Propuesta de buenas prácticas en la recolección y garantía de integridad de la evidencia digital en el cloud computing

Wilber Gaviria Álvarez

Asesor

Mgtr. Roberto Mauricio Cárdenas Cárdenas

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Maestría en Gestión de Tecnología de Información

2024

Dedicatoria

En honor a mi madre: María Lillyam del Socorro Álvarez Barrera Q.E.P.D, fuente de inspiración, esfuerzo y sacrificio, aunque no te encuentres físicamente, tus sabios consejos me acompañan y guían mi vida para alcanzar mis metas y trazarme nuevos objetivos.

Agradecimientos

A mi familia, a mi esposa Viviana Ortiz, a mis hijos: Wilber Stiven, y Yeison Alejandro, por aportar parte de su tiempo para permitirme dedicarme a las labores que demandó este proyecto, por entender que el aprendizaje debe ser permanente, y darme su apoyo incondicional en la realización y alcance de uno de los objetivos de mi vida.

A mis amigos, compañeros y colegas, por el aporte permanente a este trabajo y al fortalecimiento de la disciplina de informática forense, que día a día nos presenta nuevos retos.

Resumen

El objetivo del presente trabajo es implementar una propuesta de buenas prácticas en la recolección y garantía de integridad de la evidencia digital en el cloud computing, se toma como base la alta demanda de servicios por parte de los diferentes usuarios y empresas que ha llevado a la industria a establecer nuevos modelos de negocio en los cuales hace su aparición el cloud computing, presentando en el ámbito tecnológico la posibilidad de que sus clientes y usuarios accedan de manera remota a software, hardware, almacenamiento y procesamiento de información, razón por la cual la seguridad de la información toma una gran relevancia en este modelo enfrentándose a nuevos desafíos en los que se encuentra garantizar la integridad de la información, tanto para la operación del negocio, como para ser aportada como evidencia digital en los diferentes procesos judiciales a los que haya lugar, es por ello que en esta propuesta se analizaran diferentes publicaciones de organizaciones reconocidas en la aplicación de estas buenas prácticas, lo que nos permitirá realizar un compendio de las mejores, para el diseño de un procedimiento que abarque la preparación, identificación, recolección y/u obtención, preservación y documentación de la evidencia digital, como aporte al garantía de integridad de esta en el cloud computing, propuesta que será puesta a consideración de expertos en la disciplina de informática forense, para que sea evaluada como guía en las actividades que estos desarrollan en la materia.

***Palabras clave*:** Informática forense, Seguridad de la información, Cloud Computing, Evidencia digital, Buenas prácticas.

Abstract

The objective of this work is to implement a proposal of good practices in the collection and guarantee of integrity of digital evidence in cloud computing, based on the high demand for services by different users and companies that has led the industry to establish new business models in which cloud computing makes its appearance. presenting in the technological field the possibility for its customers and users to remotely access software, hardware, storage and information processing, which is why information security takes on great relevance in this model facing new challenges in which it is necessary to guarantee the integrity of information, both for the operation of the business, and to be provided as digital evidence in the different judicial processes that may take place, that is why in this proposal different publications of recognized organizations in the application of these good practices will be analyzed, which will allow us to make a compendium of the best, for the design of a procedure that encompasses the preparation, identification, collection and/or obtaining, preservation and documentation of digital evidence, as a contribution to the guarantee of its integrity in cloud computing, a proposal that will be put to the consideration of experts in the discipline of computer forensics, so that it can be evaluated as a guide in the activities that they develop in the field.

***Keywords*:** Computer forensics, Information security, Cloud computing, Digital evidence, Good practices.

Tabla de Contenido

Introducción 13

Planteamiento del Problema 14

Definición del Problema 14

Objetivos 16

Objetivo General 16

Objetivos Específicos 16

Justificación 17

Marco de Referencia 18

Marco Teórico 18

Sistema de Gestión de la Seguridad de la Información 18

Familia de las Normas ISO/IEC 27000 18

Marco Conceptual 21

Buenas Prácticas *21*

Cloud Computing *21*

Evidencia Digital *22*

Incidente de Seguridad *22*

Integridad *23*

Procedimiento *24*

Seguridad de la Información *24*

Virtualización *24*

Marco Legal 24

Marco Tecnológico 26

Diseño Metodológico 29

Población y Muestra 30

Población *30*

Muestra *30*

Técnicas e Instrumentos de Recolección de Información. *30*

Presentación, Interpretación y Análisis de Resultados 31

Ambientes Cloud 31

Concepto de Nube 31

Desafíos Forenses en la Nube 36

Contexto para Recopilar Evidencia Digital 39

Características de la Evidencia Digital 39

Principios de la Evidencia Digital 41

Computación Forense en la Nube 41

Análisis Forense en la Nube 42

Análisis de la Literatura 43

Estado del Arte de Buenas Prácticas en la Recolección y Garantía de Integridad de la Evidencia Digital en el Cloud Computing 47

RFC 3227 47

Directrices para la Recolección de Evidencias y su Almacenamiento 47

NIST 800-86 48

Guía para Integrar Técnicas Forenses en la Respuesta a Incidentes 48

ADFM 49

Modelo Forense Digital Abstracto 49

ISO 27037 51

Directrices para la Identificación, Recolección, Adquisición y Preservación de la Evidencia Digital 51

EDRM 53

Modelo de Referencia de Descubrimiento Electrónico 53

Propuesta de Buenas Prácticas 55

Preparación 59

Identificación 60

Recolección y/u obtención 62

Preservación 68

Documentación 69

Evaluación de la propuesta 73

Resultados de la Encuesta que Evaluó la Propuesta 74

Conclusiones 90

Recomendaciones 92

Referencias Bibliográficas 93

Lista de Tablas

Tabla 1 *Publicaciones de Organizaciones Reconocidas en Informática Forense* 19

Tabla 2 *Normatividad Colombiana Aplicada a la Evidencia Digital*..... 25

Tabla 3 *Herramientas de Software Forense* 27

Tabla 4 *Características de la Nube según NIST SP800.145*..... 31

Tabla 5 *Modelos de Servicio en la Nube*..... 32

Tabla 6 *Modelos de Implementación de Nube* 35

Tabla 7 *Revisión Bibliográfica de Buenas Prácticas* 43

Tabla 8 *Comparativo Fases de Modelos Buenas Prácticas para el Manejo de Evidencia Digital* 56

Tabla 9 *Evidencia digital potencial en la nube*..... 61

Lista de Figuras

Figura 1 *Ruta Metodológica* 29

Figura 2 *Comparativa de Responsabilidad Según los Modelos de Servicio* 34

Figura 3 *Características de la Evidencia Digital* 40

Figura 4 *Fases del modelo NIST 800-86* 49

Figura 5 *Fases del Modelo Forense Digital Abstracto*..... 51

Figura 6 *Fases del Modelo ISO 27037:2012* 52

Figura 7 *Fases del Modelo Simplificado EDRM 2.0 (2023)*..... 54

Figura 8 *Fases de Recolección y Preservación de Evidencia Digital Según Modelos de Buenas Prácticas* 57

Figura 9 *Fases de la Propuesta de Buenas Prácticas en la Recolección y Garantía de Integridad de la Evidencia Digital en el Cloud Computing.* 59

Figura 10 *Definiciones Legales con Respecto a Prueba Electrónica en el Convenio de Budapest* 65

Figura 11 *Tipos Específicos de Datos por Categoría, Definidos en el Convenio de Budapest*... 67

Figura 12 *Flujograma Recolección y Preservación de Evidencia Digital en el Cloud Computing* 71

Figura 13 *Experiencia de los Expertos en la Disciplina de Informática Forense*..... 74

Figura 14 *Tipo de Empresa en Donde Trabajan los Peritos* 75

Figura 15 *Años que los Peritos Llevan Ejerciendo la Disciplina de Informática Forense* 76

