ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/340617686

# Definition of a digital evidence acquisition methodology based on international standards

**Article** *in* RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação · May 2020

CITATIONS
0

READS
2,897

**4 authors:**



Anderson Coronel
Francisco de Paula Santander University
**33** PUBLICATIONS **124** CITATIONS
SEE PROFILE



Yesenia Areniz Arévalo
Francisco de Paula Santander University
**21** PUBLICATIONS **114** CITATIONS
SEE PROFILE



Fabián Cuesta Quintero
Francisco de Paula Santander University
**19** PUBLICATIONS **82** CITATIONS
SEE PROFILE



Dewar Rico-Bautista
Francisco de Paula Santander University
**171** PUBLICATIONS **1,150** CITATIONS
SEE PROFILE

All content following this page was uploaded by Dewar Rico-Bautista on 14 April 2020.

The user has requested enhancement of the downloaded file.

ISSN: 1646-9895

# risti

Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

M a i o 2 0 • M a y 2 0



©AISTI 2020 http://www.aisti.eu

Nº E29

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 04/12/2019
Aceitação/Acceptance: 16/02/2020

# Definición de una metodología de adquisición de evidencias digitales basada en estándares internacionales

Luis Anderson Coronel-Rojas[1], Yesenia Areniz-Arévalo[1], Fabian Cuesta-Quintero[1], Dewar Rico-Bautista[1]

**lacoronelr@ufpso.edu.co, yareniza@ufpso.edu.co, fcuestaq@ufpso.edu.co, dwricob@ufpso.edu.co**

[1] Universidad Francisco de Paula Santander Ocaña, Sede Algodonal Vía Acolsure, 546551, Ocaña, Colombia.

**Pages: 266–282**

**Resumen:** El objetivo de este documento es entregar una guía a los investigadores forenses en el momento de la ocurrencia de un crimen informático. De igual forma, que sirva como apoyo académico a estudiantes y personas interesadas en el tema de seguridad informática. El documento detalla las fases de una buena práctica para la identificación, recolección, análisis y realización de informes forenses. Se realizó un análisis de las normas y estándares internacionales existentes y relacionados con la adquisición de datos en medios digitales. Se genera una comparación con las normas y estándares identificados y analizados que permitió el desarrollo de la metodología propuesta.

**Palabras-clave:** Evidencia digital; Análisis forense; seguridad informática; metodologías; delito informático.

## *Definition of a digital evidence acquisition methodology based on international standards*

***Abstract:*** The purpose of this document is to provide guidance to forensic investigators at the time of the occurrence of a computer crime. Likewise, to serve as academic support to students and people interested in the subject of computer security. The document details the phases of a good practice for the identification, collection, analysis and realization of forensic reports. An analysis of existing international norms and standards related to data acquisition on digital media was carried out. A comparison with the norms and standards identified and analyzed was generated, which allowed the development of the proposed methodology.

***Keywords:*** Digital evidence; Forensic analysis; computer security; methodologies; cybercrime.

## 1. Introducción

El proceso de adquisición de evidencias digitales debe ser legalmente aceptable, apoyándose en métodos científicos que permitan recolectar, analizar y validar las mismas, recurriendo entonces a la Informática Forense (Fennema et al., 2017). Por tal motivo, es importante saber que la Informática Forense es una disciplina que se desprende directamente de una serie de sucesos que han afectado a la sociedad globalizada e informatizada de fines del siglo XX y principios del XXI, en donde se observa el auge de una serie de delitos que están afectando diferentes áreas de la sociedad (Darahuge & Arellano González, 2011). En este contexto se propone para el desarrollo del TFM realizar una comparación y estudio de las diferentes normas y estándares internacionales de metodologías para la adquisición de evidencias digitales, y a partir de esto, construir una metodología clara y concisa que ayude a la recolección de evidencias digitales relevantes para llevar a cabo un análisis forense en cualquier organización (Dale & Meyer, 2006).

La informática forense es un área muy interesante debido a que, gracias a ella, a sus metodologías, estándares y normas se puede identificar lo que sucedió en un lugar determinado donde haya existido un crimen informático como por ejemplo en una organización, permitiendo recolectar, analizar, preservar y presentar las evidencias digitales necesarias que sirvan de prueba para demostrar lo acontecido en la escena del crimen. Actualmente existe en el mercado muchas herramientas como software y aplicaciones para la recolección de evidencias digitales en caliente o en frio, donde cada una de esas herramientas posee funciones y características muy relevantes que ayudan a la recolección de toda la evidencia digital de una manera eficiente y eficaz que puede llegar a determinar los causantes del crimen informático. Por tal motivo, el desarrollo de este trabajo buscó una comparación entre las diferentes metodologías de recolección de evidencia digital y con base en esto, proponer una metodología clara que contribuya con fases y pasos que se deben tener en cuenta en el momento de realizar una recolección de evidencia digitales, con el fin de determinar lo sucedido en la escena del crimen y por otro lado que esta investigación sirva de apoyo en la formación académica (Lobo-Parra et al., 2019; Rueda-Rueda et al., 2019; Rueda & Rico-Bautista, 2016).

