia derivada, la cual debe ser referenciada en el informe, es decir mencionar el destino de la evidencia, el cual puede ser el almacén de evidencias, análisis de contexto para la información o custodia por parte del investigador que solicita el análisis forense.

Preguntas específicas sobre el proceso.

De acuerdo al proceso forense descrito, se indaga por normas o referencias de buenas prácticas para el manejo de evidencia digital, en lo posible relacionados con normas de seguridad de la información:

De lo cual el entrevistado manifiesta que actualmente se adoptan los procedimientos generales referenciados en la Guía de delitos informáticos de la Fiscalía para el Cuerpo Técnico de Investigación. Se desconoce ajustes o referencias relacionadas con normas o estándares de seguridad de la información. Sólo se tienen como referencia los procedimientos y buenas prácticas propuestos por la IOCE (International Organization on Computer Evidence – Organización Internacional de Evidencia Computacional), que tienen como finalidad asegurar la integridad, confidencialidad, disponibilidad y seguridad de la evidencia objeto de análisis.

Estudiante que realiza la entrevista:

Martha Lucía Hernández Perdomo

## Anexo C. Formato de recolección de datos - entrevista

Fecha: septiembre 20 de 2017

Hora: 05:00 p.m.

Empresa: Cuerpo Técnico de investigación, Fiscalía General de la Nación – Seccional Ibagué.

Entrevistado: Juan Bautista Ávila - Coordinador del grupo delitos informáticos del CTI Ibagué.

El Grupo Delitos Informáticos de la Fiscalía Seccional Ibagué se conformó desde el año 2005, fecha desde la cual se han desarrollado guías que orientan los diferentes procesos. Dichas guías son de carácter orientador en forma general, puesto que la tecnología evoluciona constantemente y por tanto se deben aplicar procedimientos que involucran herramientas de hardware y software forense para la extracción y recuperación de datos.

Por otro lado, se deben considerar los procesos donde no se aplican herramientas forenses para la extracción de información o recuperación de datos, sino que corresponde a procesos de documentación e incluso fijación mediante impresiones de pantalla o imágenes fotográficas. Estos casos son aplicados cuando las herramientas forenses no son compatibles con el elemento a examinar, como por ejemplo la obtención de la auditoria de una base de datos, otro ejemplo puede ser la recuperación de mensajes web en redes sociales u otros medios aportados en forma voluntaria por parte de las víctimas que solo son posibles de acceder a través de una plataforma como un motor de bases de datos o páginas web, lo cual conlleva a la aplicación de procesos documentados que tienen que ser recreables de ser necesarios.

Como se ha explicado, se tienen dos procesos en los cuales al final siempre se tiene como resultado una evidencia digital derivada. Con respecto a dicha evidencia digital derivada, se procede a establecer una identificación única mediante el cálculo HASH, con lo cual se garantiza la autenticidad de la evidencia. Una vez se obtiene la evidencia con el respectivo HASH, se procede a grabar en contenedor adecuado de acuerdo a capacidad de almacenamiento, comprobado el contenido almacenado o grabado se realiza embalado, rotulado y cadena de custodia, de acuerdo al manual de cadena de custodia de la Fiscalía General.

En el anterior proceso aplicado a la evidencia digital derivada se pretende garantizar la integridad, la confidencialidad y la disponibilidad de la información, lo cual es

coherente con los principios básicos de la seguridad de la información, permitiendo la originalidad, reserva y disponibilidad de la evidencia digital a posterior durante el tiempo necesario dentro una investigación de tipo penal, donde posiblemente se tiene que evaluar la originalidad de la misma para ser admitida como una prueba fehaciente que demuestra la ocurrencia de un hecho ilegal.

Estudiante que realiza la entrevista:

