**Universidad Internacional de La Rioja (UNIR)**

**Maestría en Seguridad Informática**

# Guía de trabajo para el análisis forense de los delitos informáticos en Perú

**Trabajo de Investigación**

**Presentado por:** Llamozas Escalante, Freeman Hugo

**Director:** Márquez Sánchez, Celso

Ciudad: Tacna, Perú
Fecha: Agosto de 2021

# Resumen

El creciente aumento sobre la actividad criminal sobre algunos hechos delictivos ha generado el uso de herramientas tecnológicas que ayudan a la comprensión de como se han suscitado cada actividad, para poder tener una idea clara de cómo surge un ataque y las dimensiones del riesgo ocasionado con estos hechos.

Es en este punto que la informática forense juega un papel trascendental, otorgando una serie de herramientas y métodos que faciliten al investigador reconstruir, lo más cercano posible, la secuencia de eventos que se desarrollaron.

En el presente trabajo se tiene por finalidad mostrar una guía de trabajo para el análisis forense de los delitos informáticos en el Perú, haciendo una recapitulación de bases teóricas de las diferentes normas internacionales que se tienen y parte de la legislación peruana; sincronizando todos estos elementos y mostrando las etapas de la guía, no obstante se menciona también las fases del análisis que se encuentra en la etapa central del trabajo y que brinda características que ayudan a su comprensión y apuntes de su desarrollo.

**Palabras Clave**: Informática Forense, Tecnología.

# Maestría en Seguridad Informática

UNIVERSIDAD INTERNACIONAL DE LA RIOJA unir

## Tabla de Contenido

# Índice de Figuras

# Índice de Cuadros

# 1 Introducción

En la última década la seguridad informática ha tomado gran relevancia en su implantación en las empresas debido al cambio globalizado que se generó por la pandemia, es en tal sentido que los delincuentes han migrado a nuevas formas de operación. Lamentablemente las personas naturales no han comprendido este nuevo hecho y han sido afectadas crecientemente por el desconocimiento e ignorancia de la situación, generando una serie de hechos delictivos crecientes y que a la par demanda un nuevo enfoque para afrontarlos; teniendo en consideración a la informática forense como una técnica aplicada a los delitos que tienen como medio el uso de tecnologías.

La aplicación de la informática forense se ha ido actualizando con el pasar de los años debido al avance de la tecnología, el cual genera el instinto de constante actualización por parte de los peritos informáticos en el análisis de las evidencias digitales; de igual forma cada país tiene un enfoque centralizado a sus principales hechos delictivos cometidos en su territorio, que son asociados y llevados a un marco general que avala toda practica para realizar el tratamiento de la evidencia digital, es en este que se van creando instrucciones, procedimientos, métodos y metodologías de trabajo basándose en diferentes documentos internacionales llevados a un plano local y con el uso de las herramientas necesarias.

## 1.1 Antecedentes

Desde varios años atrás se inició la revolución de la información, con un cambio constante en el desarrollo tecnológico, generando en la sociedad del siglo XXI una evolución acelerada de las Tics produciendo así el nacimiento de una cultura informática que afecta directa o indirectamente a las personas y organizaciones afectando el carácter ético, amenazas en el comportamiento y

conducta de los individuos, de la sociedad y de la organización. (Silva & Espina, 2006)

A este hecho evolutivo debemos hacer referencia a la seguridad que se debe establecer ante los activos informáticos como (Vega Velasco, 2008) establece que la información es el recurso más importante para una empresa u organización por el cual se debe implementar medidas de seguridad a nivel de hardware, software y el recurso humano teniendo a la par políticas de seguridad adecuadas y de conocimiento de todo el personal, el cual debe estar plenamente identificado.

Pero por más que se tenga todas las medidas de seguridad, la seguridad informática total no existe, debido a que el riesgo o probabilidad de que un evento nocivo ocurra nunca es cero; lo que infiere a que el proceso de seguridad nunca acaba, nunca se puede mencionar que es total y absoluto porque cada día surgen nuevas amenazas, riesgos y vulnerabilidades dentro de los activos informáticos, para evitar estos riesgos siempre se debe tener un proceso permanente y evolutivo. (Voutssas M., 2010)

Y la seguridad informática es requerida para prevenir posibles daños ocasionados por algún delito informático, que representan un acto ilícito por atentar contra la propiedad privada intelectual de la sociedad, las organizaciones y el estado en general. Cada día estos delitos toman auge en todos los niveles; como el hurto, estafa, chantaje, entre otros, perjudicando de manera fehaciente la privacidad e identidad de cualquier persona o entidad. (Acost, Benavides, & Garcia, 2020)

Pero una vez materializado el riesgo en una situación actual en la empresa u organización, se hace necesario la aplicación de la informática forense que involucra la interrelación entre el trabajo de un profesional en informática y el sustento legal o jurisdiccional; pero siempre hace falta el trabajo de difusión y concientización en temas de seguridad y preparar gente especializada para

temas de amenazas a las que se encuentra expuesta una persona u organización. (Flores Flores & Vargas Peña, 2016)

Según lo mencionado por (Guerrero Paiva, 2009), la especialidad a la que se dedica un estudio informático forense existe varios truncamientos por los cuales no se pueden realizar con exactitud y plenitud su desarrollo.

Pero como un reto a la joven especialidad que va en crecimiento para contribuir al esclarecimiento completo, multilateral y objetivo de estos nuevos modus operandi de delincuentes que emplean nuevas tecnologías de la información y comunicación en la consumación del delito, se ve un amplio campo de investigación. (Naranjo Gómez, Mendoza Pérez, de la Caridad Alonso Betancourt, & Hinojosa Calzada, 2020)

La gran problemática que se encuentra entre los delitos informáticos y el análisis forense es encontrar una legislación vigente y en constante actualización para establecer las penalidades de estos hechos gracias al aporte del personal especializado que debe enriquecer sus conocimientos con los pocos cursos o seminarios de actualización. (Colón Ferruzola Gómez & Cuenca Espinosa, 2014)

## 1.2 Objetivo

### 1.2.1 Objetivo General

Realizar una guía de trabajo para el aprendizaje del análisis forense en los diferentes delitos informáticos en la legislación peruana.

### 1.2.2 Objetivo Específico

- Generar una relación de las herramientas que proporciona las principales distribuciones empleadas para el análisis forense.
- Demostrar la usabilidad de las herramientas de acuerdo al marco legal de

delitos informáticos.

- Verificar el documento de tratamiento de evidencia digital del estado peruano.
- Identificar las diferentes metodologías que hay para emplear en el desarrollo de técnicas forenses en la actualidad.

## 1.3 Justificación

Podemos decir que anteriormente los temas de informática, seguridad de la información, protección y recuperación de datos no tuvieron tanta relevancia como lo tienen hoy en día. Actualmente surgen necesidades informáticas con el creciente desarrollo y avance de la evolución tecnológica, las personas indagan, buscan y se auto educan en la forma de trabajo con un computador al frente, hay quienes lo mira como una herramienta de desarrollo de tareas pero existen personas que van más allá, debido a esta evolución la criminalidad ha tomado una nueva forma de operación, “modus operandi”, que en este marco de pandemia se ha mostrado con más fuerza por el desarrollo de actividades digitales, es bien sabido que las personas no son tan meticulosas en la seguridad de los activos digitales, pero cada situación o accionar de la criminalidad también llamada ciberdelincuencia afecta en un entorno global, por ese motivo grandes países han apostado por el desarrollo de marcos generalizados que engloban la gran mayoría de delitos reflejándolos en un documento impreso y acatado por firmas de los representantes de estos. No obstante, un marco generalizado no detalla claramente la situación de cada país, porque la mentalidad de cada criminal es distinta, la acción que realiza cada víctima es variante y esto debido a la educación que recibe con respecto a la seguridad de su información y que lastimosamente en este nuevo mundo es poca.

Viniendo a un plano más local, Perú, uno de los países que firmó el convenio de Budapest, en el cual se viene evolucionando esta creciente forma de criminalidad afectando en su mayoría a personas mayores por la poca

educación que han recibido sobre este tema implanta medidas de accionar contra los delitos, tiene una división de alta tecnología especializada en estas situaciones pero que no se da abasto y no genera el efecto educador de prevención ante estos hechos a esto se le puede sumar el mercado de software pirata, programas crakeados y publicidad engañosa que no aporta al bien de la población; de igual forma la ley para condenar estos crímenes conllevan un trabajo arduo por parte de peritos expertos que necesitan encontrar pruebas para apoyar al ministerio público en la conclusión de un caso, detallando un falencia en nuestro sistema de justicia y nuestro marco de trabajo para estas actividades, mencionando que desde el 2013 al 2020 se ha incrementado de forma exponencial la delincuencia informática, de las cuales solo el último año se archivaron el 58% generando una sensación de impunidad e inseguridad a la población, es en este campo donde juega un papel principal un perito informático forense, debido a que necesita un conjunto de herramientas que permitan encontrar evidencia sustancial para apoyar al fiscal, no obstante también se necesita una reforma y comprensión por parte del poder judicial para el tratamiento de estos temas; de nada sirve tener un buen perito que pueda exponer la trazabilidad de un hecho criminal hasta su ejecución, si las leyes hablan de generalidades y el poco entendimiento del idioma informático por parte de jueces y fiscales.

Con lo expuesto anteriormente, es claro que se ocupa una metodología que permita el entendimiento de sus partes para llegar a un consenso y garantizar justicia ante las víctimas. En ese sentido, en este documento se presenta una guía de trabajo que permitirá brindar conceptos y aclaraciones con respecto al análisis forense de delitos que se encuentren tipificados en la legislación peruana.

## 1.4 Metodología

A continuación, se presentan las diferentes normas en las cuales se basará este trabajo y servirán para el desarrollo del mismo:

- ISO/IEC 27037:2016
  "Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence", es una norma para identificación, recolección, adquisición y preservación de evidencias digitales, proporcionando directrices para actividades específicas con respecto al proceso de manejo de la evidencia digital, así como orienta a las organizaciones en sus procedimientos de intercambio de evidencias digitales entre jurisdicciones.

- ISO/IEC 27042:2015
  "Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence", es una norma para el análisis e interpretación de evidencias digitales, proporciona directrices de como un perito informático puede abordar el análisis e interpretación de una evidencia digital en un incidente o en una intervención pericial, desde su identificación, pasando por un análisis, hasta que es aceptada como prueba en un juicio.

- RFC 3227
  "Request for comments 3227", es un documento que recoge las principales directrices para la recolección y el almacenamiento de evidencias digitales, constituyendo un verdadero estándar para la recopilación y almacenamiento de evidencias, definiendo un proceso para la recolección de evidencias que ayuda al perito informático a adquirir y catalogar las evidencias digitales.

- RFC 4810
  Define un estándar que debe seguirse para la preservación de la información al objeto de que, la existencia de determinados archivos, creados en un determinado momento del tiempo, puedan ser probados, así como su integridad desde el instante de su creación hasta el momento en que es presentada como evidencia por un perito informático.

- RFC 4998

  Define un estándar que debe seguirse para la preservación de la información, incluyendo información firmada digitalmente, al objeto de demostrar su existencia e integridad durante un periodo de tiempo que puede ser indeterminado. También define que tipo de ficheros pueden dar soporte a estos escenarios y que requisitos debe cumplir un registro de evidencias, en el que se apoye un perito informático, para garantizar la existencia de dicha información, al objeto de evitar que pueda ser repudiada.

- RFC 6283

  Define un estándar para demostrar la existencia, integridad y validez de información durante periodos indeterminados de tiempo, además define la sintaxis en lenguaje extensible de marcas XML, así como las reglas de procesado, que deben seguirse para la creación de evidencias integras de información de largo periodo al objeto de evitar su repudio.

## 1.5 Organización del Documento

El presente documento se encuentra organizado de la siguiente forma:

En el **Capítulo 2** se expone el sustento teórico basado en trabajos y artículos que dan ejemplo para el desarrollo de la presente memoria, no obstante, se toma principios generales hasta un punto particular en detalle, este fundamento teórico es complementado con ideas y pensamientos del autor el cual va de acorde o en contrastación a lo expuesto con los autores, pero siempre buscando tener un trabajo sólido y preciso sin argumentaciones extras que fatiguen al lector.