Figura 16 *Peritos que han Realizado la Recolección de Evidencia Digital en el Cloud Computing*..... 77

Figura 17 *Evidencia Digital Potencial que ha Requerido Recolectar u Obtener el Perito en el Cloud Computing* 78

Figura 18 *Empresas que Poseen Procedimientos Estandarizados para la Recolección y Garantía de Integridad de la Evidencia Digital en el Cloud Computingidencia digital en el cloud computing.* 79

Figura 19 *Procedimientos Aplicados por los Peritos en la Recolección de Evidencia Digital en el Cloud Computing* 80

Figura 20 *Conocimiento del Perito de Herramientas para la Recolección de la Evidencia Digital en el Cloud Computing* 81

Figura 21 *Utilización de Herramientas por parte del Perito para Recolectar Evidencia Digital en el Cloud Computing* 82

Figura 22 *Herramientas Utilizadas por los Peritos para Recolectar Evidencia Digital en el Cloud Computing.* 83

Figura 23 *Viabilidad de la Aplicación de Modelos de Buenas Prácticas por parte de los Peritos* 84

Figura 24 *Modelos de Buenas Prácticas Conocidos por los Peritos, para la Recolección y Preservación de la Evidencia Digital* 85

Figura 25 *Modelo de Buenas Prácticas, Considerado más Apropiado para la Recolección y Preservación de la Evidencia Digital* 86

Figura 26 *Conocimiento por parte de los Peritos, de los Procedimientos y Protocolo de Cadena de Custodia, para Garantizar la Integridad y Preservación de Evidencia Digital* 87

Figura 27 *Aporte de la Propuesta de Buenas Prácticas para Garantizar la Integridad de la Evidencia Digital en el Cloud Computing.* 88

Figura 28 *Aplicación de la Propuesta de Buenas Prácticas por parte de los Peritos, para Recolectar y Garantizar la Integridad de la Evidencia Digital en el Cloud Computing* 89

Introducción

En la actualidad no existen procedimientos estandarizados para la recolección y garantía de integridad de la evidencia digital en el cloud computing, por lo que en muchas ocasiones se depende del proveedor del servicio para obtener información relacionada con imágenes, videos, correos electrónicos, registros y demás información que pueda servir como prueba en un proceso judicial, en el que esta información se convierte en evidencia digital, que debe validarse y garantizar su no modificación, para que esta sea admitida como prueba en un estrado judicial, es por ello que en este trabajo, se realiza un análisis de las publicaciones de organizaciones reconocidas a nivel internacional, en la aplicación de buenas prácticas en la recolección y preservación de la evidencia digital, que permitió obtener de estas las mejores prácticas establecidas en los modelos RFC 3227, NIST 800-86, ADFM, ISO 27037, EDRM, SWGDE, así como otro gran número de guías, que sirvieron de base para establecer la propuesta de recolección y garantía de integridad de la evidencia digital en el cloud computing, la cual luego de ser evaluada su aplicación por expertos en la disciplina de informática forense, busca servir de guía para especialistas tanto en las áreas de la informática y del derecho, como para todo aquel que requiera recolectar, obtener, y garantizar la integridad la evidencia digital, de tal manera que esta sea admisible y validada en un proceso legal.

Planteamiento del Problema

Definición del Problema

Las evidencias digitales o pruebas electrónicas son piezas clave para llevar a cabo investigaciones en un proceso judicial, pues estas son registros de la información que es guardada o difundida a través de un sistema informático. Ahora bien, los cibercriminales intentan modificar o eliminar la evidencia digital, buscando ocultar el rastro de su delito, dificultando su custodia cuando la información está almacenada en la nube, pues adicional a que se puede alterar, dañar o destruir, también puede ser sensible al tiempo que se tarde para su recolección.

En la actualidad tanto personas como organizaciones tienden a almacenar su información en la nube, por facilidad, funcionalidad y costo, sin embargo, ese nuevo modelo de servicio de almacenamiento trae nuevos retos para garantizar los pilares fundamentales de la seguridad de la información, como son: la integridad, confidencialidad y disponibilidad. Tener garantizados estos pilares es fundamental, tanto para temas administrativos, como judiciales, de esta manera se debe garantizar que los activos de información, resguardados en la nube, no sufran alteraciones, por lo que se debe establecer e implementar buenas prácticas para la recolección de la evidencia digital, manteniendo la integridad de ésta en la nube, para su aporte a las autoridades judiciales, quienes, basados en estas, tomaran decisiones en los diferentes procesos.

Aunque existen varias normas y estándares internacionales, entre los que se encuentran las normas NIST, ISO, RFC, entre otras, estas no especifican buenas prácticas para el manejo de evidencias digitales almacenadas en la nube, por ello se debe recurrir a las buenas prácticas de manejo de evidencia digital en la nube, implementadas por organismos de ley, como el FBI, Europol, Interpol, el Grupo de trabajo científico sobre evidencia digital (SWGDE), y otras fuerzas del orden a nivel mundial, para realizar un compendio (Semprini, Nilles, y Silva, 2021)

que permita salvaguardar la integridad de la información almacenada en la nube, adicionando una autenticación a dicha información. Se habla de la integridad pues es el pilar más vulnerado (Dhake et al., 2022; Vella y Colombo, 2022). Ahora bien, acceder a ese tipo de información o material sobre la temática, que usan agencias del orden es difícil obtener, y solo se puede acceder a ella, si se es miembro de una fuerza aliada. De allí la importancia de resolver esta problemática identificada mediante la aplicación de buenas prácticas que implican la recolección y preservación de la evidencia digital, en la que esta implícita su custodia.

¿Podrían las buenas prácticas en el cloud computing garantizar la integridad de la evidencia digital?

Objetivos

Objetivo General

Diseñar una propuesta de buenas prácticas para la recolección y garantía de integridad de la evidencia digital en el cloud computing, que sirva como guía a los peritos en informática forense.

Objetivos Específicos

Realizar un análisis de la literatura y publicaciones de organizaciones internacionales reconocidas en informática forense, relacionadas con las prácticas y procedimientos utilizados para garantizar la integridad de la evidencia digital en el cloud computing.

Lograr un estado del arte de las mejores buenas prácticas, en la recolección y garantía de la integridad de la evidencia digital en el cloud computing.

Proyectar una propuesta de buenas prácticas, en la recolección y garantía de integridad de la evidencia digital obtenida en el cloud computing.

Evaluar la propuesta de buenas prácticas en la recolección de la evidencia digital y su aporte a garantizar la integridad de esta en el cloud computing, a través de expertos en la disciplina de informática forense.

Justificación

El desarrollo de este proyecto se justifica en los resultados del estudio de Palomo y Guillet (2021), que en su trabajo incluyen una guía para extraer evidencia digital contenida en servidores alojados en la nube, y el trabajo de Abdellah y Tahar (2022) al proponer un nuevo marco para el análisis forense en la nube. Trabajos que dan cuenta la relevancia del tema y su importancia.

En la actualidad tanto personas como organizaciones tienden a almacenar su información en la nube, por facilidad, funcionalidad y costo, sin embargo ese nuevo modelo de servicio de almacenamiento, trae consigo nuevos retos para garantizar los pilares fundaméntales de esta, como son la integridad, confidencialidad y disponibilidad, razón por la cual se hace necesario para el ámbito legal, en temas administrativos, disciplinarios y judiciales, establecer e implementar buenas prácticas para la recolección de la evidencia digital, manteniendo la integridad de esta en el cloud computing, lo que le permitirá a los investigadores y peritos en informática forense, aportar en debida forma dichas evidencias a las autoridades judiciales fiscales y jueces, quienes basados en estas, tomaran decisiones en los diferentes procesos que manejan, lo cual según El PAcCtO (2022) no solamente sobre temas vinculados a los denominados delitos informáticos, sino en las causas de delitos cometidos por medios informáticos y en general en todas las investigaciones penales de cualquier delito, en las que cada día más, resulta de utilidad la correcta recolección u obtención de pruebas electrónicas.