Anderson Rayo Pamo



Anexo D. Resumen analítico RAE

<b>RESUMEN ANALÍTICO RAE</b>	
Tema	Tema relacionado con la Informática Forense, con el enfoque de las áreas específica del aseguramiento evidencia digital, aseguramiento evidencia física, y procesos de cadena de custodia.
Título	DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE LA EVIDENCIA DIGITAL DERIVADA DEL ANÁLISIS FORENSE, APLICADO EN EL LABORATORIO DE INFORMÁTICA FORENSE FISCALÍA GENERAL DE LA NACIÓN, SECCIONAL TOLIMA.
Autores	ANDERSON RAYO PAMO MARTHA LUCÍA HERNÁNDEZ PERDOMO
Fuentes bibliográfica	A continuación, se relacionan las referencias bibliográficas más importantes: DE LUZ. Sergio. Criptografía: Algoritmos de autenticación (HASH). {En línea}. 09 de noviembre de 2010. {09 de septiembre de 2017} disponible en: < <a href="https://www.redeszone.net/2010/11/09/criptografia-algoritmos-de-autenticacion-hash/">https://www.redeszone.net/2010/11/09/criptografia-algoritmos-de-autenticacion-hash/</a> > FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA. Manual de procedimientos para cadena de custodia. {En línea}. {28 de septiembre de 2017} disponible en: < <a href="http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf">http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf</a> > ISO/IEC 27037:2012. {En línea}. 23 de octubre de 2012. {02 de septiembre de 2017} disponible en: < <a href="https://peritoin.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-videncias/">https://peritoin.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-videncias/</a> > NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY. Computer Security Incident Handling Guide Revision 2. U. S. Agosto, 2012. SWGDE. SWGDE Best Practices for Computer Forensics. {En línea}. 5 de septiembre de 2014. {02 de agosto de 2017} disponible en: < <a href="https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics">https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics</a> >
Año	2018
Resumen	El desarrollo del procedimiento para el aseguramiento y validación de la evidencia digital derivada del análisis forense, aplicado en el laboratorio de informática forense, Fiscalía General de la Nación, Seccional Tolima; tiene como objeto una revisión documental de normas, estándares, guías y buenas practicas, relacionadas con el manejo de evidencia digital dentro del campo de la informática forense; con lo cual se busca desarrollar un proceso técnico aplicando herramientas de hardware y software para el

	<p>aseguramiento de los datos digitales producto de procesos de informática forense.</p> <p>La guía se describe mediante procedimientos prácticos donde se recomienda la aplicación de herramientas hardware y software confiables de licencia pública o privada. Los procedimientos técnicos deben garantizar la validación de la evidencia digital, bajo los principios fundamentales de la seguridad de la información los cuales corresponden a la integridad, confidencialidad y la disponibilidad.</p>
Palabras claves	Evidencia digital, informática forense, procedimiento, cadena de custodia, integridad, disponibilidad, preservación, HASH, dispositivos de almacenamiento de información digital, herramientas de hardware y software forense, transferencia y embalado.
Contenidos	<p>2. DESCRIPCIÓN DEL PROBLEMA</p> <p>3. OBJETIVO GENERAL</p> <p>4. JUSTIFICACIÓN</p> <p>5. ALCANCE Y DELIMITACIÓN DEL PROYECTO</p> <p>6. METODOLOGÍA</p> <p>7. MARCO DE REFERENCIA</p> <p>8. DESARROLLO DE PROYECTO</p> <p>9. IDENTIFICACIÓN DE COMUNIDADES TÉCNICO CIENTÍFICAS PARA EL MANEJO DE LA EVIDENCIA DIGITAL</p> <p>10. ESTABLECER PROCESOS NECESARIOS PARA EL ASEGURAMIENTO, VALIDACIÓN Y CONSERVACIÓN DE LA EVIDENCIA DIGITAL</p> <p>11. DISEÑO DE PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE EVIDENCIA DIGITAL DERIVADA DE ANÁLISIS FORENSE INFORMÁTICOS</p> <p>12. SOCIALIZACIÓN DEL PROCEDIMIENTO PARA EL ASEGURAMIENTO Y VALIDACIÓN DE EVIDENCIA DIGITAL DERIVADA DE ANÁLISIS FORENSE INFORMÁTICO.</p>
Descripción del problema	<p>Actualmente los entes de investigación penal o judicial del Estado y el sector privado no cuentan con el desarrollo de procedimientos claros para el aseguramiento y validación de la evidencia digital derivada de procedimientos de informática forense; lo anterior se evidencia en la guía y procedimientos de informática Forense, así como el procedimiento de cadena de custodia de la FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA, de igual forma se puede conocer el vacío en el documento: "Procedimiento De Evidencia Digital" en el cual se evidencia el poco cumplimiento de requisitos relacionados con la idoneidad tecnológica, procedimientos, ajuste a normas, estándares y protocolos, para el</p>