En el **Capítulo 3** se expone la propuesta de la guía de trabajo basándose en el análisis teórico descrito en el estado de arte, para lo cual se toma se presentan 3 fases identificadas que llevan a identificar las etapas del análisis forense que son en esencia la base del desarrollo de este trabajo, no obstante, se precisa

que se presenta una idea de guía de trabajo, basándose en teoría y formas de trabajo.

En el **Capítulo 4** se presentan las conclusiones originadas por la elaboración del trabajo, para lo cual el capítulo se divide en 2 partes esenciales, hallazgos; el resultado de la realización de la guía de trabajo y la nueva idea proporcionada y trabajos futuros; que son menciones proporcionadas para la realización de futuros trabajos basándose en la idea proporcionada por este.

# 2 Marco Teórico

En este capítulo se presenta el sustento teórico de los principales conceptos que generan una aportación para el desarrollo de la guía de trabajo, no obstante, se toma como referencia las aportaciones brindadas por diferentes trabajos de investigación.

## 2.1 Seguridad Informática

La forma indebida de la utilización de términos en la actualidad hace pensar en una similitud de cada texto utilizado, para nuestro caso el hablar de seguridad informática o seguridad de la información se expresa en términos similares cuasi sinónimos, pero debemos entender que uno engloba más al detalle que el otro es por eso que (Arnedo Blanco, 2014) menciona que seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado, incluyendo la información contenida o circulante. (pág. 21)

De esta forma antes de entrar en el tema preciso de informática forense, se debe dar un apartado a la conceptualización de la seguridad debido a que ambas trabajan relacionadas, no existe el análisis forense sin la ausencia de seguridad informática y como es muy ideal la seguridad total, siempre se va tener ausencia de la seguridad total lo cual dará pie al fundamento para la informática forense.

### 2.1.1 Seguridad de la información

Después de englobar el termino de seguridad informática que se encapsula como disciplina, la seguridad de la información son un conjunto de medidas preventivas y reactivas de la entidad aplicadas en sistemas tecnológicos para resguardar y proteger la información, buscando mantener la confidencialidad, disponibilidad e integridad de la misma. (Creutzburg, Sánchez Briseño, &

Flores Oyervides, 2016, pág. 14)

Como se puede apreciar no se deben confundir los términos mencionados, seguridad informática se basa en la protección del medio, pero la información puede encontrarse en diferentes medios o formas, la información tiene un efecto significativo en la persona por eso se preserva la privacidad de esta.

### 2.1.2 Amenaza informática

Una vez determinado el termino de seguridad, se debe conceptualizar la idea que no existe la seguridad total por lo tanto siempre se tendrán amenazas que generarán un riesgo a la seguridad de la información, esta idea de amenaza se encapsula generalmente como el marco conceptual que ofrece la RAE donde se entiende que una amenaza es una acción que quiere causar un mal a algo o alguien, comprendiendo este término se debe establecer una relación con amenazas informáticas.

La amenaza informática es la probabilidad de ocurrencia de cualquier tipo de evento o acción que tenga la capacidad de ocasionar daño a los elementos de un sistema informático, pudiendo ser a nivel de software o hardware, inclusive en las dos formas juntas. (Arnedo Blanco, 2014, pág. 15)

### 2.1.3 Delito informático

También conocido por otros autores como ciberdelito, ciberdelincuencia o cibercrimen, que implica el uso de las vías informáticas para realizar acciones antijuridicas con el objetivo de destruir, dañar o secuestrar ordenadores, medios electrónicos y redes de internet. (Creutzburg, Sánchez Briseño, & Flores Oyervides, 2016, pág. 27)

La variedad de formas de operar por los delincuentes usando un computador se incrementa anualmente, y a pesar que se trata de mover la legislación para condenar estas actividades aún no se tipifican como tal, no obstante, se castiga el delito, pero no se ve el modus operandi por la cual se comete este

delito, para el caso de la legislación peruana, existen leyes identificadas con respecto a los delitos informáticos y que hacen referencia a distintas categorías como:

- Ley N°29733 – Ley de protección de datos personales.
- Ley N°30077 – Ley contra el crimen organizado.
- Ley N°30171 – Ley que modifica la ley N° 30096, Ley de delitos informáticos.

De estas leyes establecidas en el Perú, sobre todo la ley 30171 que modifica la antigua ley 30096 en la cual establece los siguientes delitos informáticos, (El Peruano, 2013):

- Delitos contra datos y sistemas informáticos.
- Delitos contra la identidad y libertad sexual.
- Delitos contra la intimidad y el secreto de las comunicaciones.
- Delitos contra el patrimonio.
- Delitos contra la fe pública.

En cada uno de ellos se establece diferentes características que fueron tomadas por el convenio sobre la ciberdelincuencia, Budapest en el 2001 al cual el Perú está adscrito.

### 2.1.4 Ataque o incidente de seguridad informática

Si se basa en la definición concreta de las palabras un ataque es una acción violenta o impetuosa contra algo o alguien y el incidente es un suceso repentino no deseado; dando una definición concreta a accidente o incidente de seguridad informática, es un suceso que contiene una acción violenta para agredir o infiltrarse dentro de un sistema de información, el cual va de acorde a lo planteado por (Arnedo Blanco, 2014), donde detalla que es un intento de violación o violación efectiva (penetración) a la seguridad de un sistema informático con fines delictivos. (pág. 15)

Para el autor (Mamani Quisbert, 2013) un ataque cumple una serie de fases para ser consolidado, los cuales se definen como:

- Reconocimiento: es un estudio previo del terreno donde se va atacar, definiendo características.
- Escaneo: se organiza la información del reconocimiento para hallar vulnerabilidades.
- Ganar acceso: el intruso aplica la mejor estrategia bajo la vulnerabilidad mejor explotable, haciendo uso de todas sus habilidades.
- Mantener el acceso: se busca mantener un acceso ganado en el sistema para poder explotar, considerando siempre mantenerse indetectable por parte del atacante.
- Cubrir las huellas: fase en donde no se debe dejar rastro alguno al terminar el ataque, se debe borrar toda evidencia posible que se deje en algún computador.

## 2.2 Informática Forense

La informática forense al igual que los anteriores términos mencionas tiene diferentes denominaciones como computación forense, forensia digital, forensia en redes, informática forense entre otras denominaciones cada termino puede llamar a la confusión debido al contexto donde se utilice pero para (Pedreros Martínez & Suárez Urrutia, 2016) define a la computación forense como una disciplina de las ciencias forenses, que ayudan a esclarecer e interpretar la información extraída de los medios informáticos como prueba principal para la justicia y para la informática. (pág. 24)

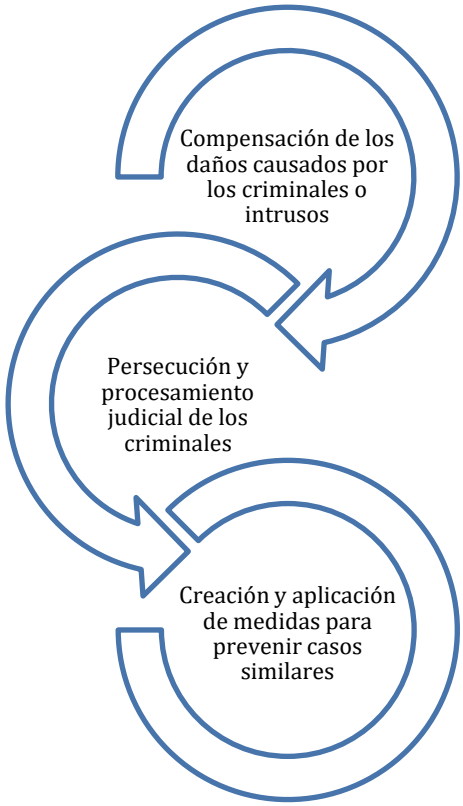
En otro aspecto la forensia digital es la materia en la cual se aplica conceptos, estrategias y procedimientos de la criminalística común a los medios informáticos con el fin de esclarecer algún delito informático. Y la forensia en

redes es netamente aplicada a eventualidades en la red, para determinar la fuente de uno o varios ataques o las vulnerabilidades existentes.

Todas estas distintas denominaciones que se dan a la informática forense convergen en un solo sentido que cumple sus fases y tiene como objetivo la preservación de la evidencia. Entonces para una definición concreta de la informática forense se menciona; que es una disciplina criminalística, que tiene por objeto, la investigación en sistemas de tecnologías de información de hechos con relevancia jurídica o para simple investigación privada. (Rafael Iglesias, 2015, pág. 8)

La informática forense se basa en la investigación de todo aquello que conlleve al tratamiento de información por lo cual busca cumplir unos objetivos, los cuales se detallan en la Figura 2.1:

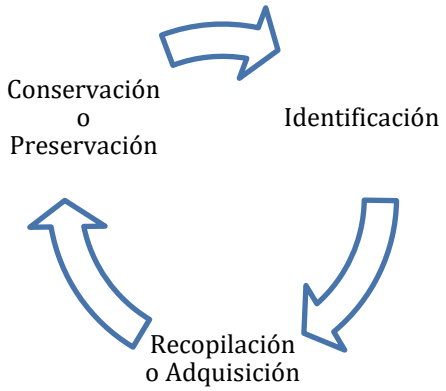
*Figura 2.1: Objetivos de la Informática Forense. Fuente: (Rafael Iglesias, 2015)*



### 2.2.1 Fases del análisis Forense

Las fases del análisis forense son variables de acuerdo a la normativa que se emplea, pero en el fondo tienen la misma finalidad en el resultado y objetivo a buscar que es la preservación de la evidencia, conservándola inalterable, sin modificaciones o correcciones. Para la presentación de las fases se tomará en cuenta las normas internacionales empleadas, detallando la versión de ISO en la Figura 2.2 y la versión RFC en la Figura 2.3.

*Figura 2.2: Fases según la ISO/IEC 27037. Fuente: (García Dahinten, 2014)*



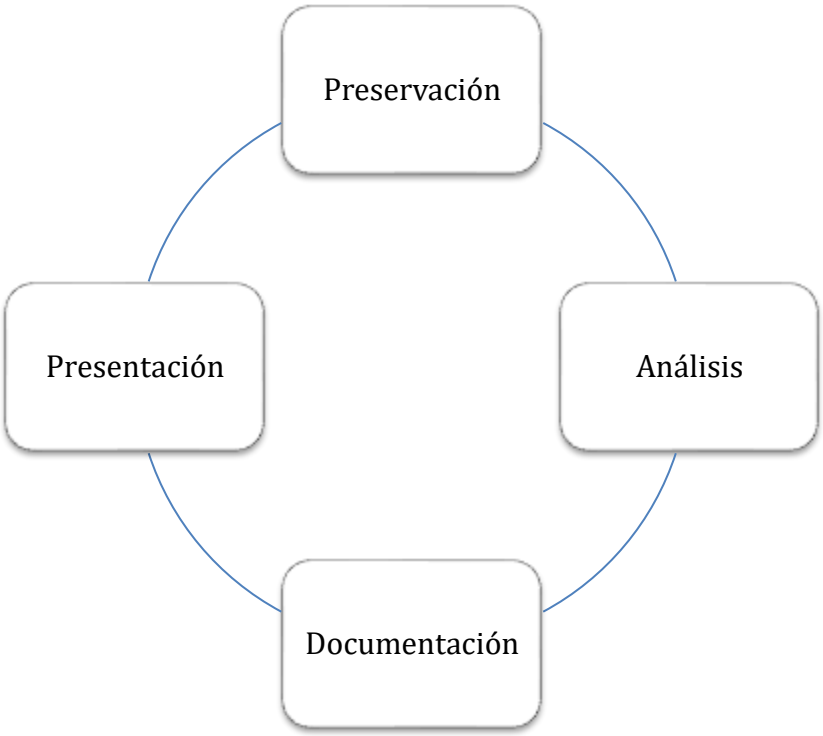

Según (García Dahinten, 2014), menciona que las fases de la informática forense según la ISO 27037 son Identificación, recopilación o adquisición y conservación o preservación, detallando:

- Identificación: es el proceso de la identificación de la evidencia y consiste en localizar e identificar las potenciales informaciones o elementos de prueba en sus dos posibles estados, el físico y el lógico según sea el caso de cada evidencia.