Hoy en día se ha visto como las organizaciones han venido en total crecimiento en cuanto a las tecnologías de la información y comunicaciones (Arévalo Ascanio et al., 2015; Y. C. Medina-Cárdenas & Rico-Bautista, 2009, 2016; Y. Medina-Cárdenas & Rico-Bautista, 2008, 2012; Rico-Bautista et al., 2015), con el fin de agilizar los procesos y de mejorar el servicio que prestan a la ciudadanía, por tal motivo su información está expuesta a personal interno o externo que buscan por algún motivo robarla o destruirla por un fin particular o colectivo, por eso es importante salvaguardarla y evitar que esto suceda, es así que en la medida en que una organización aumente en la implementación de tecnologías de la información y comunicaciones (Rico-Bautista et al., 2019), aumentará también la cantidad de ciberataques que se pueden presentar. De acuerdo con (Diero, 2019), por lo menos cada 4 de 10 empresas de américa latina han sufrido ciber ataques en los últimos años. Esto demuestra que la mayoría de ataques que se han venido

presentando en los últimos años han sido provocados a organizaciones. Por lo anterior, se evidencia que muchas organizaciones han sufrido pérdida de información relevante y por eso se han venido desarrollando metodologías y aplicaciones que contribuyan al análisis, evaluación y descubrimiento de quién ha causado dicho delito. De igual manera, es fundamental comparar las diferentes normas y metodologías existentes para el análisis de las evidencias digitales con el fin de seguir construyendo nuevas metodologías más eficaces que ayuden a las organizaciones a identificar los delitos informáticos dentro de su organización. Hoy por hoy, muchos estudios demuestran que las organizaciones son atacadas a diario por delincuentes que sólo quieren llevarse su información con fines particulares o colectivos, por tal motivo es importante desarrollar o implementar metodologías que identifiquen los escenarios del crimen informático que se ha presentado en la organización. Es así que existen diferentes metodologías y estándares que orientan a los encargados del área de informática y conocedores del tema de evidencias digitales y análisis forense a implementarlas teniendo en cuenta cada una de las fases.

El resto del artículo está dividido cinco secciones. En la sección dos se presenta la revisión de la literatura. En la sección tres se presenta la metodología propuesta, la cual consta de siete fases. En la sección 4 se presentan las conclusiones y el trabajo futuro.

## 2. Revisión de la literatura

Es importante empezar por definir el concepto de ciencia forense, que de acuerdo con (Kent et al., 2006), es la aplicación de la ciencia al derecho. Mientras que la ciencia forense digital, también conocida como ciencia forense informática y de redes, tiene muchas definiciones. Por su parte, la computación forense es definida en el NIST (National Institute of Standards and Technology) (Kent et al., 2006), como la aplicación de la ciencia a la identificación, recopilación, examen y análisis de datos, al tiempo que se preserva la integridad de la información y se mantiene una estricta cadena de custodia de los datos (Ochoa Arévalo, 2018). En tal sentido, el análisis forense informático, se podría decir que es “la forma de aplicar los conceptos, estrategias y procedimientos de la criminalística a la tecnología digital, con el fin de apoyar a la justicia en su lucha contra la delincuencia y el crimen, o como recurso especializado en esclarecimiento de incidentes de seguridad informática” (López Delgado, 2007). Según (National Institute of Justice, 2001), la evidencia digital es información y datos de valor para una investigación que se almacena, recibe o transmite a través de un dispositivo electrónico. Estas pruebas se adquieren cuando se incautan datos o dispositivos electrónicos y se aseguran para su examen.

Es así que las pruebas digitales, están latentes, como las huellas dactilares o la evidencia de ADN, cruza las fronteras jurisdiccionales de forma rápida y fácil, se altera, daña o destruye fácilmente y puede ser sensible al tiempo. Todos estos conceptos han surgido a través de los tiempos y a la par con el avance de la tecnología en sí. Son términos similares en su definición, pero han sufrido cambios que tienen que ver con el contexto. Es evidente, que se trata de conceptos que tienen un fin común y es el de almacenar, examinar, analizar y proteger la información. El departamento de justicia de los Estados Unidos publicó la guía “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition”, la cual tiene como objeto asistir a los equipos de primera

respuesta los cuales son los responsables de la identificación, recopilación / adquisición y protección de la evidencia digital (Ochoa Arévalo, 2018). Esta guía cubre las fases de:

- Documentación de la escena: abarca las actividades de fijación fotográfica y etiquetado de la evidencia que permita recrear la escena posteriormente. La documentación debe incluir el tipo, localización, posición de los equipos, componentes, periféricos, etc.
- Recopilación de evidencia: de manera que se mantenga la integridad de la evidencia, el equipo de primera respuesta debe documentar todas las actividades en los computadores, periféricos, etc.; también proporciona guías para el tratamiento de los equipos cuando estos estén encendidos o apagados.
- Preservación de la evidencia: al ser la evidencia digital frágil por naturaleza, se requiere un proceso para el empaquetado que incluya elementos como documentado, etiquetado e inventario y uso de paquetes antiestáticos; en cuanto al transporte, considerar que la evidencia digital no debe ser expuesta a campos magnéticos y siempre hacer uso de la cadena de custodia de toda la evidencia trasportada.

Toda la evidencia digital es cualquier tipo de información que se puede obtener en el lugar del crimen que tenga valor probatorio almacenada o trasmitida de forma digital. La evidencia digital se puede clasificar en dos tipos: *Volátil*, hace referencia a información temporal, como la que reside en la memoria principal (RAM) y *No volátil*, hace referencia a memoria permanente tales como discos duros, usb's, cd's, etc.; esta información se mantiene cuando se apaga el equipo. De acuerdo con (Coronel Tapia, 2018), la ISO/IEC 27037, proporciona guías para actividades específicas en el manejo de evidencia digital, dichas actividades hacen referencia a la identificación, recolección, preservación de evidencia digital potencial. Además, provee guías para: Medios de almacenamiento usados en computadores estándares, dispositivos móviles, sistemas móviles de navegación, computadores estándares y conexiones de red y redes basadas en los protocolos TCP/IP y otros. El término evidencia digital de acuerdo con la ISO/IEC 27037 (2012), se conoce como "información o datos, almacenados o transmitidos de forma binaria que pueden ser tomados en cuenta como evidencia o prueba."