Marco de Referencia

Marco Teórico

Sistema de Gestión de la Seguridad de la Información

Un Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a las empresas para implementar mecanismos de seguridad informática acordes a los objetivos del negocio, según la norma ISO 27000 (2018), es un conjunto de elementos interrelacionados o que interactúan de una organización para establecer políticas, objetivos y procesos para lograr esos objetivos.

Familia de las Normas ISO/IEC 27000

Es un conjunto de normas de gestión de la seguridad de la información con la IEC (International Electrotechnical Commission), comisión internacional de electrotecnia, tiene algunas similitudes a la familia de las normas de gestión de la calidad ISO 9000. Cada una de las normas de la familia 27000 define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la información para todo tipo y tamaño de organizaciones, sean de carácter público o privado.

Según Vargas, y Castro Mattei (2007), no se debe centrar la atención solamente en los sistemas informáticos por mucho que tengan hoy en día una importancia más que relevante en el tratamiento de la información ya que de otra forma, se podría dejar sin proteger información que puede ser esencial para la actividad de la empresa.

Producto de la revisión de la literatura y publicaciones de organizaciones internacionales reconocidas en informática forense, relacionadas con buenas prácticas y procedimientos utilizados para garantizar la integridad de la evidencia digital en el cloud computing, se dan a conocer las que tienen mayor relación con la propuesta, así:

Tabla 1

Publicaciones de Organizaciones Reconocidas en Informática Forense

Publicación	Año	Descripción
NIST SP 800-201 ipd, Cloud Computing Forensic.	2023	Documento que resume la investigación realizada por los miembros del NIST Cloud Computing Forensic Science Working Group y presenta la Referencia Forense de Cloud Computing del NIST Arquitectura, cuyo objetivo es proporcionar soporte para la preparación forense de un sistema en la nube, está destinado a ayudar a los usuarios a entender qué desafíos forenses en la nube pueden existir para el sistema en la nube de una organización.
"La prueba electrónica en el marco nacional y en el internacional en Latinoamérica". PAcCTO - Programa de Asistencia contra el Crimen Transnacional Organizado	2022	Buenas prácticas en relación con la obtención de pruebas electrónicas o digitales, es un programa de cooperación internacional financiado por la Unión Europea que busca contribuir a la seguridad y la justicia en América Latina a través del apoyo a la lucha contra el crimen transnacional organizado.
UNODC - Guía práctica para la solicitud de pruebas electrónicas transfronterizas.	2022	Guía que proporciona información a investigadores, fiscales, autoridades judiciales y autoridades nacionales responsables de la asistencia judicial reciproca de los sestados miembros de las Naciones Unidas, a conservar y entregar pruebas electrónicas que obran en poder de proveedores de servicios radicados en jurisdicciones extranjeras.

Publicación	Año	Descripción
ISO/CEI 27001, seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información.	2022	Es la norma principal de la serie, que contiene los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Este documento también incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización.
ISO/CEI 27002: seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información.	2022	Guía de buenas prácticas que proporciona un conjunto de referencia de controles genéricos de seguridad de la información, y de implementación. Aborda la ciberseguridad y protección de datos y ha evolucionado con respecto a su primera publicación en 2005, es más completa e integral y está basada en la resiliencia, protección, defensa y gestión.
Guidelines for digital forensics first responders, best practices for search and seizure of electronic and digital evidence / Directrices para primeros respondientes forenses digitales, Mejores prácticas para la búsqueda e incautación de pruebas electrónicas y digitales. INTERPOL.	2021	Guía que proporciona información y asesoramiento sobre los enfoques forenses digitales que pueden adoptarse al incautar y analizar diferentes tipos de dispositivos. Estas directrices son orientadas para su uso por parte de profesionales encargados de hacer cumplir la ley que tengan la base legal o la autorización necesaria para realizar las acciones descritas en este documento.
NIST. (2020). NISTIR 8006. NIST Cloud Computing Forensic Science Challenges / Desafíos de la ciencia forense de computación en la nube del NIST	2020	Documento base para definir las preocupaciones de la ciencia forense en los ecosistemas de nube y como punto de partida para comprender esas preocupaciones con la intención de permitir que la comunidad de computación en la nube identificar las tecnologías y estándares que pueden mitigar estos desafíos.

Publicación	Año	Descripción
ISO/CEI 27017: Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube.	2015	Es una norma que establece un marco de seguridad de la información para organizaciones que utilizan o están considerando implementar servicios en la nube.
ISO/CEI 27037: Directrices para la identificación, recolección, adquisición y preservación de evidencia digital.	2012	Guía general para los responsables del manejo de potenciales fuentes de evidencia digital.

Nota. Guías, documentos y procedimientos de buenas prácticas, utilizados para garantizar la integridad de la evidencia digital en el cloud computing.

Marco Conceptual

Buenas Prácticas

Teniendo en cuenta el concepto de la FAO (2014), es una práctica que se ha demostrado que funciona bien y produce buenos resultados, y, por lo tanto, se recomienda como modelo. Es una experiencia exitosa, probada y validada, en un sentido amplio, que se ha repetido y que merece compartirse para que la adopte el mayor número posible de personas.

Cloud Computing

Es una tecnología que permite acceso remoto a servicios de software, hardware, almacenamiento de archivos, procesamiento de datos, entre otros, por medio de Internet, convirtiéndose en una alternativa a la ejecución en un computador o servidor local. En el modelo de nube, no hay necesidad de instalar aplicaciones de forma local en los computadores (Salesforce, 2022).

La computación en la nube ofrece a las personas y a las empresas la capacidad de un sin número de recursos de computación seguro, con buen mantenimiento, de fácil acceso y bajo demanda.

La computación en la nube o Cloud Computing según Hernández y Flórez-Fuentes (2014) es una abstracción de los recursos tecnológicos en donde se puede llegar a utilizar un servidor o muchos servidores siendo invisible para el usuario final y, además, gracias al clustering, se permite tratar a muchos servidores como uno solo.

Evidencia Digital

Según la norma ISO 27037 (2012), se establece como la información o datos, almacenados o transmitidos en forma binaria que puede ser invocada como prueba, igualmente en concordancia con la norma australiana HB:171 Guidelines for the Management of IT Evidence (2003), la evidencia digital se considera como "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". En ese marco, el termino de evidencia digital, es utilizado para describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal".

Incidente de Seguridad

Al hablar de un incidente de seguridad, nos referimos a cualquier suceso que pueda comprometer la confidencialidad, integridad o disponibilidad de un activo en una organización, de acuerdo al concepto de MINTIC (2016), un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información.

Algunos de los incidentes de seguridad que más se presentan son los siguientes:

- Problemas de privacidad - acceso a datos
- Acceso no autorizado
- Modificación de recursos no autorizado
- Uso inapropiado de recursos
- No disponibilidad de los recursos
- Abuso de privilegios
- Secuestro de cuentas,
- Servicios o tráfico Malware o ransomware
- Ataques de denegación de servicios.

Cuando se presenta un incidente de seguridad, es necesario intervenir lo más rápido posible, buscando dar respuesta a los interrogantes de: ¿qué causó el incidente?,¿cómo se causó?, y ¿quién lo causo?, así como donde, lo que en la gran mayoría de ocasiones deriva en un proceso judicial, por lo que se requiere de la obtención de manera rápida de información relevante para la investigación, la cual debe realizarse por personal capacitado que garantice la integridad, preservación y custodia de la información.

Integridad

Cualidad de la información que garantiza que los datos generados no han sido modificados, de acuerdo con la norma ISO 27000 (2018), esta se refiere a la propiedad de exactitud y completitud de la información.