- Recopilación o adquisición: este proceso se define como la recolección de los dispositivos y la documentación (incautación y secuestro de los mismos) que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.

- Conservación o preservación: la evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que posteriormente pueda ser ésta admisible como elemento de prueba original e íntegra, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la cadena de custodia, la integridad y la originalidad de la prueba.

*Figura 2.3: Fases según la RFC 3227. Fuente: (Gervilla Rivas, 2014)*




Según (Gervilla Rivas, 2014) menciona que la norma RFC 3227 en todo su contexto da a conocer 4 fases del tratamiento de evidencias digitales, las cuales son preservación, análisis, documentación, presentación y se detallan:

- Preservación: en esta etapa se debe garantizar la información recopilada con el fin de que no se destruya o sea transformada. De esta forma aparece el concepto de cadena de custodia, la cual debe contener un documento donde se registra el lugar, fecha, analista y demás actores que manipularon la muestra. Haciendo uso en muchos casos de

técnicas de Hashes.

- Análisis: una vez obtenida la información y preservada, se pasa a la parte más compleja. Es la fase más técnica, donde se utilizan herramientas específicas, para esta instancia se debe considerar la evaluación de la criticidad del incidente encontrado y los actores involucrados en él.

- Documentación: si bien es una etapa casi final, se debe tener presente en todas las fases e ir documentando todas las acciones. En esta fase se debe tener claro lo analizado, contemplando lo sucedido, e intentar poner énfasis en cuestiones críticas y relevantes a la causa; se debe citar y adjuntar toda la información obtenida, asegurando la repetibilidad de la investigación.

- Presentación: se suele usar varios modelos de presentación de la documentación. Por un lado, se entrega un informe ejecutivo mostrando los rasgos más importantes de forma resumida y ponderando por criticidad en la investigación sin entrar en detalles técnicos. Este documento debe ser claro, certero y conciso. Además del informe ejecutivo se debe tener un informe técnico donde se detalla el análisis realizado, resaltando técnicas y resultados encontrados, poniendo énfasis en modo de observación y dejando de lado las opiniones personales.

### 2.2.2 La evidencia

La evidencia es una certeza clara y manifiesta de un hecho que no se puede dudar, Para (García Dahinten, 2014) la evidencia cumple unas características fundamentales. (pág. 9)

- Relevancia: se considera relevante acorde al contexto del proceso.
- Confiabilidad: está relacionada con los pasos usados para obtenerla y

la certeza que esta no ha sido alterada en ningún caso.

- Suficiencia: debe ser suficiente para probar y justificar el hecho por el cual se recolecto.

Evidencia Física

En un análisis forense informático, mencionar evidencia física es obtener elementos que permitirán conseguir información objetiva e imparcial que demostrará la veracidad de los testimonios, enmarcándose en elementos físicos tangibles que se encuentran en una escena.

Evidencia Digital

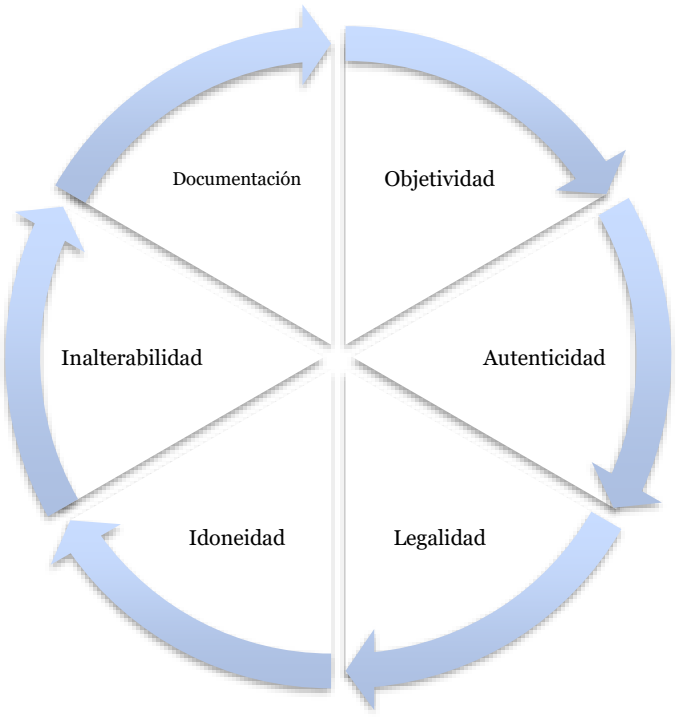
Es una denominación amplia para describir cualquier registro generado o almacenado en un sistema informático, que puede ser utilizado como prueba en un proceso legal, refiriéndose al contenido en un elemento físico de la información.

### 2.2.3 Peritaje informático

El peritaje informático es la aplicación de estudios e investigaciones orientados a la obtención de una prueba informática de aplicación en un asunto judicial para que sirva a la toma de decisiones sobre la culpabilidad o inocencia de una de las partes. Los peritos cumplen el rol de realizar el estudio técnico y tecnológico de las pruebas competentes y relevantes. (Gavilanes Molina, 2017, pág. 4)

Todo perito debe tener una serie de principios básicos que (García Dahinten, 2014) los presenta como conducta ética del perito, los cuales son presentados en la figura 2.4:

*Figura 2.4: Principios de un Perito Informático. Fuente: (García Dahinten, 2014)*




- Objetividad: el perito debe tener una independencia de la propia manera de pensar o de sentir, estar en relación a un código de ética profesional sin dejar de ser neutral y evitando la parcialidad, dejando de lado la subjetividad.

- Autenticidad: el perito debe conservar la autenticidad e integridad de los medios probatorios, todo debe estar debidamente identificado para posteriormente acreditar su autenticidad.

- Legalidad: el perito debe ser preciso en cuanto a sus observaciones, opiniones y resultados basándose en un eje legal con respecto a su actividad pericial en cumplimiento de su deber.

- Idoneidad: los medios probatorios deben ser auténticos, relevantes y suficientes para el caso, con lo cual reúnen las condiciones necesarias que permitan el desempeño de la función.

- Inalterabilidad: en todo análisis forense, existirá una cadena de custodia para asegurar que el medio de prueba no sea modificado, alterado o cambiado durante la investigación.

- Documentación: se deberá establecer por escrito cada tarea en el procedimiento de la investigación, detallando paso a paso el procesamiento de la información con la finalidad de informar los hechos.

### 2.2.4 Normativa sobre el análisis forense

Las normativas que se tienen para un análisis forense son:

Por parte de la organización internacional de normalización (ISO), las normas internacionales aplicadas a la informática forense se detallan en el Cuadro 2.1:

*Cuadro 2.1: Normas ISO para el análisis forense. Fuente: Elaboración propia*

| Norma ISO | Descripción |
|---|---|
| 27037 | Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital. |
| 27041 | Orientación para asegurar la idoneidad y adecuación del método de investigación de incidentes. |
| 27042 | Directrices para el análisis e interpretación de evidencia digital. |
| 27043 | Principios y procesos de investigación de incidentes. |
| 27050 | Descubrimiento electrónico. |

- ISO/IEC 27037:2012; brinda pautas para actividades específicas en el manejo de evidencia digital que pueden tener valor probatorio. Brinda orientación en el proceso del manejo de evidencia digital.

- ISO/IEC 27041:2015; brinda orientación para garantizar que los métodos y procesos utilizados en una investigación en relación a la

seguridad de la información sean adecuados para el propósito.

- ISO/IEC 27042:2015; presenta pautas con respecto al análisis y la interpretación de la evidencia digital de una manera que aborda cuestiones de continuidad, validez, reproducibilidad y repetibilidad.

- ISO/IEC 27043:2015; menciona pautas basadas en modelos idealizados para procesos de investigación de incidentes comunes en varios escenarios de investigación. Mencionando procesos desde la preparación previa al incidente hasta el cierre de la investigación.

- ISO/IEC 27050:2018-2021; mencionas los pasos para el descubrimiento electrónico de la evidencia digital que están constituidos en la identificación, preservación, recopilación, procesamiento, revisión, análisis, producción y producción, esta norma se divide en 4 partes y se debe precisar que la norma no pretende contradecir o reemplazar las leyes y regulaciones jurisdiccionales locales; la división de esta norma se conceptualiza en:

    - ISO/IEC 27050-1:2019; Parte 1: Descripción general y conceptos.
    - ISO/IEC 27050-2:2018; Parte 2: Orientación para la gobernanza y la gestión del descubrimiento electrónico.
    - ISO/IEC 27050-3:2020; Parte3: Código de prácticas para el descubrimiento electrónico.
    - ISO/IEC 27050-4:2021; Parte 4: Preparación técnica.

Cabe precisar que la norma ISO general para el tratamiento de la evidencia digital utilizada es la ISO/IEC 27037 y después de estolas otras normas sirven como sustento y colaboración a la norma principal.

Por parte de las directrices RFC, se detallan ene l Cuadro 2.2 las siguientes normas:

*Cuadro 2.2: Normas RFC para análisis forense. Fuente: Elaboración propia*

| Norma RFC | Descripción |
|---|---|
| 3227 | Directrices para la recopilación y el archivo de pruebas. |
| 4810 | Requisitos del servicio de archivo a largo plazo. |
| 4998 | Sintaxis de registro de pruebas (ERS). |
| 6283 | Sintaxis de registro de evidencia de lenguaje de marcado extensible (XMLERS). |

- RFC 3227:2002; proporciona pautas a los administradores del sistema sobre la recopilación y el archivo de pruebas relevantes para algún incidente de seguridad informática.

- RFC 4810:2007; menciona una clase de servicios de archivos para el soporte y demostración de documentos firmados digitalmente en diferentes escenarios y la técnica de requisitos para interactuar con dichos servicios.

- RFC 4998:2007; especifica la sintaxis y el procesamiento de un registro de pruebas, una estructura diseñada para respaldar a largo plazo evitando el repudio a la existencia de datos, buscando la integridad de estos.

- RFC 6283:2011; brinda pautas para demostrar la integridad y validez de los datos, incluidos los datos firmados para períodos de tiempo largos o indeterminados, en particular especifica las reglas de sintaxis y procesamiento para documentos XML.

De esta normativa la que primordialmente brinda información es la RFC 3227 para el análisis forense, las otras normas son para casos específicos debidos a la necesidad de firma digital y documentos firmados.

## 2.3 Modelos de análisis forense

Cabe mencionar que muchos autores definen modelo como metodologías empleadas para la realización del análisis forense, pero existe una diferencia significativa entre cada termino, para lo cual se debe proceder a diferenciar:

- Modelo: es una forma en cómo se concibe que ha de desarrollarse el proceso de análisis forense, representando de manera teórica la conceptualización de las actividades a realizar cuando se lleve a la practica en un contexto concreto.

- Método: es la manera de poner en práctica el modelo. No obstante, el método que se utilice para un análisis forense depende de las herramientas y procedimientos que se tenga.

- Metodología: es la concreción del método basado en el contexto del análisis forense, una metodología puede contener una serie de métodos y técnicas que se pueden aplicar sistemáticamente, funcionando como un soporte conceptual.