Así mismo, la ISO 27037:2012; guidelines for identification, collection, acquisition, and preservation of digital evidence (ISO, 2012). Define lo siguiente:

- Identificación. Involucra el reconocimiento y documentación de evidencia digital, se pone énfasis en la consideración del orden de volatilidad de manera que se proteja la evidencia.
- Recopilación de evidencia. Consiste en remover la evidencia de su origen a laboratorio o sitio seguro. Es importante considerar si el equipo se encuentra encendido o apagado, de manera que se tomen en consideración las actividades a ser ejecutadas y las herramientas a ser usadas.
- Adquisición. Es realizar una imagen (copia) de los dispositivos que mantienen evidencia digital, se establecen las actividades y herramientas de manera que el proceso sea lo menos intrusivo y finalmente se debe mantener la documentación completa.

- Preservación. Involucra la salvaguarda de la potencial evidencia digital, la preservación debe mantenerse durante todo el proceso. Uno de los componentes claves dentro del proceso es la cadena de custodia la cual inicia las actividades de adquisición y/o recopilación.

Por su parte, la ISO/IEC 27042, provee guías en el análisis y la interpretación de la evidencia digital, de forma que se logre garantizar o abordar cuestiones de continuidad, validez, reproductibilidad y repetitividad (Arévalo Ascanio et al., 2015; Y. Medina-Cárdenas et al., 2019). Contiene, además, buenas prácticas para la selección, diseño e implementación de un proceso analítico y recoge suficiente información que permita que dichos procesos puedan ser sometidos a escrutinios independientes cuando sea necesario. En resumen, este estándar provee un marco común, para lidiar con incidentes en sistemas de seguridad analizando e interpretando los elementos propios del incidente (IsecT Ltd, 2019). En ese mismo sentido, surgen la UNE 71505 y UNE 71506, estas normas publicadas por la Asociación Española de Normalización y Certificación tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales. Según la asociación, esta norma debe dar respuesta a las infracciones legales e incidentes informáticos en las distintas empresas y entidades. Con la obtención de dichas pruebas digitales, que serán más robustas y fiables siguiendo la normativa, se podrá discernir si su causa tiene como origen un carácter intencional o negligente. Estas normativas son de aplicación a cualquier organización con independencia de su actividad o tamaño, así como a cualquier profesional competente en este ámbito. Se dirige especialmente a incidentes y seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas. (Rivas, 2014)

La RFC 3227 (Brezinski, 2002), proporciona las directrices para la recopilación y almacenamiento de evidencia. Dentro de las fases y actividades más importantes se destacan:

- Recopilación de evidencia: se debe considerar listar los sistemas involucrados en el incidente de manera que se cuente con una perspectiva de cuál es la evidencia que debe ser recolectada. Así mismo, considerar elementos como: generar una imagen del sistema lo más precisa posible, documentar cada acción que se ejecute, considerar el orden de volatilidad en la adquisición, iniciar desde lo más volátil (registros y contendidos del cache) al menos volátil (documentos). También proporciona guías de situaciones que se deben evitar, como lo son: apagar el equipo, confiar en la información que proporcionan los comandos del sistema, etc.
- Preservación de evidencia: se pone especial énfasis en la cadena de custodia y el almacenamiento de información en dispositivos con seguridad demostrada y que permitan control de acceso. (Ochoa Arévalo, 2018)

Pedreros Martínez & Suárez Urrutia (2016), en su investigación explican el uso de las herramientas que utilizan los expertos forenses en materia digital para dar con los intrusos y poder conocer a ciencia cierta qué ataque fue cometido en el sistema de información y sus posibles consecuencias para aquellas personas o entidades que han sufrido ataques mal intencionados. Estas herramientas ayudan a priorizar y a realizar tareas, facilitan e identifican las causas que afectaron el sistema, igualmente se seguirán

desarrollando herramientas bastante sofisticadas que vayan en contra de los análisis forenses que intentan no dejar rastros, borrar u ocultar información esencial a la hora de llevar a cabo las tareas in situ por parte del perito o investigador, de tal manera que se dificulte o posibilite el vencimiento de términos en un determinado proceso ya sea este administrativo o judicial, se habla de esa fracción de tiempo de que dispone un fiscal para presentar dichas pruebas ante un juez que lleve el caso. Se puede evidenciar que hay un sinnúmero de guías, normas, estándares que buscan presentar directrices para llevar a cabo una adecuada identificación, recopilación, adquisición y preservación de evidencias digitales que garanticen un adecuado tratamiento a las mismas. Todas estas normas de respaldo internacional, con la experiencia de muchas organizaciones que han demostrado tener éxito en la aplicación de estas buenas prácticas.

A continuación, se presentan los estándares más representativos relacionados con la adquisición de evidencias digitales en un análisis forense:

**ISO/IEC 27037:2012.** Esta guía proporciona una serie de directrices que nos orientan en la identificación, recolección, adquisición y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos, para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones (ISO, 2012). A diferencia de la RFC 3227, la norma ISO/IEC 27037 hace referencia a componentes tecnológicos más avanzados y tiene esta característica en cuenta en el desarrollo de la misma (Navarro Clérigues, 2016), (Roatta et al., 2017).Este estándar internacional intenta proporcionar una directriz para aquellos individuos responsables de la identificación, recolección y preservación de potencial evidencia digital (Caballero Quezada, 2015),(Roatta et al., 2017). En la norma se presenta también el concepto de cadena de custodia, ver figura 1.

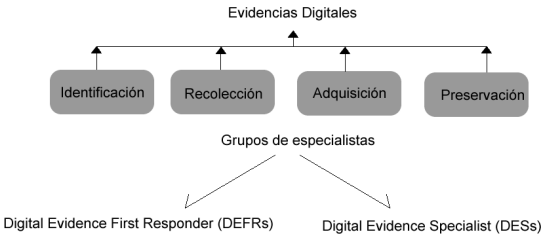



Figura 1 – ISO/IEC 27037:2012.