Procedimiento

Se llama a los pasos establecidos y ordenados para obtener un resultado, según la norma ISO 9000 (2015), a la forma especificada de realizar una actividad o un proceso.

Seguridad de la Información

Es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información personal o empresarial, cuyo fin principal es proteger los activos de información (equipos, usuarios e información), que, según la norma ISO 27001 (2022), busca preservar la integridad, confidencialidad y disponibilidad de esta.

Virtualización

De acuerdo con la Guía de seguridad para tecnologías de virtualización completa de NIST (2011), la virtualización es la simulación del software y/o hardware sobre el que se ejecuta otro software. Este entorno simulado se denomina máquina virtual (VM), el cual es la base del funcionamiento de la nube, que consiste en la asignación de recursos físicos para la instalación de un sistema operativo.

Marco Legal

En el ámbito internacional, como en el nacional, dentro del campo del análisis forense, existe normatividad que le indica al perito en informática forense, como llevar a cabo su trabajo dando cumplimiento a la ley, esto ya que un análisis forense puede hacer parte de una investigación, o un proceso judicial en cualquier especialidad, por lo que es importante que esta normatividad sea tenida en cuenta al momento de realizar dicho análisis.

Es indispensable que el perito tenga conocimiento que cada país posee su propia regulación por lo que se debe tener clara la jurisdicción en la cual se va a realizar la recolección y análisis de la evidencia, esto ya que, aunque la empresa esté ubicada en un país, esta puede

tener contratados servicios en la nube con proveedores (Amazon, Microsoft, Google, etc.) ubicados en otros, por lo que debe tener claro cuáles son las leyes que se aplican, las que deben quedar definidas en el contrato suscrito entre la empresa y el proveedor.

Para la elaboración y desarrollo del presente trabajo se tuvo en cuenta como referencia legal, la normatividad aplicable en Colombia, la cual se aprecia en la siguiente tabla:

Tabla 2

Normatividad Colombiana Aplicada a la Evidencia Digital

Normatividad	Año	Descripción
Ley 527. Comercio electrónico	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, indicando su admisibilidad y la fuerza probatoria de los mismos, así como los criterios para valorarlos probatoriamente
Ley 599. Código Penal	2000	Por la que se expide el Código Penal.
Ley 906. Código de procedimiento penal	2004	Por la cual se expide el Código de Procedimiento Penal.
Ley 1273. Protección de la información y de los datos	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos
Ley 1928. Convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest	2018	Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest, 2001 pg. 24)

Normatividad	Año	Descripción
Manual del sistema de cadena de custodia.	2018	Directrices establecidas por la Fiscalía General de la Nación, para el sistema de cadena de custodia colombiana, durante las etapas asociadas al hallazgo, recolección, embalaje, transporte, análisis y almacenamiento de los Elementos Materiales Probatorios y Evidencia Física (EMP y EF), con el fin de garantizar su autenticidad y capacidad demostrativa, mientras que la autoridad competente ordena su disposición final.
Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia (Convenio de Budapest)	2022	Colombia firmó el Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia (Convenio de Budapest), instrumento destinado a mejorar la cooperación y la divulgación de pruebas electrónicas.

Nota. Legislación colombiana adoptada para el manejo de evidencia digital.

Marco Tecnológico

Frente al aspecto tecnológico y uso de herramientas forenses, para la recolección y preservación de la evidencia digital, estas han ido evolucionando, encontrándose en el mercado gran número de ellas, tanto de uso libre (Open Source) como de pago, en las que se inicia con el uso básico de software especializado, pasando por su automatización, hasta la utilización de software que permite la recolección de la evidencia digital de forma remota, es por ello que se presenta más adelante, algunas de las herramientas más utilizadas a nivel mundial por parte de investigadores y peritos en el campo judicial, para la recolección y preservación de evidencia digital en cloud, aclarando que el orden en el que se presentan, no responde a ningún criterio especifico, sino a la ordenación alfabética de estas.

Tabla 3

Herramientas de Software Forense

Herramienta	Funcionalidad	Fabricante
Belkasoft Acquisition Tool	Permite descargar los datos de las nubes más importantes, tales como iCloud, Google Drive y Google Plus.	Belkasoft
CloudTrail	Es un servicio que ofrece capacidades forenses para sistemas Cloud AWS, permite consultar las llamadas API y las acciones llevadas a cabo en la AWS Management Console, AWS Command Line Interface y las API y los SDK de AWS.	AWS
Elcomsoft Cloud eXplorer	Permite la extracción de todos los datos de la cuenta de Google. Descarga del historial de las ubicaciones del usuario, archivos y documentos, contactos, mensajes en Hangouts, Google Keep, historial de Chrome, historial de búsquedas y visitas de páginas, calendarios, imágenes y muchos otros datos. (Elcomsoft, 2024).	ElcomSoft
FAW	Adquisición forense de sitios web, capaz de adquirir cualquier tipo de sitios web: estáticos y dinámicos, CMS, comercio electrónico, redes sociales, Dark Web, etc.	Envolve Forensics LTD
Forensic Email Collector	Realiza búsquedas instantáneas in situ en los buzones de correo del servidor antes de la adquisición y conservar de forma forense solo los resultados de la búsqueda.	Metaspike
Magnet AXIOM Cloud	Recupera datos almacenados en las nubes de: WhatsApp, Facebook, Instagram, Twitter, iCloud, Google, entre otros. También, Procesa la devolución de garantías de Facebook, Instagram, Google, Apple y Snapchat	Magnet Forensics
MOBILedit Cloud Forensic	Localiza todas las copias de seguridad de iOS en la nube y le permite elegir las que desea extraer, analizar y crear informes. es un completo descargador forense de datos en la nube y generador de informes para los servicios más populares.	Compelson Labs
UFED Cloud Analyzer	Permite extraer, preservar y analizar dominios públicos y privados, datos de redes sociales, mensajería instantánea, almacenamiento de archivos, páginas web y otro contenido basado en la nube mediante un proceso con solidez forense.	Cellebrite

Herramienta	Funcionalidad	Fabricante
Oxygen Forensic® Cloud Extractor	Ofrece extracción rápida de datos de WhatsApp, Telegram, Discord, Viber y Line Messengers. (IMAP). De redes sociales como: Facebook, Twitter, Instagram.	Oxygen Forensics
Oxygen Remote Explorer	Permite encontrar evidencia crítica de manera rápida y completa mediante la recopilación de datos personalizable desde estaciones de trabajo remotas, servicios en la nube y dispositivos móviles e IoT.	Oxygen Forensics

Nota. Software utilizado por expertos en informática forense, para la recolección y preservación de la evidencia digital en el cloud computing.

Diseño Metodológico

La metodología empleada en este proyecto es deductiva, la cual (B, Cesar A. 2010) consiste en tomar conclusiones generales para obtener explicaciones particulares. El método se inicia con el análisis de los postulados, teoremas, leyes, principios, etcétera, de aplicación universal y de comprobada validez, para aplicarlos a soluciones o hechos particulares.