Los modelos de análisis informático forense, se tienen como objetivo presentar el ciclo de fases del tratamiento de la evidencia digital, el cual comienza desde su identificación hasta su presentación sirviendo como guía al perito forense o al técnico de la investigación, pero se debe precisar que no existe un modelo estándar que generalice el trabajo, pero si existen modelos reconocidos. (Arnedo Blanco, 2014, pág. 54)

### 2.3.1 Modelo Digital Forensic Research Workshop (DFRWS)

Este modelo se desarrolló entre 2001 y 2003 en el Digital Forensic Research Workshop. Trajo consigo la capacidad de aportar “Clases de Acción dentro de la investigación digital”. Tiene técnicas que dan la posibilidad de clasificar en grupos las diferentes actividades que se desarrollan en un proceso de

investigación. Este modelo rige que cada investigación se debe realizar de forma independiente y muy detallada sobre una matriz. También se debe indicar las actividades que se realizan y todas las técnicas usadas en la misma. Las actividades que se realizan en este proceso son:

- Identificación
- Colección
- Preservación
- Análisis
- Examen
- Informe
- Decisión

### 2.3.2 Modelo Casey (2000)

Dentro de los modelos de análisis informático forense se encuentra el desarrollado por Eoghan Casey en el 2000. Este modelo ha tenido un largo proceso evolutivo desde su versión inicial. Los procesos que el modelo incorpora para su realización son:

- Localización e identificación de las evidencias.
- Adquisición, conservación y documentación de evidencias.
- Clasificación, individualización y comparación entre las evidencias.
- Reconstrucción de los hechos sucedidos.

Es importante detallar que, en los últimos procesos, se pueden repetir ciclos. También se pueden presentar nuevas evidencias. Si es así es necesario un nuevo procesamiento. Debido a esto las actividades son denominadas por Casey como ciclo de procesamiento de las pruebas.

### 2.3.3 Modelo Casey (2004)

Es una versión más completa y mejorada del anterior modelo. Se compone de diferentes fases:

- Preparación y autorización de las pruebas
  En esta fase se abarcan todas las actividades de la recopilación de pruebas. También las que se realizan antes de las autorizaciones legales que se den en el proceso de peritación.

- Reconocimiento de las evidencias
  Es el detalle y estudio de todas las pruebas y evidencias que se han encontrado.

- Documentación de las pruebas
  Esta fase se trata de una repetición. Se realiza durante todo el tiempo que dure la investigación. Se trata de documentar por escrito todos los procesos que se llevan a cabo para poder localizar las pruebas que dan la posibilidad de esclarecer los hechos que se dan en el incidente de seguridad informática.

- Obtención de las pruebas
  Dentro de los modelos de análisis forense, se produce una imagen de los datos o contenido digital del dispositivo de almacenamiento que se esté analizando. Todo esto se podrá utilizar en futuro como prueba en un procedimiento judicial.
  Es necesario realizar diferentes copias de todos los elementos. Esto se realiza para garantizar una mayor seguridad a la hora de preservar la integridad de las pruebas originales, estas nunca se deben de tocar, manipular o borrar.

- Conservación de las pruebas

  Se aseguran todas las pruebas. También, en este paso deben de ser capaces de garantizar de forma plena la integridad de los datos originales.

- Análisis de las evidencias

  Usando las herramientas de software indicadas se analizan las copias de las evidencias. También se realizará una hipótesis. Igualmente se comenzará con el proceso de investigación, arrojando información relevante que permitirá la validación y el acaloramiento de los hechos.

- Reconstrucción de los hechos

  En esta fase ya se debe haber respondido las preguntas; ¿Desde dónde?, ¿De qué forma?, ¿Cuál es la víctima del ataque?, ¿Quién o quiénes atacaron? y ¿Cuándo?

- Informe de la pericia

  Esta es la fase final en la que se elaborará un informe detallado de todos los procesos que se han llevado a cabo. Así como todos los resultados.

### 2.3.4 Modelo Forense del Departamento de Justicia de EEUU

Según la división especializada llamada "Sección de Crimen Computacional y Propiedad Intelectual". Basándose en una gran cantidad de aportaciones de funcionarios relacionados con la informática forense, dando como resultado tres fases principales que establece este modelo, haciendo hincapié en cómo se deben realizar estas fases:

- Preparativos y extracción
- Identificación de las pruebas
- Análisis

También establece especificaciones básicas dentro de la investigación.

- Uso de métodos científicos
- Recopilación y preservación
- Validación
- Identificación
- Interpretación y análisis
- Registro, documentación y preservación.

### 2.3.5 Manual para el tratamiento de evidencia digital

Es un documento elaborado por el (Ministerio de Justicia y Derechos Humanos, 2017) para afianzar la relación entre la policía y la fiscalía a fin de elaborar y coordinar, con dirección del fiscal, una estrategia de investigación en la que se discutan y optimícenlos mecanismos de recolección de evidencia digital, estableciendo unas fases:

- Aseguramiento de la escena
- Reconocimiento e identificación
- Adquisición y captura
- Preservación de la evidencia

## 2.4 Herramientas de software para el análisis forense

Actualmente se cuenta con una gran variedad de herramientas de análisis forense que se especializan en un determinado aspecto a analizar, estas herramientas pueden ser obtenidas de forma independiente de acuerdo al sistema operativo en el que se trabaje o pueden estar contenidas en suites especializadas para este trabajo. No obstante, la certificación del uso de la herramienta o la facilidad del empleo de esta no garantiza su aprobación por parte de una parte legal, en consecuencia, dependerá del criterio del analista forense para la utilidad de alguna de estas; a continuación, se presentan algunas herramientas utilizadas, así como suites especializadas para el tratamiento de la evidencia digital.

### 2.4.1 Herramientas de análisis de red

Estas herramientas se especializan en el escaneo de los puertos de red, verificación del tráfico, algunos bajo una serie de reglas para el tráfico de paquetes, funcionando como rastreadores, depuradores de tráfico, auditoria de paquetes, analizadores de protocolos y datos. Entre los cuales se tiene Snort, Nmap, Wireshark, Xplico entre otros.

### 2.4.2 Herramientas para tratamiento de discos

Estas herramientas sirven para el tratamiento de discos duros en sus ámbitos de HD o SSD, procuran la realización de una imagen en bajo nivel, byte a byte, incorporando las zonas ocupadas y los espacios libres para su análisis, protegiendo así la evidencia más importante a ser analizada dentro de la evidencia digital. Entre las herramientas que se tienen se pueden mencionar Dcdd3, Acronis, Guymager, entre otros.

### 2.4.3 Herramientas para tratamiento de memorias

Dentro del proceso de adquisición de la memoria en casos de equipos encendidos, se debe considerar herramientas que faciliten esa tarea, analizar los procesos, volcados de memoria, siempre verificando que no se altere la evidencia a tratar. Entre estas herramientas se tiene Volatility, Memoryze, RedLine, entre otros.

### 2.4.4 Herramientas para el análisis de aplicaciones

Dentro del análisis de aplicaciones en las evidencias digitales, se utilizan herramientas que verifican códigos hexadecimales o ensamblador, sabiendo que este modo de código es más entendible que el código binario utilizado para crear una aplicación. Entre las herramientas utilizadas se tienen OllyDbg, OfficeMalScanner, Radare2, Process explorer. PDFStreamDumper, entre otros.

### 2.4.5 Suites para el análisis forense

Las suites de análisis forense son sistemas operativos que tienen la característica de ser ejecutados a través de un cd-live, esto genera que se puedan utilizar las herramientas que contienen dentro de la distribución,

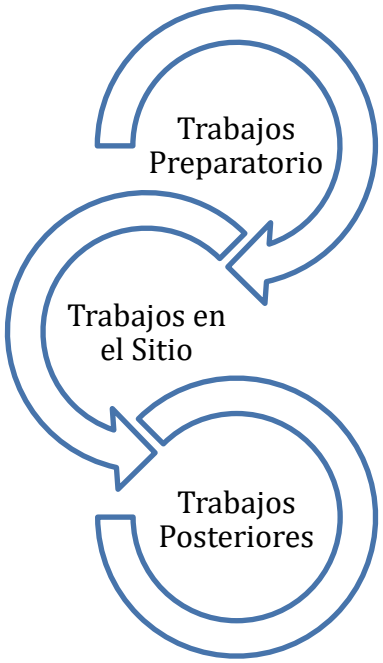
mayormente las más usadas son CAINE; es una distribución live de GNU/Linux italiana, creada como un proyecto de Digital Forensics, ofrece un entorno forense completo que está organizado para integrar herramientas de software existentes como módulos de software y para proporcionar una interfaz amigable. Deft Zero; es una distribución personalizada de CD live de Linux basado en Debian, Lubuntu. Es un sistema fácil de usar que incluye excelente detección de equipo y aplicaciones de código abierto dedicadas a la respuesta ante incidentes y al análisis forense computacional. Kali Linux; Anteriormente conocido como BackTack Linux, es una distribución Linux de código abierto basado en Debian. Destinada para la realización de pruebas de penetración, auditoría de seguridad y herramientas forenses. Parrot OS; Es una distribución GNU/Linux basada en Debian y diseñada pensando en la seguridad y la privacidad, contiene una gama de herramientas para todo tipo de operaciones de seguridad cibernética, desde pentesting hasta análisis forense digital e ingeniería inversa, todas las versiones de Parrot vienen con herramientas y documentación referente a ellas para usarlas. Backbox; Es una distribución Linux orientada a pruebas de penetración y evaluación de seguridad que proporciona un conjunto de herramientas de análisis de redes y sistemas, que fue creada con el objetivo de promover la cultura de seguridad en el entorno de TI, utilizando exclusivamente Software Libre de código abierto, incluye algunas de las herramientas de análisis y seguridad más comunes conocidas y utilizadas desde análisis de aplicaciones web hasta el análisis de redes, pruebas de estrés, rastreo, evaluación de vulnerabilidades, análisis forense informático, automoción y explotación.

# 3 Guía de trabajo propuesta

Con la verificación de las bases teóricas y de la argumentación del estado del arte con base en otros autores y sus aportes en distintos trabajos se debe establecer en que se basa la guía de trabajo; las normas, estándares y aspectos legales internacionales establecen un marco de trabajo bajo distintas fases del análisis forense y eso es todo donde se centra, mas no establece procedimientos anteriores y posteriores a esta, en esta guía también se aborda estos aspectos como parte esencial, una parte preparatoria para el recojo de información y una parte post presentación de la documentación encontrada, esto abarcando todo un proceso significativo.

Con esto se pone de manifiesto todo un conjunto de puntos importantes a tener en cuenta para realizar un trabajo, dentro de las etapas que se ponen en manifiesto se detallan 3 importantes, presentados en la Figura 3.1:

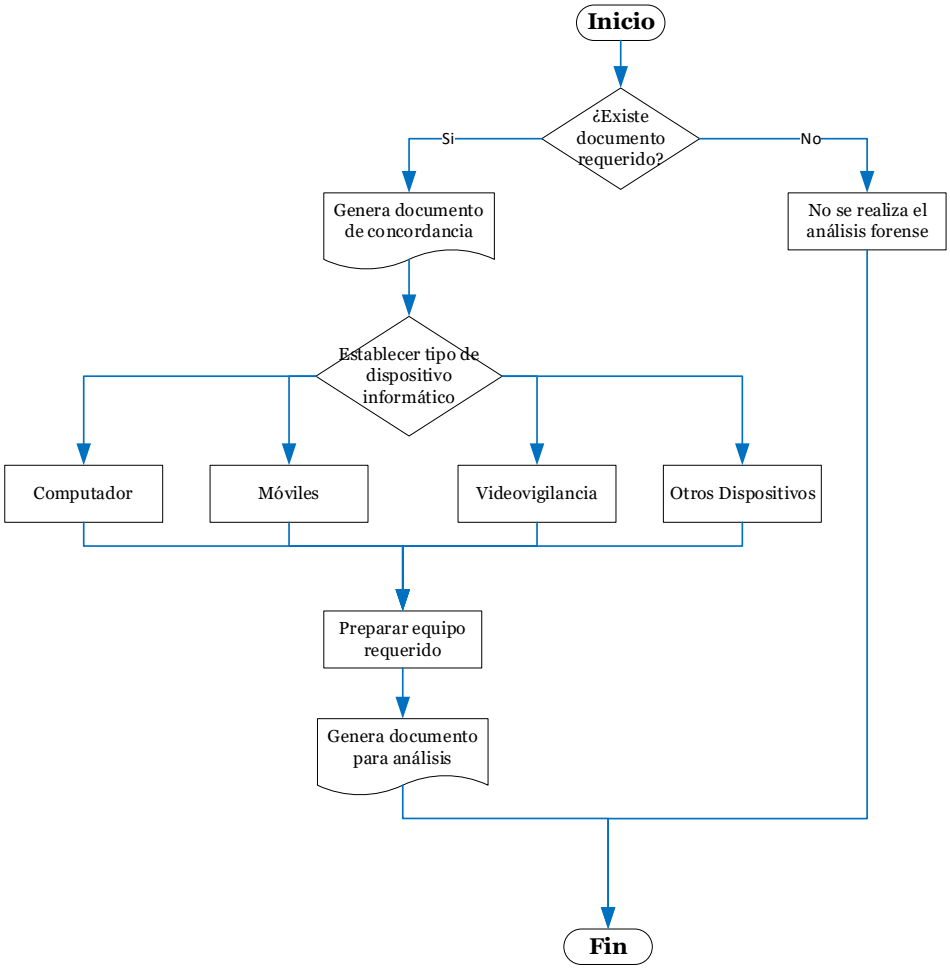
*Figura 3.1: Etapas de trabajo. Fuente: Elaboración propia*