**ISO/IEC 27042:2015.** Guía para el análisis e interpretación de evidencia digital. Esta guía fue publicada en junio de 2015 y Proporciona orientación sobre el análisis e interpretación de la evidencia digital de una manera que aborda los problemas de continuidad, validez, reproducibilidad y repetibilidad. Encapsula las mejores prácticas para la selección, diseño e implementación de procesos analíticos y registra información suficiente para permitir que dichos procesos sean sometidos a un escrutinio independiente cuando sea necesario (ISO, 2015), (ISO, 2019), (Navarro Clérigues, 2016). Finalmente, recoge las competencias de los peritos forenses: formación, aprendizaje, habilidades, objetividad y ética profesional, ver figura 2.

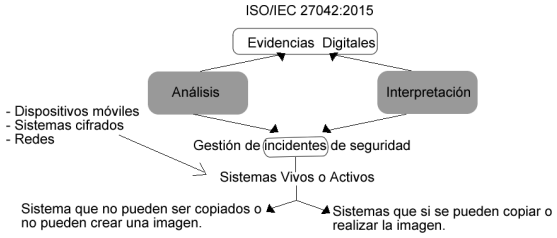



Figura 2 – ISO/IEC 27042:2015.

**Instituto Nacional de Estándares y Tecnología (NIST).** Esta metodología está enfocada especialmente a todo el análisis forense de las evidencias digitales, el objetivo relevante del análisis es el de obtener una mejor comprensión del caso a investigar, encontrando y analizando los hechos relacionados a este caso (Cajo et al., 2018). La NIST tiene como misión promover la innovación y competitividad industrial mediante la medición avanzada de la ciencia, estándares y tecnología, de forma que se mejore la seguridad económica y la calidad de vida. (Cruz Vela, 2016), ver figura 3.

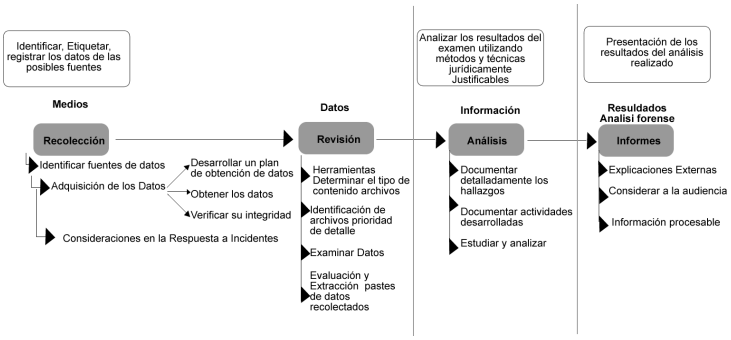



Figura 3 – Instituto Nacional de Estándares y Tecnología (NIST).

**Departamento de Justicia de Estados Unidos.** El departamento de justicia de los Estados Unidos publicó la guía "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition", la cual tiene como objeto asistir a los equipos de primera respuesta los cuales son los responsables de la identificación, recopilación / adquisición y protección de la evidencia digital (Ochoa Arévalo, 2018). Esta guía tiene por objeto ayudar a las fuerzas del orden estatales y locales y a otros equipos de respuesta rápida que pueden ser responsables de la preservación de la escena de un crimen electrónico y el reconocimiento, la recopilación y la salvaguardia de las pruebas digitales (National Institute of Justice, 2001). Las fases de la guía se observan en la figura 4 (Mera Mero & Benavides Córdova, 2018).

**RFC 3227.** La RFC (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 (Brezinski, 2002). Provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones (Rico-Bautista et al., 2016). Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir qué recolectar, desarrollar

la recolección y determinar cómo almacenar y documentar los datos (Veloza, 2017). En cuanto a los principios para la recolección de evidencias destacan básicamente tres, el orden de volatilidad de los datos, las acciones que deben evitarse y las consideraciones sobre la privacidad, así mismo sobre el procedimiento de almacenamiento tiene en cuenta la cadena de custodia de las pruebas recogidas anteriormente y dónde y cómo se deben almacenar estas para que estén a buen recaudo (Rivas, 2014), ver figura 5.

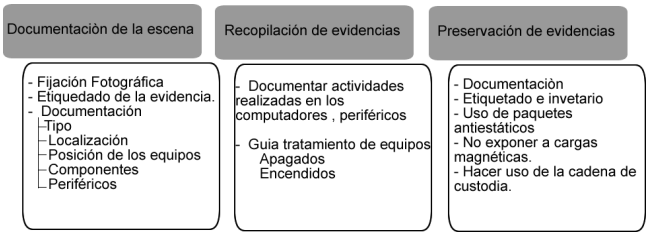



Figura 4 – Fases Guía para equipos de primera respuesta.

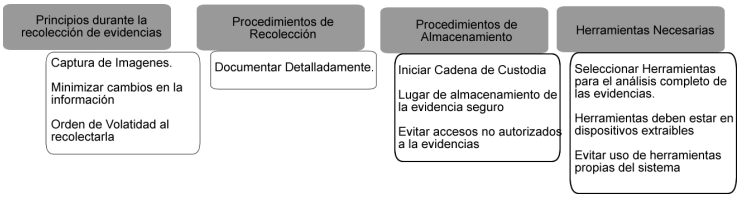



Figura 5 – Puntos de recolección de la información en la RFC 3227.