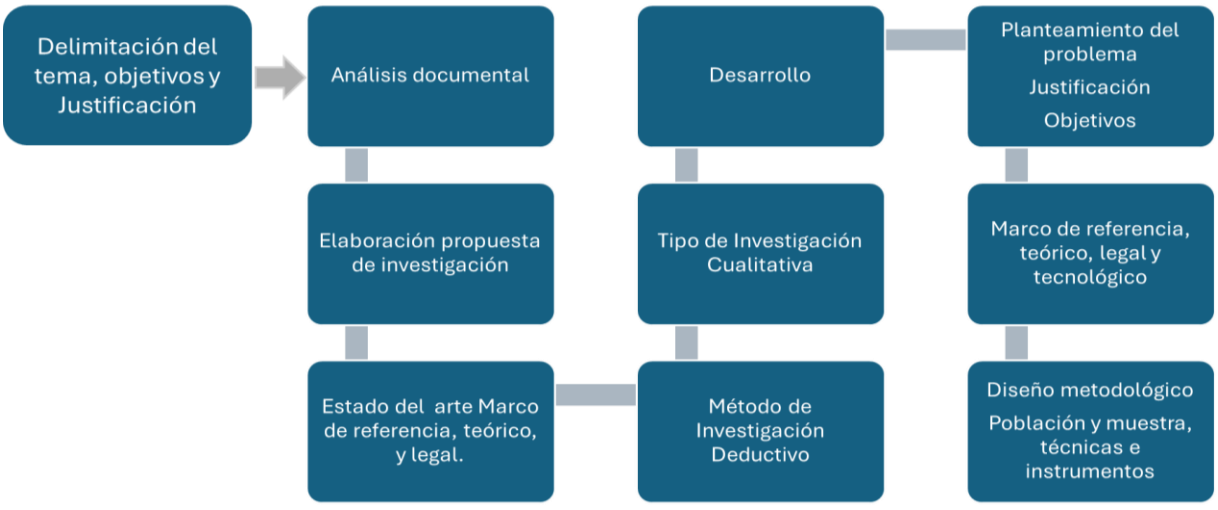
En esta se plantea proponer buenas prácticas en la recolección y garantía de integridad de la evidencia digital, frente a la dificultad que se presenta al realizar este procedimiento en el cloud computing.

Según Quecedo, Rosario; Castaño Carlos, (2002) definen la metodología cualitativa como la investigación que produce datos descriptivos: las propias palabras de las personas, habladas o escritas, y la conducta observable.

De acuerdo con lo anterior, se procedió a elaborar la propuesta de investigación a adelantar, llevando a cabo el siguiente esquema de trabajo:

Figura 1

Ruta Metodológica



Nota. Ruta metodológica de la propuesta de investigación desarrollada.

Población y Muestra

Población

De acuerdo con López, Pedro Luis. (2004), la población es el conjunto de personas u objetos de los que se desea conocer algo en una investigación, para esta la población seleccionada serán las publicaciones obtenidas relacionadas con la recolección de evidencia digital y su garantía de integridad en el cloud computing.

Muestra

En concordancia con López, Pedro Luis. (2004), se define como un subconjunto o parte del universo o población en que se llevó a cabo la investigación, en este caso fue un subconjunto de las publicaciones recolectadas, las cuales contenían posibles buenas prácticas para la recolección y garantía de integridad de la evidencia digital en el cloud computing.

La muestra fue intencionada, ya que no se obtuvo de un proceso de selección aleatorio, sino que los sujetos de la muestra fueron seleccionados en función de su accesibilidad o a criterio personal e intencional del investigador.

Técnicas e Instrumentos de Recolección de Información.

Para la obtención de la información se utilizó la técnica del análisis documental, como lo postularon (Tamayo, Carla; Silva S., Irene. 2022) se recolectaron datos de fuentes secundarias, como lo son libros, boletines, revistas, folletos, periódicos, guías, manuales, publicaciones, artículos, trabajos de grado que aportaban datos sobre la variable de interés, en este caso la recolección y garantía de integridad de la evidencia digital en el cloud computing.

Presentación, Interpretación y Análisis de Resultados

Ambientes Cloud

Concepto de Nube

Según la NIST SP800.145 (2011) la computación en la nube permite acceder a la red ubicuo, conveniente y bajo demanda en recursos informáticos configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con una mínima administración o interacción con el proveedor de servicios, modelo con cinco características, como se indica en la siguiente tabla.

Tabla 4

Características de la Nube según NIST SP800.145

Agrupación de recursos	Amplio acceso a la red	Elasticidad rápida	Servicio medido	Autoservicio bajo demanda
Los recursos informáticos del proveedor se agrupan para servir a varios consumidores mediante un modelo de múltiples inquilinos, con diferentes recursos físicos y virtuales asignados y reasignados dinámicamente según la demanda del consumidor.	Las capacidades están disponibles a través de la red y se accede a ellas a través de teléfonos móviles, tabletas, computadoras portátiles y estaciones de trabajo).	Las capacidades se pueden aprovisionar y liberar elásticamente, en algunos casos automáticamente, para escalar rápidamente hacia afuera y hacia adentro de acuerdo con la demanda.	Los sistemas en la nube controlan y optimizan automáticamente el uso de los recursos al aprovechar una capacidad de medición en algún nivel de abstracción apropiado para el tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas). El uso de recursos se puede	Un consumidor puede aprovisionar unilateralmente capacidades informáticas, como el tiempo del servidor y el almacenamiento en red, según sea necesario de forma automática sin requerir la interacción humana con cada proveedor de servicios.

Agrupación de recursos	Amplio acceso a la red	Elasticidad rápida	Servicio medido	Autoservicio bajo demanda
			monitorear, controlar y reportar, proporcionando transparencia tanto para el proveedor como para el consumidor del servicio utilizado.	

Nota. Cinco características principales del modelo de computación en la nube.

Para este proyecto de grado, el alcance de la recolección y garantía de integridad de la evidencia digital en servicios de almacenamiento en la nube estuvo orientado para el modelo de Software como Servicio (SaaS) como lo establece la norma NIST SP800.145 (2011), esto ya que es el más utilizado por los usuarios y porque la recolección de la evidencia digital para estos procesos es mucho mayor.

Tabla 5

Modelos de Servicio en la Nube

SaaS (Software como servicio)	PaaS (Plataforma como servicio)	IaaS (Infraestructura como servicio)
La capacidad que se proporciona al consumidor es utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube. Se puede acceder a las	La capacidad proporcionada al consumidor es implementar en la infraestructura en la nube aplicaciones creadas o adquiridas por el consumidor creadas mediante	La capacidad que se proporciona al consumidor es la de aprovisionar procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales en los que el consumidor puede implementar y

SaaS (Software como servicio)	PaaS (Plataforma como servicio)	IaaS (Infraestructura como servicio)
aplicaciones desde varios dispositivos cliente a través de una interfaz de cliente ligero, como un navegador web (por ejemplo, correo electrónico basado en la web) o una interfaz de programa. El consumidor no administra ni controla la infraestructura subyacente en la nube, incluida la red, los servidores, los sistemas operativos, el almacenamiento o las capacidades de las aplicaciones individuales, salvo los ajustes de configuración de aplicaciones específicas del usuario limitados.	programación idiomas, bibliotecas, servicios y herramientas admitidos por el proveedor. El consumidor no administra ni controla la infraestructura subyacente en la nube, incluida la red, los servidores, los sistemas operativos o el almacenamiento, pero tiene control sobre las aplicaciones implementadas y, posiblemente, los ajustes de configuración para el entorno de alojamiento de aplicaciones.	ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no administra ni controla la infraestructura de nube subyacente, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas; y posiblemente un control limitado de determinados componentes de red.