## 3.1 Trabajos preparatorios

Es toda actividad anticipada a realizar previo a dirigirse a un evento que indique o requiera el análisis forense, estas actividades preparatorias consisten en alistar todas las herramientas de software y hardware necesarias para poder realizar un buen trabajo, con la eficiencia que se requiera para la precisión que se demanda según sea el caso. Esta etapa es necesaria para proceder con las demás, se debe precisar que todo análisis forense no se realiza sin un documento que indique su necesidad bien por parte de la fiscalía o por parte del ministerio del interior; en ese documento se precisa a qué tipo de dispositivo se va realizar el análisis por lo tanto se procede a utilizar herramientas requeridas para cada tipo de análisis. Se puede mencionar un esquema de trabajo preparatorio en la Figura 3.2:

*Figura 3.2: Diagrama de la fase de Trabajos preparatorios. Fuente: Elaboración propia*



### 3.1.1 Herramientas de Software

Dentro de las herramientas de software se compone de toda aquella herramienta informática que ayuda al tratamiento de la evidencia digital, estas pueden estar compuestas por herramientas especializadas por algún tipo de dispositivo, sistema operativo o también herramientas libres que son compuestas dentro de un kit a través de un cd-live o independientes para su uso, se debe precisar que todas estas herramientas son de libre distribución o propietarias o proporcionadas por el estado, cabe destacar que para usos específicos de alguna institución se cuenta con herramientas más especializadas.

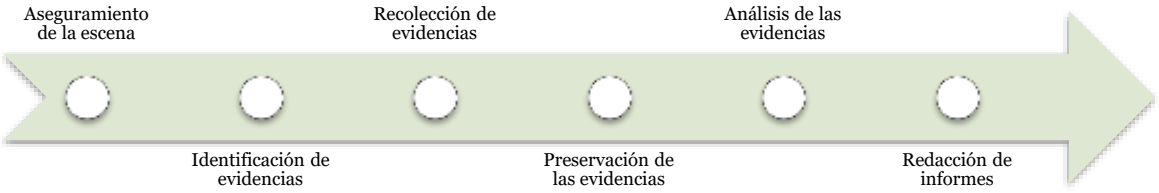
### 3.1.2 Herramientas Hardware

Dentro de las herramientas de hardware no solo se tiene en cuenta el material que nos pueda garantizar almacenar una imagen de la evidencia digital, también se debe agregar el material que ayude como equipo de protección al perito para realizar su trabajo, por tato es necesario que se tenga algún material especial para su tratamiento, un kit que ayude a realizar trabajos manuales si se debe incautar alguna evidencia o desarmar algún equipo informático, de igual forma se debe tener algún equipo que garantice la integridad de la evidencia.

## 3.2 Trabajos en el sitio

Los trabajos en el sitio están referidos a la realización de las etapas del tratamiento de la evidencia digital, desde su identificación del sitio para trabajo hasta la presentación de la documentación pertinente. La realización de estas etapas de acuerdo a o mencionado en las normas se establecen en 6 etapas, tales como se presenta en la Figura 3.3:

*Figura 3.3: Etapas de los trabajos en sitio. Fuente: Elaboración propia*




### 3.2.1 Aseguramiento de la escena

Como es típico en toda etapa de análisis es asegurar el escenario donde se va trabajar, para nuestro caso el área donde haya ocurrido un incidente que contenga una probabilidad de riesgo alta o se ejecutando en el momento, no solo es centrarnos en un análisis técnico mediante el uso de herramientas que nos brinde información requerida para ver la línea de tiempo de hechos, también es incorporar una serie de procedimientos que nos ayude a establecer la escena, para lo cual siempre se debe considerar lo siguiente:

"Conservar en forma original el área física donde ocurrieron los hechos para evitar cualquier manipulación, alteración, destrucción, perdida, contaminación o sustracción de algún dispositivo."

Es por ello que se deben realizar actividades para el reconocimiento de la escena:

- Generar un documento de intervención, donde se detalle el personal a cargo que realizara actividades competentes a su cargo, se debe precisar que este personal debe estar debidamente acreditado y con el equipo requerido que no altere la escena, ni obstaculice las actividades de algunos otros peritos.

- Aislar la escena de los hechos de personal que cumpla alguna función dentro del área, debido a que son implicados en la escena y contar con un representante del área para que brinde información requerida de accesos y trabajadores o en su defecto de la persona que es propietaria del equipo intervenido.

- Realizar una evaluación situacional sobre cómo se encuentran los dispositivos a la hora de la intervención, detallando en un cuaderno de actividades de intervención, toda aquella información que sea relevante para la realización de la actividad e implique algún riesgo latente que interfiera con alguna tarea a realizar, de igual forma características que se hallan encontrado a la hora de la intervención.

- Realizar tomas fotográficas del entorno donde se desarrollaron los hechos, de igual forma del equipo a intervenir, las fotos deben tener un pie de página que indique la hora y fecha en la que han sido realizadas, para tener una secuencia de inspección.

- Proteger en todo momento el área de la escena, no dejando huellas dactilares que puedan obstaculizar el trabajo de otros peritos, verificando conexiones del equipo implicado.

Una vez finalizada la primera fase, y con la escena bien asegurada teniendo en cuenta todos los puntos expuestos anteriormente, se puede pasar a una segunda fase.

### 3.2.2 Identificación de evidencias

En este punto hay que tener en cuenta una serie de factores acerca de la identificación de la evidencia, teniendo en cuenta en que dispositivo se encuentra la evidencia, la volatilidad de esta, el estado en el que se encuentra el equipo y características requeridas del medio.

a) Dispositivos tecnológicos

Para todos los casos de dispositivos que puedan formar parte de la evidencia digital, estos dispositivos se pueden subdividir en 2 grupos:

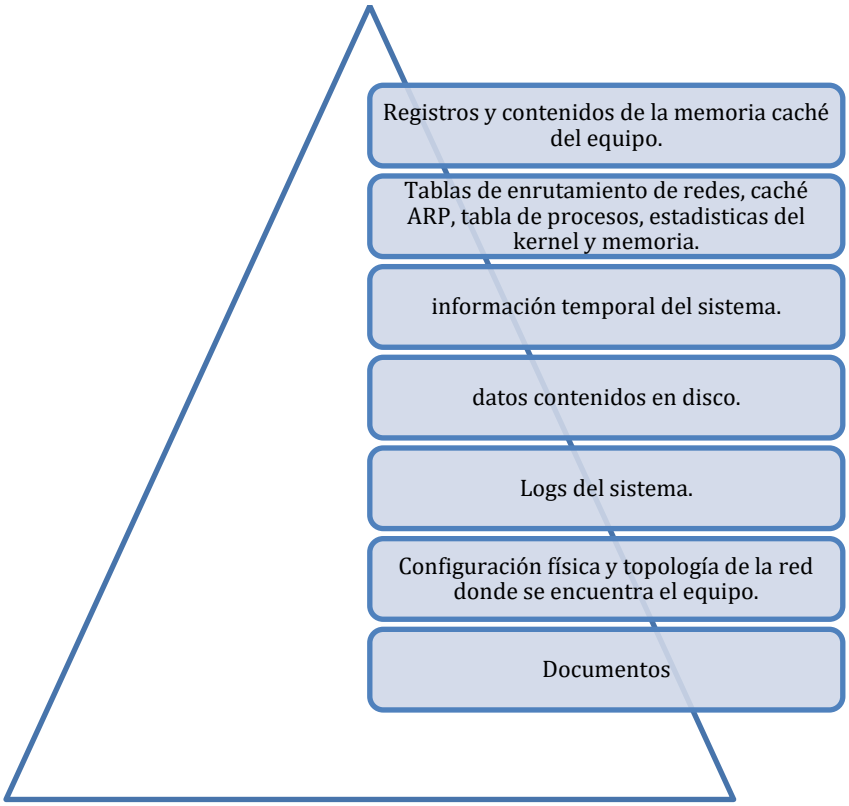
- Dispositivos informáticos
  - Computador personal (PC).
  - Computador portátil (laptop, notebook).
  - Servidor.
  - Disco duro.
  - Disco duro externo.
  - Pendrive.
  - Memoria externa (SD, MicroSD)
  - Lector de banda magnética (Skimmer).
  - Tarjeta electrónica.
  - Sistema de video vigilancia (DVR, NVR, NDVR)
  - Equipos de telecomunicaciones (router, switch, firewall).
  - Impresora multifuncional.
  - Cámara espía.
  - Caja de liberación y desbloqueo.
  - Cámaras filmadoras y fotográficas.

- Dispositivos móviles
  - Equipo de terminal móvil (teléfono celular).
  - Tarjeta SIM (chip).
  - Modem USB (internet móvil).
  - Sistema de posicionamiento global (GPS).
  - Palm.
  - Tableta (tablets).
  - Vehículo aéreo no tripulado.
  - Reloj inteligente (smartwatch).
  - Terminal de punto de venta (POS).

b) Volatilidad

Cuando ya nos referimos a la volatilidad, se menciona la forma de acceso a los datos o el periodo de tiempo en el que estarán accesibles en el equipo debido a que estos son muy susceptibles al cambio, por lo cual se debe identificar si se tuviera un equipo encendido se debería identificar cual sería la secuencia de captura de datos que también por las normas anteriormente vistas se puede llegar a una concordancia presentada en la figura 3.4:

*Figura 3.4: Volatilidad en un computador. Fuente: Elaboración propia*




c) Estado del dispositivo

En el estado del dispositivo se debe detallar dos casos puntuales, cuando el equipo se encuentra prendido o apagado, para cada caso en el que se encuentre se debe contemplar acciones diferentes:

- Dispositivo encendido

  Para un dispositivo encendido se debe visualizar la pantalla donde se presentan los procesos que se estaban ejecutando, la verificación de la hora y fecha del equipo, carpetas o programas que se ejecutaron a la hora de la intervención, fotografiar todos los aspectos relevantes encontrados, de igual forma si se verifica la existencia de alguna conexión externa o de red se debe documentar y generar la toma fotográfica correspondiente.

- Dispositivo apagado

  En un sistema apagado se debe realizar tomas fotográficas de las conexiones establecidas en el equipo, a través de algún dispositivo externo, si el equipo se encuentra conectado a algún suministro eléctrico establecer si existe algún riesgo si se corta este suministro.

d) Características del dispositivo

   Entre las características del dispositivo es la identificación de cada equipo a través de sus características específicas que contiene como su marca, modelo, características técnicas de funcionamiento y detalles principales o rasgos que estén relacionados con el dispositivo, garantizando que no se realice ninguna actividad inadecuada y preservando la integridad del equipo.