	aseguramiento y validación de la evidencia digital (Ministerio de Tecnologías de la Información y Comunicaciones –MINTIC -).
Objetivo general y específicos	<p><b>OBJETIVO GENERAL</b></p> <p>Diseñar un procedimiento estándar para el aseguramiento y validación de la evidencia digital, derivada de procesos de informática forense en el laboratorio de la Fiscalía general de la Nación Seccional Tolima encargado de dichas tareas.</p> <p><b>OBJETIVOS ESPECÍFICOS</b></p> <ul style="list-style-type: none"> <li>• Diagnosticar las herramientas con las que cuenta actualmente el laboratorio de informática forense de la Fiscalía General Seccional Tolima, para el aseguramiento de evidencia digital.</li> <li>• Identificar las diferentes normas y estándares para el aseguramiento de la información en Colombia.</li> <li>• Caracterizar las comunidades de interés (stakeholders) en buenas prácticas para el manejo de la evidencia digital.</li> <li>• Proponer nuevos procesos para el aseguramiento, validación y conservación de la evidencia digital deriva de procesos de informática forense.</li> <li>• Socializar un nuevo procedimiento para el aseguramiento y validación de la evidencia digital derivada del análisis forense, en el laboratorio de informática forense Fiscalía General De La Nación, seccional Tolima.</li> </ul>
Metodología	Para el desarrollo del proyecto se realiza una investigación documental a través de medios electrónicos o impresos, a fin de identificar normas y estándares bajo los conceptos de seguridad de la información y medios tecnológicos, adaptables a laboratorios de informática forense; de lo cual se seleccionan los referentes más significativos para el diseño del procedimiento para el aseguramiento y validación de evidencia digital derivada de análisis informáticos. Adicional se obtienen los datos actuales del proceso desarrollado en el laboratorio de informática forense.
Principales referentes teóricos y conceptuales	El principal referente teórico corresponde a la aplicación de los cálculos HASH para datos digitales a fin de obtener una cadena de texto hexadecimal que permita individualizar y asegurar la integridad de la información digital frente a una posible evaluación y validación posterior a la obtención inicial de la misma. Adicional se tienen como marco referencial diferentes documentos, entre los cuales se destacan la Norma ISO/IEC 27037:2012, Guía NIST 80061 R2 y el Model Quality Assurance Manual for Digital Evidence Laboratories (SWGDE).
Resultados	Como resultado se tiene el diseño de procedimiento para el aseguramiento y validación de la evidencia digital derivada del

	análisis forense, aplicado en el laboratorio de informática forense Fiscalía General De La Nación, Seccional Tolima.
Conclusiones	
<p>El aseguramiento y validación de la evidencia digital depende de los pilares fundamentales de la seguridad de la información, los cuales corresponden a la integridad, disponibilidad y confidencialidad; lográndose mediante la aplicación de técnicas y procedimientos dependientes de la seguridad informática.</p> <p>La integridad de los datos digitales se logra mediante el cálculo HASH inicial, el cual debe perdurar en el tiempo para dar la autenticidad del dato digital considerado como evidencia dentro de un resultado de análisis forense informático.</p> <p>La implementación o adopción de normas, estándares y guías relacionadas con la seguridad informática y seguridad de la información, permite generar un referente válido para el aseguramiento y validación de la evidencia digital producto de análisis de informática forense.</p> <p>El presente proyecto permite identificar claramente la necesidad de un modelo o guía que permita el desarrollo de manera sistemática de los procesos de verificación de la evidencia digital, en el caso específico La Fiscalía General de la Nacional Seccional Ibagué; donde se debe realizar una socialización para dar a conocer el procedimiento y de esta manera aplicarlo en la entidad, de esta manera se estaría cumpliendo con el principal objetivo de crear un procedimiento para el mejoramiento de la calidad de los procesos o servicio relacionados con la informática forense.</p> <p>Con el análisis realizado se ha evidenciado el poco estudio sobre el tema relacionado con el aseguramiento y validación de la evidencia digital, producto del análisis forense, debido a que no se hallaron investigaciones específicas en el área, lo que le permite a la presente investigación ser una guía para los futuros especialistas, y así generar nuevas fases al proyecto, logrando realizar varios enfoques, dentro de ellos el análisis forense a evidencias electrónicas, donde se requieren otros procedimientos y se observaría, como un estudio complementario al presente.</p> <p>El presente estudio es una fuente de conocimientos para la especialización de seguridad informática, fortalece la presentación de resultados de análisis forenses informáticos dentro del campo pericial al servicio de la ley y permite a los nuevos egresados de las instituciones de educación superior perfilarse para tomar la especialización en seguridad informática con profundización en la informática forense, de esta manera el conocimiento no es dominio exclusivo de un sector o número determinado de personas, sino que existan más ingenieros especialistas en este campo que se orienta a generar y evaluar la seguridad tecnológica en las organizaciones de tipo privado como también gubernamentales.</p>	