**UNE 71506:2013.** Según detalla la Asociación Española de Normalización y Certificación (2011) la UNE 71506:2013 fue elaborada por el comité técnico AEN/CTN 71 y consta de 23 páginas. Así mismo, la norma en referencia junto con la UNE 71505, son muy utilizadas por profesionales, organismos, fuerzas y cuerpos de seguridad del estado español; cuyo objetivo es obtener resultados válidos en un proceso forense. La figura 6 muestra las etapas compuesta por la metodología UNE 71506:2013. La UNE 71506:2013 es de aplicación a cualquier organización con independencia de su voluntad o tamaño, así como también como a cualquier profesional competente en éste ámbito (UNE 71506, 2013), (Cajo et al., 2018)

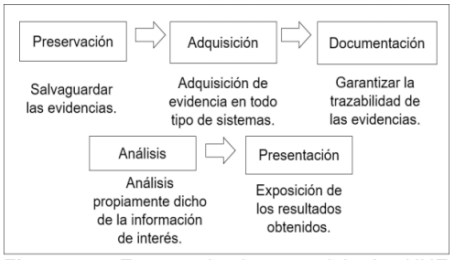



Figura 6 – UNE 71506:2013. Fuente: (Mera Mero & Benavides Córdova, 2018).

Como se puede observar en la tabla 1, cada metodología maneja diferentes fases para la adquisición de evidencias digitales, algunas influyen en todas las fases la identificación, recolección, análisis y presentación y otras incluyen más desglosado cada paso y con más fases para la adquisición de las evidencias digitales.

| Metodología | Fases del Análisis Forense | | | |
|---|---|---|---|---|
| | Identificación | Recolección | Análisis | Presentación |
| Modelo de Casey (versión 2000) | ⏻ | ⏻ | ⏻ | |
| Modelo de Casey (Versión 2004) | ⏻ | ⏻ | ⏻ | ⏻ |
| Modelo publicado por el U.S. Dep. of Justice (2001) | ⏻ | ⏻ | ⏻ | ⏻ |
| Modelo publicado por el U.S. Dep. of Justice (2004) | | ⏻ | ⏻ | ⏻ |
| Modelo de Reith, Carr y Gunsch (2002) | | ⏻ | ⏻ | |
| Modelo de Lee | ⏻ | ⏻ | | |
| Modelo mejorado propuesto por Venansius Baryamureeba y Florence Tushabe. | ⏻ | ⏻ | ⏻ | ⏻ |
| Modelo del DFRWS Forensics Digital Research WorkshoP. (2001) | ⏻ | ⏻ | ⏻ | ⏻ |
| Modelo integrado de Brian Carrier y Eugene Spafford. | | ⏻ | ⏻ | ⏻ |
| Modelo Cohen (2009) | ⏻ | ⏻ | ⏻ | ⏻ |
| SANS Institute Information Security Reading Room | ⏻ | ⏻ | ⏻ | ⏻ |

Tabla 1 – Comparativa de metodologías y sus fases

## 3. Metodología propuesta

La metodología propuesta está compuesta por siete fases, a saber: (i) Fase de Acordonamiento del lugar de los hechos; (ii) Fase de Identificación de evidencias; (iii)

Fase de Adquisición de evidencias; (iv) Fase de Preservación de evidencias; (v) Fase de Examen de evidencias; (vi) Fase de Análisis de las evidencias y (vii) Fase de Informes de Evidencias, como se muestra en la Figura 7.

**Fase 1. Acordonamiento del lugar de los hechos.** Una vez realizada la solicitud del análisis forense, el investigador debe conocer la situación en la que debe trabajar, para eso, es importante que se acordone o se asegure el lugar de los hechos, con el fin de evitar el ingreso de personal no autorizado y la modificación de la escena del crimen. Pasos:

- Se debe acordonar señalando que el lugar del crimen está siendo intervenido por personal especializado en el análisis forense.
- Identificar el incidente que ha sucedido.
- Realizar fotografías al lugar de los hechos, a las pantallas de los equipos de cómputos que se encuentren encendidos.
- Evaluar el entorno, es importante conocer que fue lo que pasó o se sospecha que ha pasado para poder identificar el alcance de la investigación y poder tener claro cuáles son las evidencias más relevantes que sirvan como pruebas para realizarles el análisis correspondiente.
- Escuchar a las personas víctimas o entrevistarnos con personal cercano, esto ayuda a obtener información que puede orientar el rumbo de la investigación.
- Documentar todo lo que suceda dentro de la escena del crimen, recuerde que puede modificarse dicha escena, desconectando la red de datos o apagando forzadamente el equipo de cómputo.

**Fase 2. Identificación de evidencias.** En esta fase es importante tener claro cuáles son las evidencias que se pueden recolectar en la siguiente fase. En la identificación de las evidencias se tiene:

- Identificar las posibles evidencias volátiles o no volátiles
- Documentos de textos electrónicos
- Archivos temporales de navegación
- Todos los registros de eventos del sistema operativo
- Archivos de imágenes o videos.
- Los ficheros de logs
- Pendrive, Unidades de dvd, Discos duros externos, Usb
- Listar los equipos se estén implicados en la escena del crimen.
- Listados de equipos que sin haber sufrido el incidente pueden estar relacionados con el mismo.
- Listado de las personas a que pertenezcan los equipos o que ingresen a la zona investigada.