Para la identificación se debe establecer también algunas precisiones:

- Contar con un identificador único de dispositivo.
- En el cuaderno de actividades de la intervención redactar la persona que identifico la evidencia, detallando lugar (ubicación), fecha y hora.
- Identificar si será posible la recolección del equipo en físico a través de su incautamiento o si se debe realizar alguna copia para trabajo en el laboratorio, siempre recordando que esto no afecte alguna política de privacidad de la empresa o en su debido defecto establecer los permisos

necesarios para estos dispositivos, esto porque posiblemente se vea información confidencial, información sensible y muy privada.

### 3.2.3 Recolección de evidencias

Una vez asegurada e identificada la escena se procede a la recolección de las evidencias, para esta recolección se debe tener en cuenta lo siguiente:

- Verificar si los dispositivos pueden ser transportables o no (por su volumen, limitaciones legales, funcionalidades, entre otros), esto ayuda a definir en el sitio el mejor camino a seguir.

- Toda recolección de evidencia se debe realizar con un documento previo, de igual forma en el cuaderno de actividades se debe detallar aspectos de quien está recolectando, motivo, hora, fecha, observaciones al dispositivo y procedencia de actividad.

- Realizar las tomas fotográficas necesarias en la recolección de cada evidencia, de ser necesario se puede utilizar medios de grabación para garantizar el levantamiento de la información requerida, esta acción se realiza antes, durante y después de hecha la actividad.

- La información recogida se debe embalar y lacrar individualmente, colocando siempre un rotulo y código de identificar de dispositivo que en la anterior etapa se había definido.

Cabe destacar que para cada dispositivo se debe realizar una actividad distinta, por lo tanto, se debe tener presente dos definiciones básicas que se utilizaran en esta etapa; las cuales son:

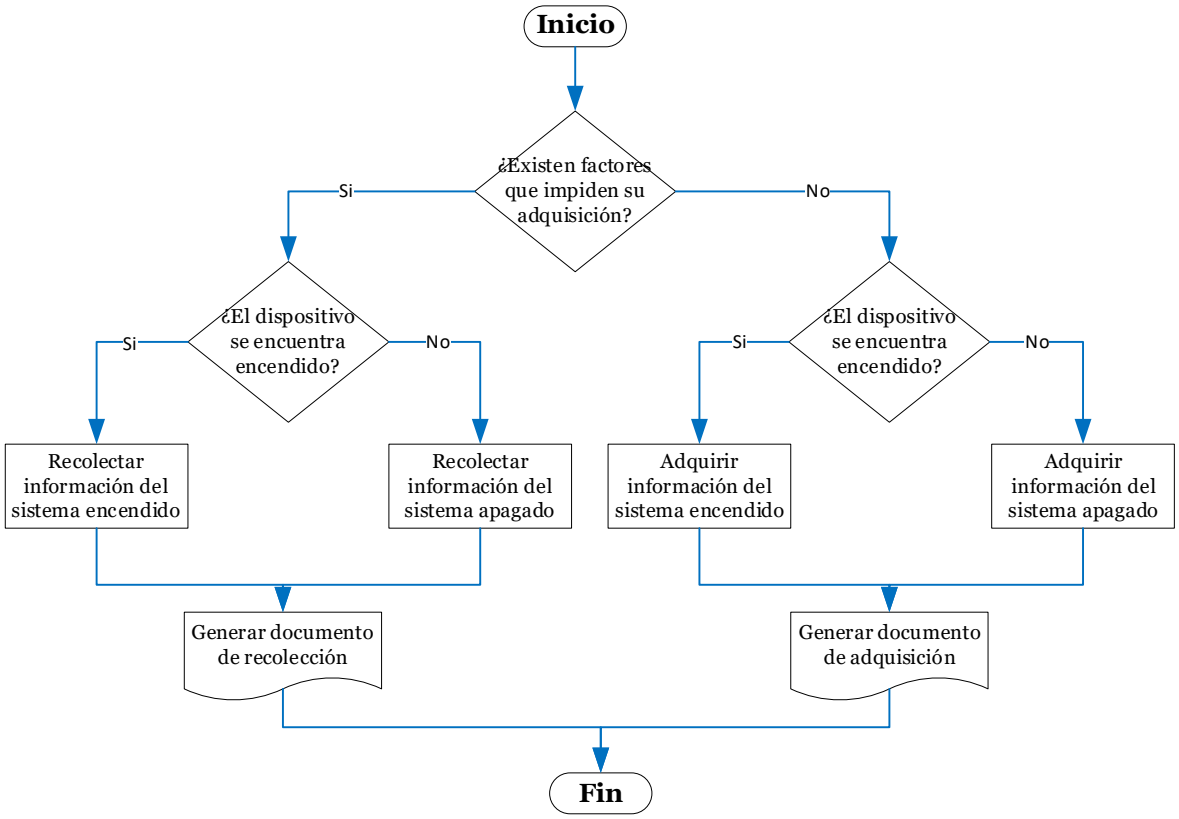
Recolección: cuando decimos recolectar, es trabajar con una copia fiel al original, debido a factores en los cuales imposibilita obtener el dispositivo de alguna institución, estos factores pueden ser legales, burocráticos o

simplemente impedimentos establecidos por alguna entidad debido a la sensibilidad de la información contenida.

Adquisición: la adquisición está establecida por la facilidad de la obtención del dispositivo afectado, el cual es brindado por la entidad u organización que facilita el incautamiento de este dispositivo y posterior análisis.

Una ves comprendida la definición de estos términos, podemos detallar un flujo de la actividad, como se presenta en la Figura 3.5:

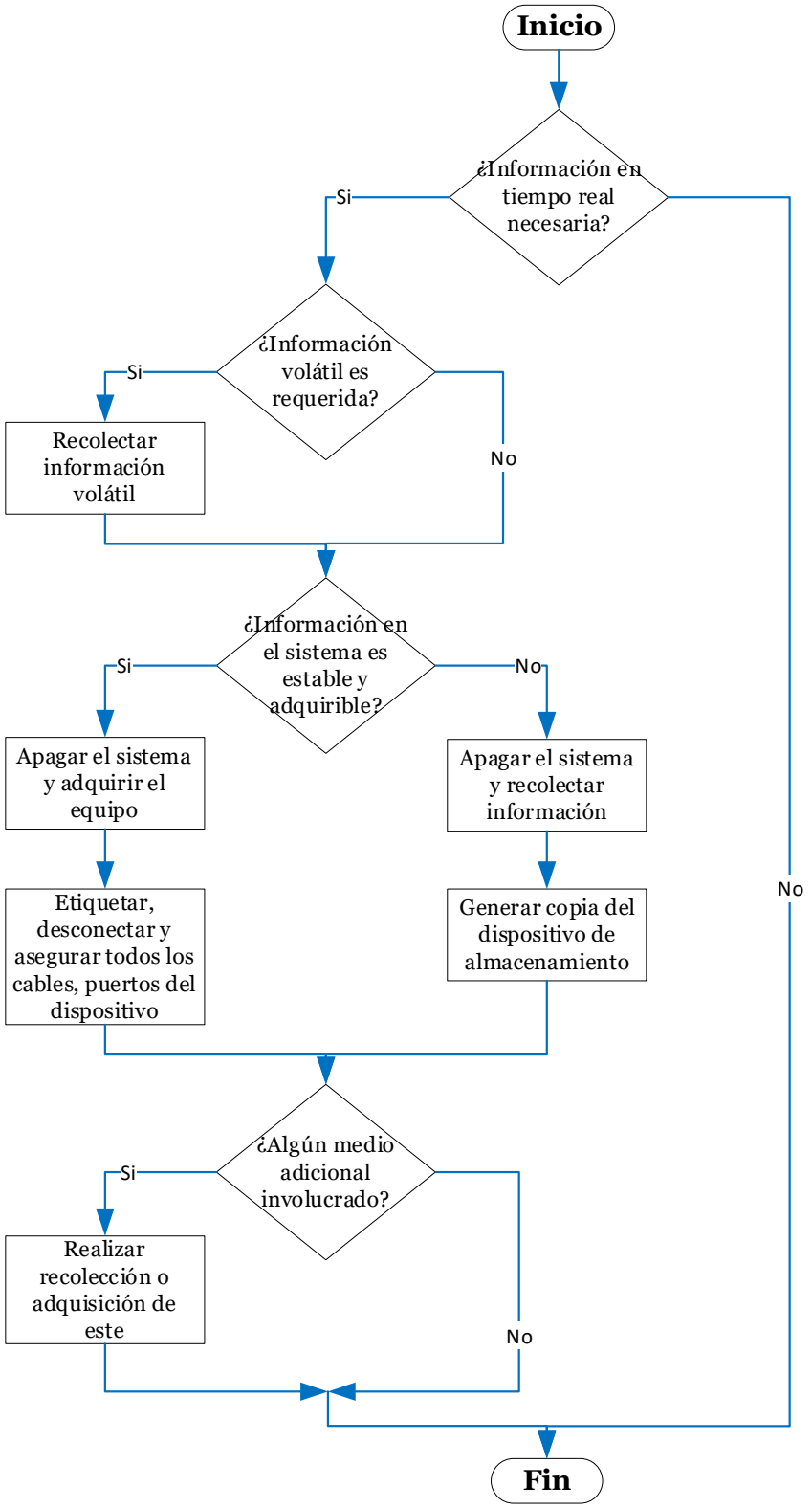
*Figura 3.5: Recolección de evidencias. Fuente: Elaboración propia*




Con esto podemos comprender que existen 2 casos para la recolección o adquisición, sabiendo que en las anteriores etapas ya se mencionó la prioridad de recolección de información, los tipos de dispositivos y características esenciales que se deben tener en cuenta, para lo cual se deben seguir los pasos para dispositivos encendidos como en la Figura 3.6 y para dispositivos apagaos como se muestra en la Figura 3.7:

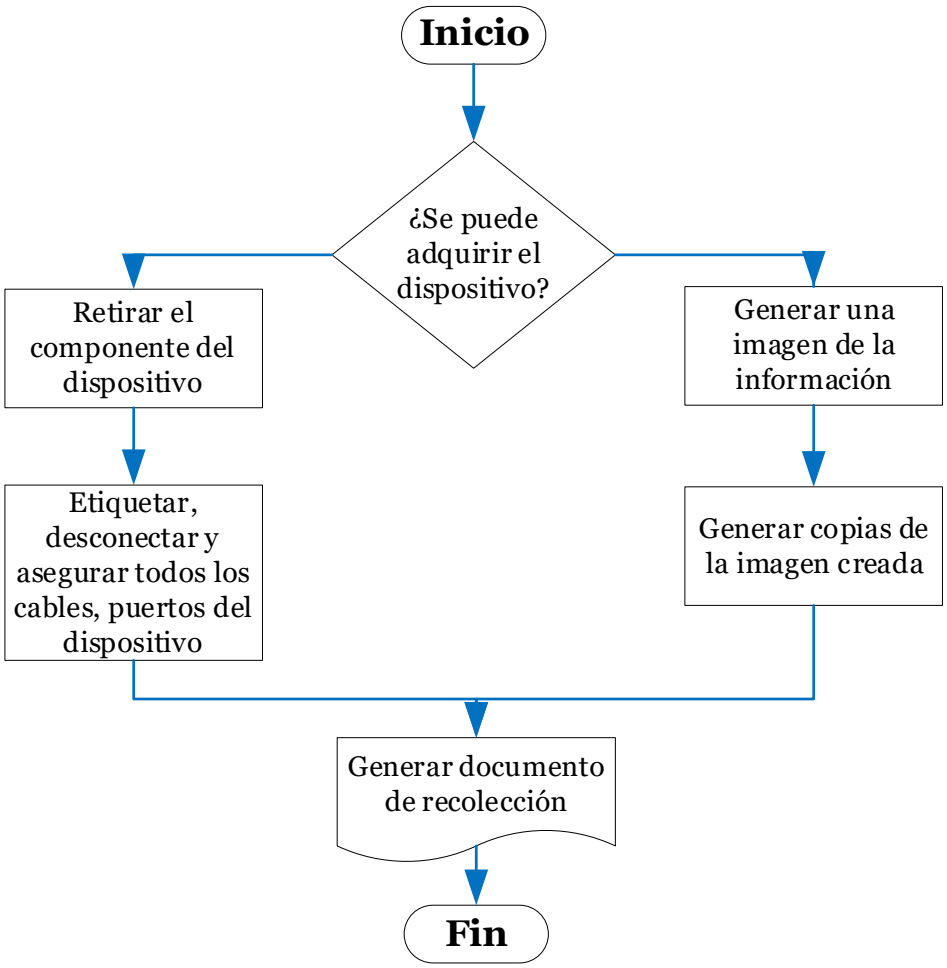
## Dispositivo encendido

*Figura 3.6: procedimiento para dispositivo encendido. Fuente: Elaboración propia*