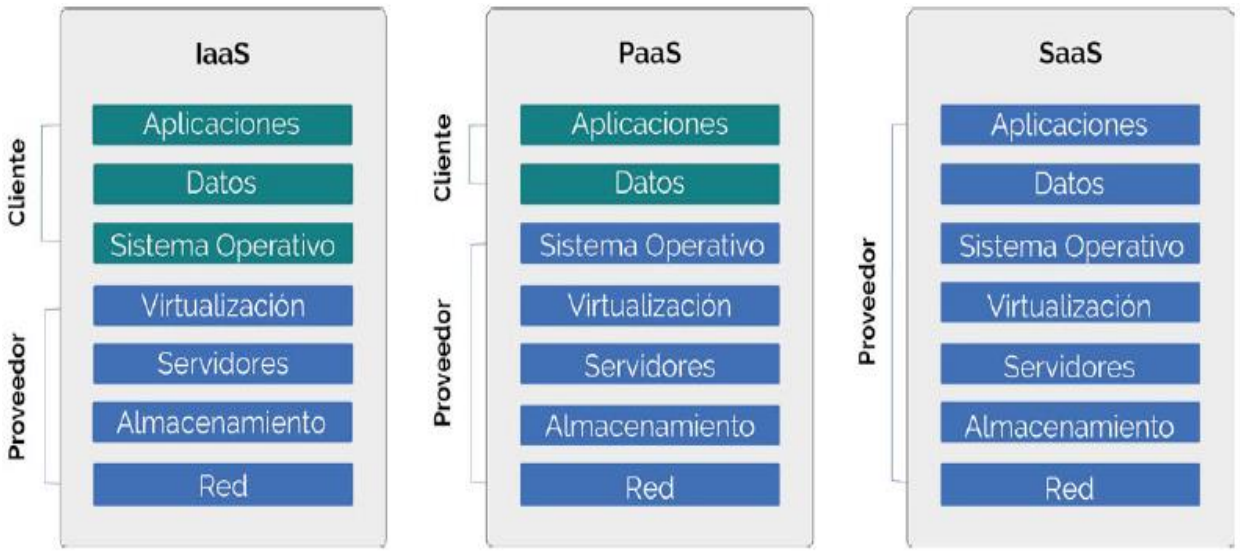
Nota. Principales modelos de servicio de computación en la nube, según NIST SP800.145.

En todos los modelos los proveedores de estos servicios son los que proporcionan la infraestructura y los únicos con acceso total, esto preocupa la privacidad, ya que pueden acceder a los datos del cliente en cualquier momento, sea accidental o deliberadamente para alterar o eliminar información, sin mencionar que pueden compartir la información con terceras partes, cuyos propósitos no se relacionan con la ley o los derechos de los usuarios.

En la siguiente figura se muestra una lista de recursos que puede administrar tanto el usuario, como el proveedor de nube en cada modelo de servicio.

Figura 2

Comparativa de Responsabilidad Según los Modelos de Servicio



Nota: Modelos de servicio en la nube, comparados según administración del cliente y proveedor. Ismsforum. (2018). CLOUD AUDIT & FORENSICS, comparativa de los modelos de servicio, pág. 14 (https://www.ismsforum.es/ ficheros/descargas/cloudauditforensics 2018v41 544463021.pdf). Copyright 2018 de Cloud Security Alliance España e ISMS Forum Spain.

En todo caso, los proveedores no son los únicos que pueden acceder a la información de los clientes o usuarios. Los ciberdelincuentes también pueden acceder a esta si la seguridad no es lo suficientemente fuerte como para mantener su integridad.

Conforme a la predicción del futuro de las infraestructuras de Cloud, realizado por Costello, Katie (2021) de la empresa Gartner, el uso de la computación en la nube (cloud computing) se está disparando, con la migración de las aplicaciones empresariales a la nube pública y con organizaciones cuyas implementaciones son cada vez más nativas de la nube, lo

que hace que sea pertinente para la investigación, tener conocimiento acerca de estrategias para el manejo general de la evidencia digital en este ámbito, por lo que este proyecto se relaciona con el modelo de nube pública, considerando lo dispuesto por la NIST SP800.145 (2011).

Tabla 6

Modelos de Implementación de Nube

Nube Pública	Nube Privada	Nube Comunitaria	Nube Híbrida
La infraestructura en la nube se aprovisiona para el uso abierto del público en general. Puede ser propiedad, administrada y operada por una organización empresarial, académica o gubernamental, o alguna combinación de ellas. Existe en las instalaciones del proveedor de la nube.	La infraestructura en la nube se aprovisiona para uso exclusivo de una sola organización compuesta por varios consumidores (por ejemplo, unidades de negocio). Puede ser propiedad, administrada y operada por la organización, un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones.	La infraestructura en la nube se aprovisiona para uso exclusivo de una comunidad específica de consumidores de organizaciones que comparten preocupaciones (por ejemplo, misión, requisitos de seguridad, políticas y consideraciones de cumplimiento). Puede ser propiedad, administrada y operada por una o más de las organizaciones de la comunidad, un tercero o alguna combinación de ellas, y puede existir dentro o fuera de las instalaciones.	La infraestructura en la nube es una composición de dos o más infraestructuras en la nube distintas (privada, comunitaria o pública) que siguen siendo entidades únicas, pero que están unidas por una tecnología estandarizada o patentada que permite la portabilidad de datos y aplicaciones (por ejemplo, la expansión de la nube para el equilibrio de carga entre nubes).

Nota. Características de los modelos de implementación de computación en la nube, según NIST SP800.145.

Desafíos Forenses en la Nube

De acuerdo con la NIST SP 800-201 ipd, (2023) el Grupo de Trabajo de Ciencias Forenses de Computación en la Nube del NIST (NCC FSWG), identifico los desafíos relacionados con la informática forense en la nube, los cuales según NIST IR 8006, (2020), se clasifican en nueve categorías, así:

1. Arquitectura (diversidad, complejidad, procedencia, multitenencia, segregación de datos). Los desafíos de la arquitectura en el análisis forense de la nube incluyen:

a. Lidiar con la variabilidad en las arquitecturas de nube entre proveedores

b. Compartimentación y aislamiento de datos de inquilinos durante el aprovisionamiento de recursos

c. Proliferación de sistemas, ubicaciones y puntos finales que pueden almacenar datos.

d. Procedencia precisa y segura para mantener y preservar la cadena de custodia

2. Recopilación de datos (por ejemplo, integridad de datos, recuperación de datos, ubicación de datos, imágenes). Los desafíos de recopilación de datos en el análisis forense en la nube incluyen:

a. Localización de artefactos forenses en sistemas grandes, distribuidos y dinámicos

b. Localización y recopilación de datos volátiles

c. Recopilación de datos de máquinas virtuales

d. Integridad de los datos en un entorno multiinquilino en el que los datos se comparten entre varios equipos en varias ubicaciones y son accesibles para varias partes

e. Imposibilidad de obtener imágenes de todos los artefactos forenses en la nube

f. Acceder a los datos de un inquilino sin violar la confidencialidad de otros inquilinos

g. Recuperación de datos eliminados en un entorno virtual compartido y distribuido

3. Análisis (por ejemplo, correlación, reconstrucción, sincronización de tiempo, registros, metadatos, líneas de tiempo). Los desafíos de análisis en el análisis forense de la nube incluyen:

a. Correlación de artefactos forenses entre proveedores de nube y dentro de ellos

b. Reconstrucción de eventos a partir de imágenes virtuales o almacenamiento

c. Integridad de los metadatos

d. Análisis de la línea de tiempo de los datos de registro, incluida la sincronización de marcas de tiempo.