**Fase 3. Adquisición de evidencias.** Antes de comenzar a la adquisición de las evidencias es fundamental que el investigador forense prepare todo lo relacionado con los procedimientos forenses y el manejo de las pruebas en el momento de adquirirlas, para eso debe tener claro y documentar todo el proceso de extracción de información, de almacenamiento y trasporte, además es necesario saber qué herramientas y equipos forenses debe utilizar. Por esto, se debe identificar e instalar en el equipo forense el hardware y software necesarios para la adquisición de evidencias con base

a las necesidades identificadas. Una vez preparado todo, dentro de la recolección de la información de las evidencias digitales, recuerde que se deben hacer en medios que aseguren la no modificación de las evidencias. Por este motivo, se recomienda que el dispositivo donde se realice la adquisición de las evidencias tenga instalado un bloqueador contra escritura para evitar la modificación. Una vez identificadas en la fase anterior las evidencias a recolectar, se debe tener en cuenta lo siguiente: las evidencias pueden ser recolectadas con el equipo encendido y/o apagado, para eso se debe seguir los siguientes pasos:

- Si el equipo no puede ser apagado recuerde que las evidencias deben ser tomadas en caliente, por lo que es importante la información volátil que tenga en esos momentos el equipo, Cache de la CPU, Tabla de enrutamiento, la cache ARP, lista de usuarios que iniciaron sesión, lista de procesos, memoria RAM, Archivos Temporales, los datos del disco duro, Datos Almacenados remotamente y datos almacenados en dispositivos removibles. Es indispensable tener en cuenta el orden de recolección de evidencia volátil.
- Evitar la utilización de herramientas ya instaladas en el equipo de cómputo, las herramientas deben estar corriendo en dispositivos externos.
- Seleccionar las herramientas relevantes para el análisis completo.
- En caso de que el equipo pueda ser apagado, antes de realizar ese procedimiento se debe identificar si el disco se encuentra encriptado o no, si está encriptado se deben tomar las evidencias en caliente.
- Si el equipo se puede apagar, se puede extraer el disco de almacenamiento.
- Si va a obtener información no volátil la puede recolectar de la siguiente manera: 1) puede hacer un clonado del disco duro, este clonado se hace en un disco externo que tenga la misma capacidad o mayor para evitar la pérdida de la información, recuerde que este clonado se realiza bit a bit del dispositivo físico del equipo que se encuentra en la escena del crimen al disco duro externo o pendrive. 2) El investigador forense también puede adquirir la evidencia como una imagen forense, que es la copia exacta de un dispositivo físico en otro dispositivo capaz de almacenar la imagen forense. Este dispositivo debe tener la misma capacidad o mayor en espacio de almacenamiento, para eso es importante utilizar herramientas que ayuden a crear una imagen forense, una vez realizado cualquiera de estas dos opciones es necesario para mantener la integridad de las evidencias, calcular el hash; es así que, con el hash del disco original y el hash de la copia, se certifica que los dos son idénticos ante un juez, demostrando que las evidencias no han sido manipuladas.
- Si la evidencia es no volátil se debe realizar el etiquetado (Tipo, fecha de recolección identificador)
- Documentar tipo de evidencia, localización de la evidencia y componentes, todo lo que suceda y la información que está siendo recolectada como evidencia digital.
- Una vez recolectada la evidencia esta debe ser trasportada a un lugar adecuado para que continúe con la fase de examen.

**Fase 4. Preservación de evidencias.** Para la preservación de la evidencia se debe tener en cuenta el buen manejo de la misma, ya que si se hace un mal procedimiento

puede ocurrir que se invalide toda la investigación, por no tener el cuidado y los soportes adecuados para la conservación de las evidencias. Por tal motivo es muy importante la cadena de custodia en esta fase, ya que permite realizar un procedimiento controlado y aplicable a las evidencias desde el momento en que son encontradas en la escena del crimen hasta su análisis en los laboratorios o en los equipos forenses que se estén utilizando en la investigación. Esta cadena de custodia debe garantizar la integridad, la autenticidad, la posibilidad de localización donde se encuentra la evidencia, la trazabilidad y por último garantizar la preservación a largo plazo, por tal motivo la cadena de custodia lo que busca es que se evite la manipulación de las evidencias y tener un control sobre todos los dispositivos o elementos obtenidos, es importante tener en cuenta lo siguiente:

- Inicio de la cadena de custodia
- Definir los métodos para garantizar la autenticidad e integridad de las evidencias recolectadas.
- Almacenamiento de la evidencia en dispositivos y lugares seguros.
- En el almacenamiento de la evidencia se debe tener claro la preservación de la integridad para mantener la cadena de custodia.
- Operaciones realizadas (Fecha, hora inicio/final).
- Registro de personas que realicen cualquier operación (fecha, hora de inicio, hora de finalización, nombre y apellidos de la persona que realizó la operación y operación realizada)
- Documentar actividades realizadas.

**Fase 5. Examen de evidencias.** Es esta fase es importante utilizar todas las herramientas necesarias para llevar a cabo el análisis forense y las técnicas adecuadas para examinar los datos recolectados en la fase anterior que fueron identificados como evidencias de pruebas para posterior análisis. En esta fase se busca de una manera profunda las evidencias relacionadas con el crimen. Todos los casos ocurridos siempre son diferentes, por tal motivo para cada caso el examen de las evidencias y los métodos utilizados pueden ser diferentes, el examen siempre que sea posible no se debe realizar a las evidencias originales si no a las copias siempre y cuando no hayan sufrido ninguna modificación alguna en su hash.

**Fase 6. Análisis de las evidencias.** En la fase de análisis se debe interpretar de una manera muy responsable y cuidadosa la información extraída en la escena del crimen y que ya lleva un proceso de identificación, adquisición, recolección, preservación y examen, por tal motivo se deben analizar y estudiar los datos relevantes que sirvan de prueba, identificando las personas, dispositivos, equipos, elementos y acontecimientos para comenzar a determinar las posibles causas del ¿Qué fue alterado? ¿Cómo lo alteraron? ¿Quién realizó la alteración? y quien cometió el crimen informático y de este modo comenzar a armar el rompecabezas que tengan relación con la escena del crimen.