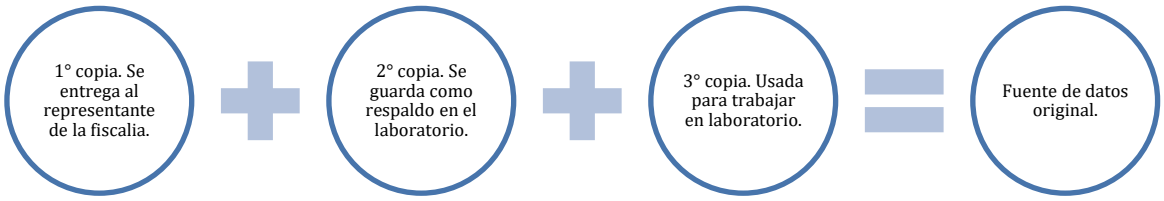
Dispositivo apagado

*Figura 3.7: procedimiento para dispositivos apagados. Fuente: Elaboración propia*




Detallando la situación con la elaboración de copias o imágenes de los discos se debe precisar que se necesita a la elaboración del disco la creación del Hash que permite mantener la integridad de la imagen elaborada, el hash puede ser obtenido por funciones SHA256, SHA1 o MD5 que son funciones únicas para elaborar el Hash de un archivo. Además, se debe precisar que se tienen que tener más de 1 copia de la imagen de algún disco como fuente de datos originales, esta indicación se presenta en la Figura 3.8:

*Figura 3.8: Copias de la fuente de datos. Fuente: Elaboración propia*




### 3.2.4 Preservación de las evidencias

Cuando se habla de la preservación de la evidencia, se trata de guardar la integridad de toda evidencia recopilada o adquirida, debido a que un mal uso o mala manipulación de esta podría invalidar toda la investigación, con llevando al repudio de esta en un tribunal como prueba. Para la preservación de la evidencia se habla en toda norma sobre la cadena de custodia que es un procedimiento aplicado a toda evidencia desde su identificación hasta su análisis en el laboratorio, la cadena de custodia busca siempre evitar cualquier tipo de manipulación y tener un control absoluto sobre los elementos incautados.

Durante toda esta cadena de custodia se debe realizar anotaciones y gracias a eso se puede tener un control sobre cada evidencia, desde la identificación se establece una identificación, datos del personal responsable del material, descripción del mismo, lugar donde se encontró la evidencia, fecha y hora del evento y observaciones de la misma, para la recolección o adquisición del mismo se debe establecer los datos de la persona que realizo esta actividad, colocar el dispositivo con la seguridad necesaria para su traslado al laboratorio, si es necesario bolsas antiestáticas, bolsa de burbujas o cajas selladas y rotuladas para el traslado, tomando todos los cuidados necesarios.

Una vez llevado desde el lugar de recojo y antes de pasar al laboratorio, se debe realizar anotaciones de su ingreso al área de almacenamiento momentánea donde esta área debe cumplir con características que no pongan en riesgo la evidencia, además se debe tener una bitácora de anotaciones de cada ves que se realiza una retirada de la evidencia para análisis con las

características del traslado y personal a cargo. La documentación de la cadena de custodia debe contener todos los lugares por donde ha pasado la evidencia y quien ha realizado su transporte y acceso.

### 3.2.5 Análisis de las evidencias

La fase de análisis es la medula espinal del trabajo del informático forense, es donde se establece la absolución de preguntas realizadas de quien causo, como lo causo, que afecto y como se puede evitar. En esta fase de análisis se debe tener como primera consideración que no se trabaja con los dispositivos o información original, siempre se trabaja con una copia realizada, respetando la normativa del tratamiento de información; al final los resultados obtenidos deben ser verificables y reproducibles para que en cualquier momento se puede montar un entorno donde se pueda reproducir la investigación y mostrar a quien corresponda.

Es importante disponer de una serie de documentos que brinden una información de la evidencia a analizar, por lo tanto, se debe tener:

- El oficio principal donde se detalle el motivo de la intervención y se precise el requerimiento del análisis forense informático.

- Documento de autorización para realizar el procedimiento de identificación de la evidencia y bajo que personal esta realizándose esta acción.

- Documentos relacionados a hallazgos, recojo, recopilación o adquisición, entrega y recepción de evidencia para la cadena de custodia.

- Documento de lacrado y rotulado de la evidencia.

- Documento de autorización por parte de la entidad u organización afectada para el tratamiento de la información, de no ser así resolución judicial de autorización.

- Documento de traslado de la evidencia del almacén al laboratorio para su análisis.

En esta fase debemos tener claro que existen diferentes tipos de procesos de acuerdo a la evidencia a tratar y que cada uno se debe analizar de forma distinta, no obstante, teóricamente se puede presentar la idea de cómo desarrollar el análisis, pero en la práctica se debe diferenciar la herramienta que se debe utilizar para cada tipo de análisis. En todo caso se debe tener las siguientes precisiones para la realización del análisis de las evidencias.

a) Preparación del entorno de trabajo de acuerdo a la evidencia
   Antes de realizar el análisis, propiamente dicho, se debe preparar el ambiente para esta actividad, debido a que se tienen 2 opciones de trabajo, tanto un análisis en caliente o un análisis en frio de la evidencia.

   - Análisis en caliente: se realiza el análisis sobre un dispositivo original, teniendo cuidado que no se realice alguna adulteración sobre este, para momentos en que es importante no apagar la ejecución del incidente, de esta forma se evalúa la gravedad del ataque, también se debe recordar en no realizar adulteraciones a un disco o memoria para lo cual este solo lo tendremos en modo lectura.

   - Análisis en frio: esta opción resulta ser la mas atractiva debido a que se trabaja con una imagen realizada del dispositivo (información contenida), para esta situación nos facilita siempre

tener más de una copia del disco, para lo cual se puede montar la imagen y verificar en laboratorio lo suscitado.

b) Reconstrucción de la línea temporal de los hechos sucedidos
Se debe crear una línea de tiempo donde se ubiquen los hechos o acontecimientos que han tenido lugar en el equipo desde sus inicios, para lo cual se debe tener presente lo siguiente:

- Se debe tener los tiempos MACD de los archivos, detallando las fechas de modificación, acceso, cambio y borrado en cada caso que sea necesario.

- Determinar en los registros las modificaciones establecidas, detallando también la fecha de instalación del sistema, los archivos temporales que se tienen para registro de actividades.

- Determinar los usuarios creados en el caso de un sistema operativo, cuando fueron creados, perfiles, modificaciones y corroborar con la descripción mencionada por parte del encargado del equipo.

- Localizar los programas instalados y los que han tenido cambios en el sistema, algunos programas no utilizan la ruta tradicional de instalación o son instalados por defecto en otros espacios.

- No todos los archivos van a estar a la vista, algunos archivos se van a encontrar ocultos, borrados o archivos con técnicas de esteganografía, de esta forma es necesario verificar las extensiones de los archivos que resulten extrañas.

- Los archivos borrados del disco, mientras no se haya sobrescrito en las secciones donde se encontraban se pueden recuperar a través de herramientas especializadas, posiblemente se encuentren indicios necesarios para trazar la línea temporal.

c) Determinación de los procesos realizados por parte del atacante

Para determinar cómo actuó el atacante se debe examinar los procesos, la memoria y los programas que se estaban ejecutando, si bien en primer plano, también en segundo plano, con esto se puede definir que procesos se ejecutan y que librerías se ven involucradas, normalmente se deben verificar todos los procesos, pero también aquellos que pueden ser inofensivos, habituales y legítimos del sistema. Debido a que en ocasiones se camuflan con nombres muy parecidos a otros para pasar desapercibidos; estos hechos también nos pueden ayudar con los logs de cada sistema o enlaces a direcciones de internet, dando pistas de qué forma se realizó el ataque.

d) Identificación de la raíz de los hechos

Para poder realizar la identificación de la raíz de los hechos aparte de verificar la memoria a través de su volcado, también se verifica las conexiones abiertas, puertos empleados; con esto se puede relacionar el origen de los hechos a través de alguna dirección que realizo algún envió de información, con esta información obtenida se debe ser cauto debido a que se debe corroborar todo hallazgo para tener certeza.

En este punto se puede determinar cómo fue el accionar, como se realizó el ataque o de donde provino, cabe resaltar que acá podemos hacer mención a posibles ataques o capaz malas configuraciones establecidas, de acuerdo a esto se puede dar un alcance del impacto causado a través de esta amenaza.

e) Evaluación de la amenaza con el impacto causado

A la larga todo incidente ocurrido en un dispositivo conlleva un importe económico de gasto, que debe ser cubierto por la entidad, organización o la persona afectada; además se genera tiempo de inutilización si el incidente conlleva a la clausura de un servicio o un bien, retrasó de las actividades cuando no se tenga un plan de contingencia, además también se puede identificar el filtrado de información, la mala utilización de información privilegiada, datos hurtados que puedan generar daño a la reputación de la entidad.

### 3.2.6 Redacción de informes

En esta última fase del análisis forense, queda la redacción del documento donde se informa sobre todos los hallazgos, antecedentes del evento, los procedimientos realizados, el método seguido por el técnico en el análisis y las conclusiones e impacto que se ha generado de todo el incidente suscitado.

Para la redacción de informes se debe tener en cuenta dos tipos de informes necesarios para la culminación de todos los procesos aplicados, el informe técnico y el informe ejecutivo, la diferencia de estos informes se basa en el grado de detalle en que se exponen los asuntos.

a) Informe ejecutivo

Informe elaborado para personas no comprendidas en la materia, este debe ser claro, preciso y sin tecnicismos, evitando terminología propia del campo de informática forense o computacional, expresiones confusas para el público, se debe recordar que este informe está pensado en los fiscales y jueces, quienes deben tener una versión clara de los hechos.

Este tipo de informe será un resumen de todas las actividades realizadas con las evidencias digitales, debiendo contener al menos los siguientes aspectos mencionados en el Cuadro 3.1:

*Cuadro 3.1: Detalles del informe ejecutivo. Fuente: Elaboración propia*

| | |
|---|---|
| Explicación de los motivos de la intrusión por el atacante. | Explicación de porque se produjo el incidente, el motivo del atacante. |
| | Cuál era la finalidad del atacante para ocasionar este incidente. |
| Explicación sobre cómo se desarrolló la intrusión por parte del atacante. | Como se logró el acceso por parte del atacante. |
| | Cuáles fueron los cambios realizados en el sistema. |
| Resultados del análisis establecido a las evidencias. | Explicación de lo sucedido por parte del análisis técnico. |
| | Determinación de os daños causados, producidos o que se iban a producir. |
| | Interpretación con causalidad legal en el marco de la legislación jurídica. |
| | Explicación del o los autores implicados en el suceso. |
| Recomendaciones sobre el trabajo. | Cuáles son las acciones a realizar después del incidente. |
| | Recomendaciones para la protección de los equipos ante alguna anomalía similar. |

b) Informe técnico

Este informe es elaborado para personal con conocimiento sobre la materia, se debe detallar todos los hechos realizados, procedimientos a seguir, programas utilizados, técnicas empleadas, descripción paso a paso de lo realizado.