4. Antiforense (p. ej., ofuscación, ocultación de datos, malware). Los antiforense son un conjunto de técnicas utilizadas específicamente para prevenir o inducir a error el análisis forense. Los desafíos antiforense en el análisis forense en la nube incluyen:

a. El uso de ofuscación, malware, ocultación de datos u otras técnicas para comprometer la integridad de la evidencia

b. El malware puede eludir los métodos de aislamiento de máquinas virtuales

5. Primeros respondedores de incidentes (por ejemplo, confiabilidad de los proveedores de la nube, tiempo de respuesta, reconstrucción). Los desafíos de la primera respuesta a incidentes en el análisis forense en la nube incluyen:

a. Confianza, competencia y confiabilidad de los proveedores de la nube para actuar como primeros respondedores y realizar la recopilación de datos

b. Dificultad para realizar el triaje inicial

c. Procesamiento de un gran volumen de artefactos forenses recolectados

6. Gestión de roles (por ejemplo, propietarios de datos, gestión de identidades, usuarios, control de acceso). Entre los desafíos de la administración de roles en el análisis forense en la nube se incluyen:

a. Identificar de forma única al propietario de una cuenta

b. Desacoplamiento entre las credenciales de usuario en la nube y los usuarios físicos

c. Facilidad de anonimato y creación de identidades ficticias en línea

d. Determinación de la propiedad exacta de los datos

e. Autenticación y control de acceso

7. Legal (por ejemplo, jurisdicciones, leyes, acuerdos de nivel de servicio, contratos, citaciones, cooperación internacional, privacidad, ética). Los desafíos legales en el análisis forense en la nube incluyen:

a. Identificar y abordar los problemas de las jurisdicciones para el acceso legal a los datos

b. Falta de canales efectivos para la comunicación y la cooperación internacional durante una investigación

c. Adquisición de datos que se basa en la cooperación, la competencia y la confiabilidad de los proveedores de la nube

d. Falta de términos en contratos y acuerdos de nivel de servicio

e. Emitir citaciones sin conocimiento de la ubicación física de los datos

8. Estándares (por ejemplo, procedimientos operativos estándar, interoperabilidad, pruebas, validación). Los desafíos de los estándares en el análisis forense de la nube incluyen:

a. Falta de procedimientos operativos estándar mínimos/básicos, prácticas y herramientas

b. Falta de interoperabilidad entre los proveedores de la nube

c. Falta de procedimientos de prueba y validación

9. Capacitación (por ejemplo, investigadores forenses, proveedores de nube, calificación, certificación). Los desafíos de capacitación en análisis forense en la nube incluyen:

a. Uso indebido de materiales de capacitación forense digital que no son aplicables al análisis forense en la nube

b. Falta de formación y experiencia forense en la nube, tanto para los investigadores como para los instructores.

c. Conocimiento limitado sobre las pruebas por parte del personal de mantenimiento de registros en los proveedores de servicios en la nube.

Contexto para Recopilar Evidencia Digital

De conformidad con la norma ISO 27037 (2012), la evidencia digital puede requerirse para su uso en varios escenarios distintos, cada uno de los cuales tiene un equilibrio diferente entre los impulsores de la calidad de la evidencia, la puntualidad del análisis, la restauración del servicio y el costo de la recopilación de evidencia digital.

Características de la Evidencia Digital

Teniendo en cuenta la norma ISO 27037 (2012), la evidencia digital se diferencia de la evidencia convencional, ya que esta posee características especiales, las cuales se presentan a continuación:

Volátil: se refiere a la posibilidad de que esta pueda desaparecer, cambiar o variar con facilidad de forma poco previsible, sino es recolectada y preservada de manera adecuada y oportuna.

Anónima: si bien la información de los metadatos nos permite identificar que dispositivo electrónico o software la genero, es difícil vincular y/o adjudicar a una persona, la responsabilidad de su creación o titularidad de esta.

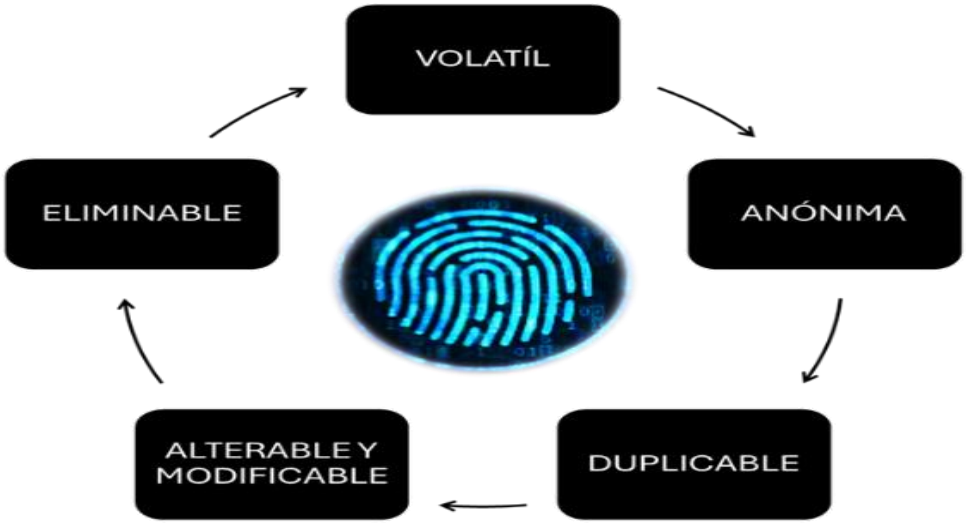
Duplicable: esta puede ser duplicada de manera exacta, copiada o almacenada simultáneamente en diferentes repositorios en su formato original.

Alterable y modificable: teniendo en cuenta sus características, con las herramientas adecuadas, esta puede ser fácilmente objeto de alteración y/o modificación.

Eliminable: debido a una acción voluntaria o involuntaria de quien tiene contacto con ella, pulsos electromagnéticos, descargas eléctricas, golpes o daños físicos, puede generarse la pérdida definitiva de la misma.

Figura 3

Características de la Evidencia Digital



Nota. Principales características de la evidencia digital.

Principios de la Evidencia Digital

Conforme a la norma ISO 27037 (2012), la evidencia digital se rige por tres principios fundamentales: relevancia, confiabilidad y suficiencia. Estos tres principios son importantes para todas las investigaciones, no solo para que las pruebas digitales sean admisibles en los tribunales.

Por lo tanto, las organizaciones deber tener un proceso de priorización, que identifique sus necesidades y equilibre la calidad de las pruebas, la rapidez y la oportuna restauración del servicio. Dicho proceso implica realizar la evaluación del material disponible, para determinar en la medida de lo posible el valor probatorio, así como el orden en que se debe obtener, recopilar, adquirir o conservar la evidencia digital potencial, esta priorización busca minimizar los riesgos asociados a la perdida de esta, y maximizar el valor probatorio de las posibles pruebas digitales obtenidas.

Computación Forense en la Nube

Según NIST.IR.8006 (2020), la ciencia forense de la computación en la nube es la aplicación de principios científicos, prácticas tecnológicas y métodos derivados y probados, para reconstruir eventos pasados de computación en la nube, a través de la identificación, adquisición, preservación, examen, interpretación y presentación de informes de posibles pruebas digitales.

En estas se han desarrollado varios modelos de procesos para el análisis forense digital, que incluye los siguientes ocho pasos y atributos distintivos:

1. Autoridad de búsqueda: se requiere autoridad legal para llevar a cabo un registro, recolección y/o incautación de datos.

2. Cadena de custodia: en contextos jurídicos, se requiere documentación cronológica del acceso y manejo de los elementos probatorios para evitar acusaciones de manipulación de pruebas o mala conducta.

3. Función de imagen/hashing: cuando se encuentran elementos que contienen evidencia digital potencial, cada uno debe duplicarse cuidadosamente y luego aplicarse un hash para validar la integridad de la copia.

4. Herramientas validadas: siempre que sea posible, las herramientas utilizadas para el análisis forense deben validarse para garantizar su fiabilidad y corrección.

5. Análisis: el análisis forense es la ejecución de técnicas de investigación y análisis para examinar, analizar e interpretar los artefactos probatorios recuperados.

6. Repetibilidad y reproducibilidad (aseguramiento de la calidad): los procedimientos y conclusiones del análisis forense deben ser repetibles y reproducibles por el mismo u otros analistas forenses.

7. Informes: el analista forense debe documentar su procedimiento analítico y sus conclusiones para su uso por parte de otros.

8. Presentación: en la mayoría de los casos, el analista forense presentará sus hallazgos y conclusiones ante un tribunal u otra audiencia.

Análisis Forense en la Nube

El análisis forense en cloud, o cloud forensics, está dirigido a las investigaciones de incidentes o la comisión de los delitos que se producen en este entorno, lo que incluye todos los tipos de ciberataques y violaciones de datos, así como conductas punibles establecidas en las diferentes legislaciones de índole penal, es allí donde se hace necesario la aplicación de un conjunto de procedimientos y técnicas metodológicas que permiten la identificación, recolección u obtención, preservación, interpretación y presentación de evidencia digital en este equipamiento informático.