**Fase 7. Informes de Evidencias.** La presentación del informe de las evidencias una vez recolectadas y analizadas se debe hacer ante las personas interesadas los resultados obtenidos. El informe es el proceso con el cual se finaliza el análisis forense y se da a conocer a los interesados, los resultados obtenidos, para eso es importante tener en cuenta:

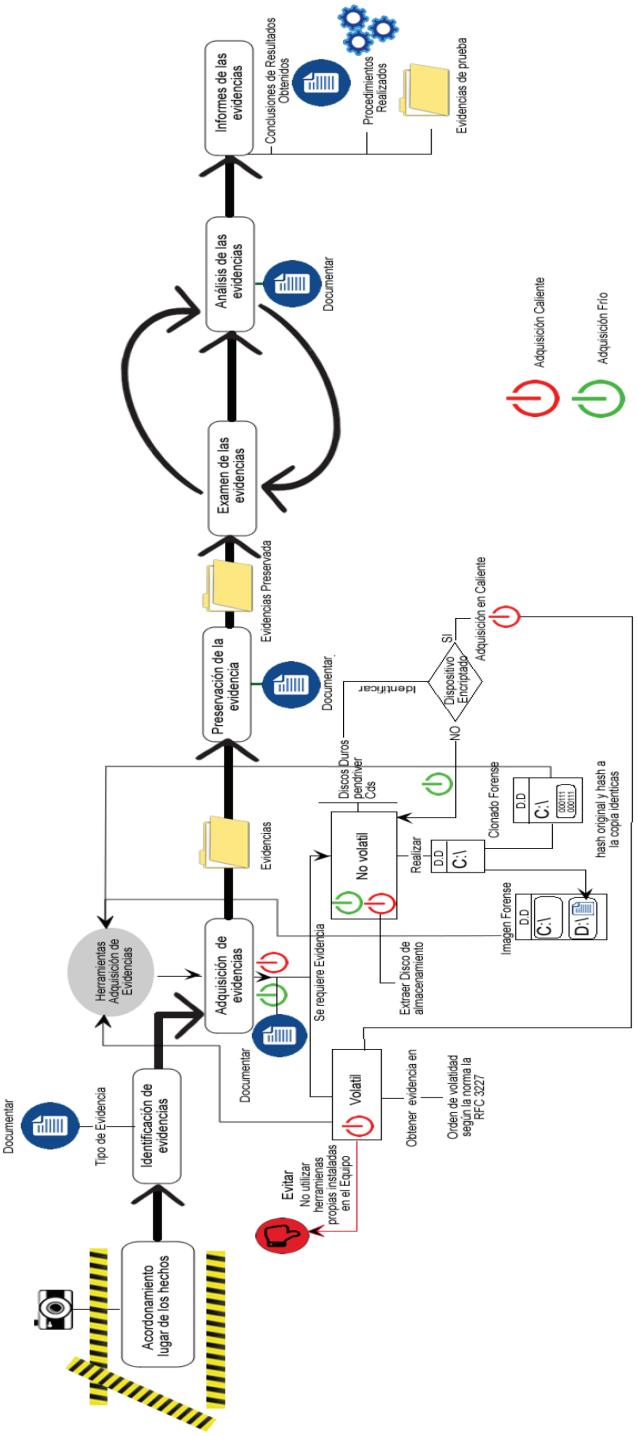



Figura 7 – Metodología Propuesta.

- La descripción del equipo informático o dispositivos tratados en el análisis
- Los procedimientos realizados por el investigador forense y los resultados obtenidos
- Las conclusiones del investigador forense a las cuales ha llegado con base a los resultados obtenidos.

Es muy importante antes de realizar el informe identificar al personal al cual va dirigido, debido a que muchas personas no tienen conocimientos muy técnicos y esto ocasionaría poco entendimiento del mismo. El informe debe estar soportado con el mayor número de evidencias, ya sean físicas o lógicas (fotografías, videos, cds, pendrive, discos duros externos, USB) y cualquier otra evidencia que no pueda ser presentada impresa, se debe tener el soporte y almacenada en un dispositivo electrónico.

Entrando en profundidad en el informe se debe resaltar que es un resumen muy bien explicado de todas las tareas que se llevaron a cabo con el fin de obtener los resultados necesarios que nos lleven a las causas, personas involucradas en el incidente o en la escena del crimen, recuerde que este informe es corto y deberá contener: Datos del investigador forense; Título del informe; Especificar el tipo de informe ejecutivo o técnico; Fecha del informe; Fecha de inicio y fecha de finalización del análisis forense; Una descripción clara de los procedimientos realizados en el análisis forense; Descripción de las evidencias obtenidas y analizadas; Herramientas utilizadas hardware y software; Metodologías usadas; Resultados y conclusiones; Recomendaciones de protección y prevención de nuevos incidentes.

## 4. Conclusiones

Dentro de las herramientas que manejan la filosofía del software libre encontramos una gama de posibilidades que nos posibilitan realizar un análisis forense en un entorno académico. Estás herramientas de fácil adquisición por su disponibilidad para su descarga y uso, su bajo costo es fundamentales en un entorno académico donde los recursos son limitados, donde el proceso se centra en la investigación y aprendizaje. Las guías con las que se dispone a nivel internacional se están quedando cortas debido al ritmo de avance que tienen los dispositivos móviles y la falta de actualización de las mismas por parte de las instituciones que las soportan.

Los modelos forenses estudiados están más orientados al proceso forense en general, a los equipos de cómputo tradicionales y a las redes de comunicación. No se encuentra muchos modelos que estén orientados a los dispositivos móviles. Muchas de estos modelos hacen suposiciones, como, por ejemplo, que el lector conoce el proceso de la cadena de custodia. Lo que dificulta la apropiación de estos criterios por parte de aquellas personas que quieren iniciar en el aprendizaje de esta rama del conocimiento.

## Referencias

Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico-Bautista, D. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Revista Tecnura*, *19*(46), 123. https://doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10

Brezinski, K. (2002). *RFC 3227 Evidence Collection and Archiving*.

Caballero Quezada, A. E. (2015). *Introducción a ISO/IEC 27037:2012*.