A diferencia del informe ejecutivo, el informe técnico debe ser más extenso y con mayor contenido de detalle, sobre todo en el análisis realizado a profundidad y los hallazgos encontrados, presentando en el Cuadro 3.2 algunas características a tener en cuenta:

*Cuadro 3.2: Detalle del informe técnico. Fuente: Elaboración propia*

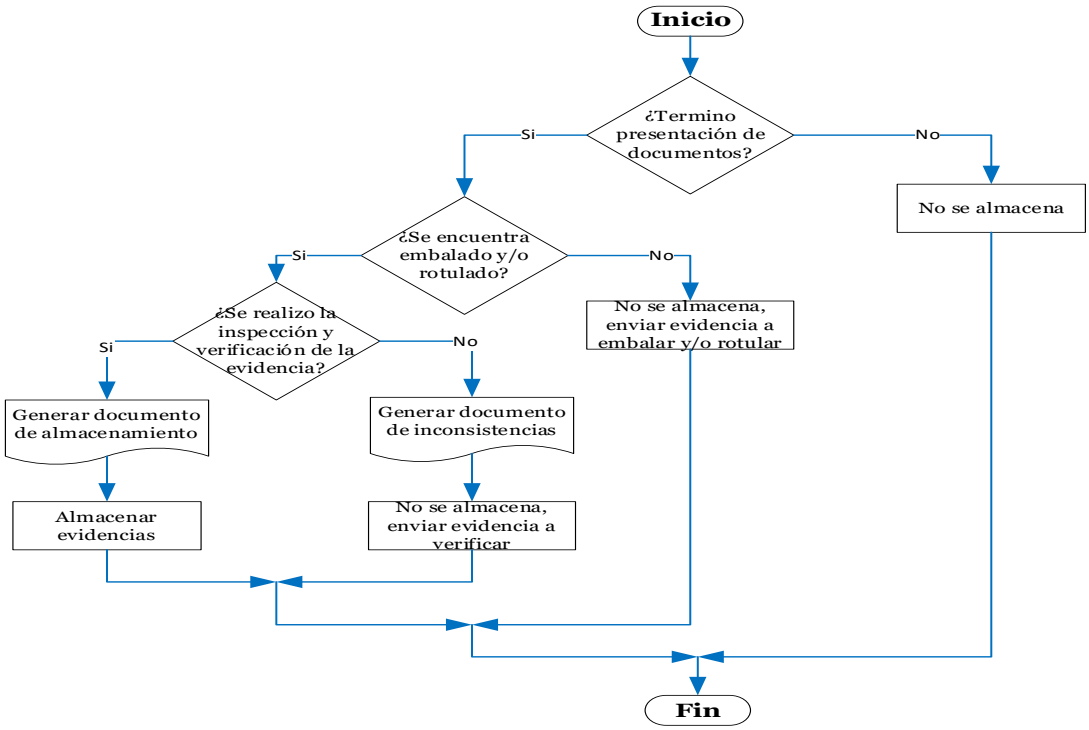
| | |
|---|---|
| Antecedentes del incidente. | Se debe detallar la situación antes de la ocurrencia y cuál era el normal funcionamiento, describir el área donde se realizó el incidente. |
| Identificación de evidencias. | Detallar sobre el inicio de la investigación, características del equipo, identificadores de cada evidencia, características de la situación encontrada. |
| Recolección o adquisición de datos. | Cuáles son las evidencias recolectadas y como se llevó a cabo el proceso, quien estuvo a cargo en la realización de la actividad y medidas tomadas para preservar la evidencia. |
| Descripción de la evidencia encontrada. | Detalle sobre la evidencia encontrada, contenido, estado, contenido, características, identificador entre otros. |
| Trabajos realizados en el laboratorio durante el análisis. | Que herramientas se han empleado, detalle del procedimiento empleado y la funcionalidad de la herramienta, detalle de cada paso realizado; informando sobre las características del dispositivo analizado, sistema operativo, aplicaciones que se encuentre, procesos en ejecución, vulnerabilidades detectadas y metodología utilizada. |
| Presentación de los resultados. | Presentar la herramienta utilizada por el atacante, el alcance e impacto ocasionado por el incidente, mencionar el origen del ataque y cómo fue posible el hallazgo y reconocimiento. |
| Detallar la línea temporal de los eventos ocurridos durante el ataque y el análisis de la evidencia, apoyándose en las tomas fotográficas realizadas. | |
| Las conclusiones elaboradas deben ser de carácter técnico, con vías a causar concientización para una mejora de posibles eventos futuros. | |
| Las recomendaciones deben estar basadas en las vulnerabilidades explotadas por el atacante, para no volver a repetir el incidente o consideraciones legales sobre estos hechos. | |

## 3.3 Trabajos posteriores

Los trabajos posteriores se basan en el almacenamiento de la evidencia una vez terminados la presentación de los informes para ser utilizados en un argumento legal, este almacenamiento es necesario para tener una disponibilidad de la evidencia posteriormente se pida la revisión de los hallazgos encontrados por los especialistas en materia de informática forense.

A diferencia de otras modalidades, las evidencias digitales deben tener un campo de almacenamiento digital, específico para volúmenes grandes de información, debido a esto un almacén para evidencia digital seria como un servidor de almacenamiento de datos, donde se guarden cada documento, archivo, imágenes de discos, entre otros. Para lo cual se debe establecer un área específica para preservar toda la evidencia hasta pasado tres años después de ser presentada, posterior a esto se procederá a destruir la evidencia almacenada, este tiempo es esencial debido a que toda evidencia digital siempre tiende a ser de gran volumen. Presentado en la Figura 3.9 un procedimiento para su trabajo.

*Figura 3.9: Etapas de los trabajos posteriores. Fuente: Elaboración propia*



# 4 Conclusiones

## 4.1 Hallazgos

Con la realización de esta guía se pudo dar una pauta para la realización del análisis forense, no solo pensando en la parte de desenvolvimiento durante la escena del hecho, sino pensando antes y después de esta situación, también se precisa que esta guía puede ayudar de complemento al manual que se tiene por parte de la entidad a cargo del ministerio del interior del estado peruano donde se detallan particularidades para realizar el trabajo pero no se contemplan procedimientos a situaciones que en la actualidad toman una repercusión a las entidades, organizaciones o personas que hacen uso de los medios informáticos. La informática forense es un campo que va en crecimiento debido a que el modo de operación de los delincuentes y su creatividad para mal utilizar su destreza en acciones que perjudican y dañan a las personas hacen necesario la constante capacitación, la generación de ramas específicas para determinados análisis.

## 4.2 Trabajos futuros

Dentro de los trabajos a futuros se puede mencionar que se puede presentar esta guía y llevarla a situaciones variantes como son dispositivos móviles, dispositivos personales (computador de escritorio o laptop), dispositivos servidores, mecanismos en la nube, servicios web, servicios de bases de datos; así mismo se puede generar ramas de esta guía para convertirlo en procedimientos mas detallados, de igual forma se pueden crear manuales de usuarios para suites de herramientas existentes en el mercado, detallar características de un laboratorio forense y como debería estar implementado.

# Referencias

Acost, M., Benavides, M., & Garcia, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89), 351-368. Recuperado el 02 de Julio de 2021, de https://www.redalyc.org/comocitar.oa?id=29062641023

Arnedo Blanco, P. (2014). *Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos*. Valledupar: Universidad Internacional de la Rioja. Recuperado el 13 de julio de 2021, de https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

Carvajal, A. (2007). *Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático*. Bogota, Colombia: Globaltek Security.

Colón Ferruzola Gómez, E., & Cuenca Espinosa, H. (2014). Cómo responder a un Delito Informático. *Revista Ciencia Unemi, 7*(11), 43-50. Recuperado el 03 de Julio de 2021, de https://www.redalyc.org/articulo.oa?id=582663858004

Creutzburg, R., Sánchez Briseño, M. M., & Flores Oyervides, J. C. (2016). *Seguridad Informática y Análisis Forense Digital*. Brandeburgo, Alemania: Techniche Hochschule Brandeburg. Recuperado el 13 de julio de 2021, de https://www.researchgate.net/publication/303974058_Seguridad_Informatica_y_Analisis_Forense_Digital

El Peruano. (22 de octubre de 2013). Ley de delitos informáticos. *Ley N°30096*, págs. 505484 - 505488. Recuperado el 13 de julio de 2021, de https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Flores Flores, I., & Vargas Peña, L. (2016). Informática Forense. *Revista Investigación y Tecnología, 4*(1), 105-110. Recuperado el 02 de Julio de 2021, de http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S2306-05222016000100015&lng=pt&nrm=iso&tlng=es

García Dahinten, C. R. (2014). *Cadena de custodia Digital de las evidencias para la Realización de un peritaje*. Guatemala: Universidad de San Carlos de Guatemala. Recuperado el 15 de julio de 2021, de http://biblioteca.usac.edu.gt/tesis/08/08_0755_CS.pdf

Gavilanes Molina, A. F. (2017). *Guía Metodológica para el Peritaje Informático aplicado a los laboratorios de computación de la universidad tecnológica "Indoamérica"*. Quito, Ecuador: Universidad Tecnológica Equinoccial. Recuperado el 15 de julio de 2021, de http://repositorio.ute.edu.ec/bitstream/123456789/21397/1/69203_1.pdf

Gervilla Rivas, C. (2014). *Metodología para un Análisis Forense*. Catalunya, España: Universitat Oberta de Catalunya. Recuperado el 17 de julio de 2021, de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

Guerrero Paiva, A. (2009). Informática forense y sus beneficios. *Revista de Información, Tecnología y Sociedad*(3), 105-107. Recuperado el 02 de Julio de 2021, de http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442009000200025&script=sci_arttext

Hidalgo Cajo, I. M., Yasaca Pucuma, S., Lema Ayala, L. Á., & Hidalgo Cajo, B. G. (2018). *Informática Forense*. Riobamba, Ecuador: Escuela Superior Politécnica de Chimborazo.

López Delgado, M. (2007). *Análisis Forense digital*. Madrid, España: Hackers & Seguridad.

Mamani Quisbert, D. J. (2013). Fases de un ataque Hacker. *RITS, 8*, 70-71. Recuperado el 14 de julio de 2021, de http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442013000100029&lng=es&nrm=iso

Naranjo Gómez, V., Mendoza Pérez, J., de la Caridad Alonso Betancourt, E., & Hinojosa Calzada, J. S. (2020). Informática criminalística: una especialidad en desarrollo. *Opinión Jurídica, 19*(38), 245-257. doi:https://doi.org/10.22395/ojum.v19n38a12

Pedreros Martínez, W. L., & Suárez Urrutia, J. C. (2016). *HERRAMIENTAS APLICADAS EN EL DESARROLLO DEL ANÁLISIS FORENSE INFORMATICO EN COLOMBIA*. Bogotá, Colombia: Universidad Militar Nueva Granada. Recuperado el 15 de julio de 2021, de https://repository.unimilitar.edu.co/bitstream/handle/10654/14395/SuarezUrrutiaJenniferCatherine2016.pdf?sequence=1&isAllowed=y

Rafael Iglesias, L. (2015). *Herramientas Open Source para Informática Forense*. Buenos Aires: Universidad de Buenos Aires. Recuperado el 8 de julio de 2021, de http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-0187_IglesiasLF

Silva, N., & Espina, J. (2006). Ética Informática en la Sociedad de la Información. *Revista Venezolana de Gerencia, 11*(36), 559-580. Recuperado el 02 de Julio de 2021, de http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1315-99842006000400004&lng=es&tlng=es

Vega Velasco, W. (2008). POLITICAS Y SEGURIDAD DE LA INFORMACION. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia, 2*(2), 63-69. Recuperado el 02 de Julio de 2021, de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008&lng=es&tlng=es.

Voutssas M., J. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica, 24*(50), 127-155. Recuperado el 02 de Julio de 2021, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=es&tlng=es.

# Bibliografía

Carvajal, A. (2007). *Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático.* Bogota, Colombia: Globaltek Security.

Hidalgo Cajo, I. M., Yasaca Pucuma, S., Lema Ayala, L. Á., & Hidalgo Cajo, B. G. (2018). *Informática Forense.* Riobamba, Ecuador: Escuela Superior Politécnica de Chimborazo.

López Delgado, M. (2007). *Análisis Forense digital.* Madrid, España: Hackers & Seguridad.