Cajo, I. M. H., Pucuna, S. Y., Cajo, B. G. H., Coronado, V. M. O., & Orozco, F. V. S. (2018). Estudio Comparativo De Las Metodologías De Análisis Forense Informático Para La Examinación De Datos En Medios Digitales. *European Scientific Journal, ESJ*, *14*(18), 40. https://doi.org/10.19044/esj.2018.v14n18p40

Coronel Tapia, B. D. (2018). *Metodología para la recolección de evidencia forense generada durante la utilización de aplicaciones desplegadas en entornos web*. 141.

Cruz Vela, E. M. (2016). *Modelo Para El Análisis Y Gestión De Riesgos En Fases Carentes De Técnicas Y Herramientas: Caso Tratamiento De La Evidencia Digital En El Entorno Del Software Libre Utilizando Procesos Unificados*. 137.

Dale, D. B. Van, & Meyer, W. J. (2006). *"Estrategia de la investigación descriptiva" en Manual de técnica de la investigación*.

Darahuge, M. E., & Arellano González, L. E. (2011). *MANUAL DE INFORMÁTICA FORENSE* (Errepar).

Diero. (2019). *No Title*.

Fennema, M. C., Figueroa, L. M., Viaña, G., Lesca, N., & Lara, C. (2017). Tratamiento de Evidencias Digitales Forenses en Dispositivos Móviles. *XIX Workshop de Investigadores En Ciencias de La Computación*, 648–652.

IsecT Ltd. (2019). *ISO/IEC 27042 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*.

ISO. (2012). *ISO / IEC 27037: 2012*.

ISO. (2015). *ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*. *1*, 14.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. *The National Institute of Standards and Technology*.

Lobo-Parra, L. D., Rico-Bautista, D., Medina-Cárdenas, Y., & Sanchez-Ortiz, E. A. (2019). Defining of a practical methodology for the acquisition and analysis of digital evidence in the context of a research post mortem. *RISTI: Revista Ibérica de Sistemas y Tecnologías de La Información*, *E18*, 369–384.

López Delgado, M. (2007). Análisis Forense Digital. *Journal of Chemical Information and Modeling*, *2*, 32. https://doi.org/10.1017/CBO9781107415324.004

Medina-Cárdenas, Y. C., & Rico-Bautista, D. (2009). Modelo de gestión basado en el ciclo de vida del servicio de la Biblioteca de Infraestructura de Tecnologías de Información ( ITIL ). *Revista Virtual Universidad Católica Del Norte*, *27*, 1–21.

Medina-Cárdenas, Y. C., & Rico-Bautista, D. (2016). Alineación estratégica bajo un enfoque organizacional de gestión tecnológica: ITIL & ISO 20000. *Revista Tecnura*, *20*(1), 82–94. https://doi.org/10.14483/22487638.11681

Medina-Cárdenas, Y., & Rico-Bautista, D. (2008). Model of Administration of Services for the Universidad of Pamplona: ITIL. *Scientia Et Technica Scientia et Technica Año XIV*.

Medina-Cárdenas, Y., & Rico-Bautista, D. (2012). Mejores prácticas de gestión para la calidad de los servicios en tecnologías de información. In *Gerencia Tecnológica Informática* (Vol. 11, Issue 29, pp. 47–58).

Medina-Cárdenas, Y., Rico-Bautista, D., & Arevalo-Ascanio, J. G. (2019). Impact of the implementation of ISO 9001 in the university: perception auditor and leader. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2019*(E19), 28–41.

Mera Mero, D. M., & Benavides Córdova, V. M. (2018). *Maestría En Auditoria De Tecnología*. 55.

National Institute of Justice. (2001). Electronic Crime Scene Investigation Guide: A Guide for First Responders. *United States Department of Justice Office of Justice*, 93.

Navarro Clérigues, J. (2016). *Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico*. 148.

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

Pedreros Martínez, W. L., & Suárez Urrutia, J. C. (2016). Herramientas aplicadas en el desarrollo del análisis forense informatico en colombia. *Universidad Militar Nueva Granada*, 71. https://doi.org/10.1017/CBO9781107415324.004

Rico-Bautista, D., Areniz Arévalo, Y., & Medina Cárdenas, Y. C. (2015). La apropiación del direccionamiento estratégico: Una cuestión de competencias organizacionales. *FACE: Revista de La Facultad de Ciencias Económicas y Empresariales*, *15*(2), 71. https://doi.org/10.24054/01204211.v2.n2.2015.1617

Rico-Bautista, D., Guerrero, C. D., Medina-Cárdenas, Y., & García-Barreto, A. (2019). Analysis of the potential value of technology: Case of universidad francisco de paula santander Ocaña. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *E17*, 756–774.

Rico-Bautista, D., Rojas-Osorio, J., & Medina-Cárdenas, Y. (2016). Pentesting empleando técnicas de ethical hacking en redes IPv6. *Revista Ingenio UFPSO*, *11*(1), 79–96.

Rivas, C. G. (2014). *Metodología para un análisis forense*. 1–69.

Roatta, S., Casco, M. E., & Fogliato, M. (2017). *El tratamiento de la evidencia digital y las normas ISO / IEC 27037 : 2012 Resumen Contexto Introducción*. *1*, 6.

Rueda-Rueda, J. S., Rico-Bautista, D., & Florez-Solano, E. (2019). Open Practice Guide for Digital Forensics on Android Devices. *RISTI (Revista Ibérica de Sistemas y Tecnologías de La Información)*, *18*, 442–457.

Rueda, R. J. S., & Rico-Bautista, D. (2016). Defining of a practical model for digital forensic analysis on Android device using a methodology post-mortem. *2016 8th Euro American Conference on Telematics and Information Systems (EATIS)*, 1–5. https://doi.org/10.1109/EATIS.2016.7520109

Veloza, R. (2017). *Análisis forense de malware*. 1–75.



View publication stats