Análisis de la Literatura

Teniendo en cuenta que la investigación es cualitativa, se inició con una revisión y análisis bibliográfico relacionado con el objeto de estudio, en la que se encontraron publicaciones de organizaciones internacionales reconocidas en informática forense, guías, libros y artículos, a fin de obtener un criterio, sobre las buenas prácticas en la recolección y garantía de integridad de la evidencia digital, como aporte a identificar los riesgos que se presentan por la recolección y preservación inadecuada de esta en el cloud computing, los mismos que deberán ser disminuidos mediante la ejecución de esta propuesta.

Tabla 7

Revisión Bibliográfica de *Buenas Prácticas*

No.	Titulo	Autor	Año	Tipo Documento
1	Request for Comments: 3227 (RFC3227), Directrices para la recopilación y el archivo de pruebas.	Network Working Group, D. Brezinski	2002	Guía
2	HB:171, Guidelines for the Management of IT Evidence	Normas Internacionales de Austrália	2003	Guía
3	Guide to Integrating Forensic Techniques into Incident Response.	Karen Kent and S. Chevalier and Timothy Grance and Hung Dang	2006	Guía
4	NIST 800-86. Guide to Integrating ForensicTechniques into Incident	NIST-National Institute of Standards and Technology	2006	Guía
5	SWGDE Data Integrity Within Computer Forensics.	Scientific Working Group on Digital Evidence	2006	Guía
6	Digital Forensics and Cyber Crime	Ibrahim Baggili	2011	Libro
7	ISO 27037 Directrices para la identificación, recolección, adquisición y preservación de evidencia digital.	ISO - Organización Internacional de Normalización	2012	Guía
8	Digital forensic investigation in cloud computing environment: Impact on privacy	Filipo Sharevski	2013	Artículo

No.	Titulo	Autor	Año	Tipo Documento
9	A forensically robust method for acquisition of iCloud data	Kurt Oestreicher*	2014	Artículo
10	Cloud forensics: Identifying the major issues and challenges	Stavros Simou; Christos Kalloniatis; Evangelia Kavakli	2014	Artículo
11	RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento.	INCIBE - Instituto Nacional de Ciberseguridad	2014	Guía
12	Digital forensic investigation and cloud computing	Keyun Ruan	2015	Libro
13	Scenario-based digital forensics challenges in cloud computing	Erik Miranda Lopez, Seo Yeon Moon and Jong Hyuk Park	2016	Artículo
14	Challenges of Digital Forensics in Cloud Computing Environment	Deevi Radha Rani, Sk. Nazma Sultana and Pasala Lourdu Sravani1	2016	Artículo
15	Digital forensics: Review of issues in scientific validation of digital evidence	Humaira Arshad; Aman Jantan; Oludare Isaac Abiodun	2018	Artículo
16	Challenges of cloud forensics	Syed Ahmed Ali; Shahzad Memon; Farhan Sahito	2018	Artículo
17	CLOUD AUDIT & FORENSICS	ISMS Forum -International Information Security Community	2018	Guía
18	Digital forensic static acquisition analysis for cloud environments	Harris Simaremare, Reza Tanujiwa Putra, Rahmad Abdillah	2019	Artículo
19	A Cloud Forensics Method Based on SDS and Cloud Forensics Trend Analysis	Liu Xuehua, Ding Liping, Liu Wenmao, Zheng Tao, Li Yanfeng, Wu Jingzheng	2019	Artículo
20	Analysis of cloud digital evidence	Irfan Ahmed; Vassil Roussev	2019	Libro
21	La guía del CIO para la nube distribuida	Garner. Costello, Katie	2020	Guía
22	NISTIR 8006. NIST Cloud Computing Forensic Science Challenges	NIST. National Institute of Standards and Technology	2020	Guía
23	SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers.	Scientific Working Group on Digital Evidence	2020	Guía
24	Evidencia digital de la nube. El aporte probatorio en Santiago del Estero	Lilia Eugenia Palomo; Sergio Mario Guillet	2021	Artículo
25	Metodología de obtención de Evidencia en la Nube	Semprini, Gastón ; Nilles, Gerardo; Silva, Gastón	2021	Artículo

No.	Titulo	Autor	Año	Tipo Documento
26	Cloud and edge computing-based computer forensics: Challenges and open problems	Vijay Prakash 1, AlexWilliams 2, Lalit Garg 1,3, Claudio Savaglio 4, * and Seema Bawa 1	2021	Artículo
27	Gartner predice el futuro de las infraestructuras de Cloud y Edge Computing.	Garner. Costello, Katie	2021	Artículo
28	Guidelines for digital forensics first responders, best practices for search and seizure of electronic and digital evidence.	INTERPOL - Organización Internacional de Policía Criminal	2021	Guía
29	e-Evidence Cooperation in Criminal Matters from an-EU Perspective	Rojszczak M.	2022	Artículo
30	An improved forensic-by-design framework for cloud computing with systems engineering standard compliance	AbdellahAkilalaM-TaharKechadib	2022	Artículo
31	D-Cloud-Collector: Admissible Forensic Evidence from Mobile Cloud Storage	Marcos Vella; Cristian Colombo	2022	Libro
32	Detection and extraction of digital footprints from the iDrive cloud storage using web browser forensics analysis	Adesoji Adesina, Ayodele Adebiyi, Charles Ayo	2022	Artículo
33	Cloud Forensics: Threat Assessment and Proposed Mitigations	Bhavesh Dhake; Heramba Limaye; Dilip Motwani	2022	Artículo
34	La prueba electrónica en el marco nacional y en el internacional en Latinoamérica.	El Pacto - Programa de Asistencia contra el Crimen Transnacional Organizado	2022	Guía
35	Análisis forense en cloud: ¿qué es y en qué consiste?	Fuentes, Fernando	2022	Artículo
36	NIST (SP) 800-201 ipd. Arquitectura de referencia forense de computación en la nube del NIST	Herman M, Iorga M, Salim AM, Jackson RH, Hurst MR, Leo RA, Mishra AK, Landreville NM, Wang Y	2022	Guía
37	Guía práctica para la solicitud de pruebas electrónicas transfronterizas.	UNODC - United Nations Office on Drugs and Crime	2022	Guía
38	Modelo EDRM.	EDRM (EDRM.NET).	2023	Guía

No.	Titulo	Autor	Año	Tipo Documento
39	Modelo forense digital abstracto.	Geeksforgeeks	2023	Guía
40	Guía de ISMS Fórum, Antes, durante y después de ir a la Nube, Respuesta ante Incidentes	ISMS Forum -International Information Security Community	2023	Guía

Nota. Referencia de libros, guías, manuales, publicaciones, artículos, utilizados para el análisis de buenas prácticas en la recolección y garantía de integridad de la evidencia digital.

Estado del Arte de Buenas Prácticas en la Recolección y Garantía de Integridad de la Evidencia Digital en el Cloud Computing

A través del tiempo se han propuesto diferentes guías, modelos, y directrices de buenas prácticas, en el manejo de la evidencia digital, que permiten abordar de la mejor manera la identificación, recolección, obtención y preservación de la evidencia digital, identificando luego del análisis de la literatura actual y la experiencia adquirida como perito, que las buenas prácticas más aplicadas internacionalmente por expertos en la disciplina de informática forense, son las siguientes:

RFC 3227

Directrices para la Recolección de Evidencias y su Almacenamiento

El RFC «Request For Comments» 3227, es un documento que recoge la propuesta de expertos en esta materia, para establecer pautas que permiten la creación de estándares y buenas prácticas en la recolección y almacenamiento de evidencia digital. De acuerdo con el RFC 3227, la investigación requiere de la identificación de todos los dispositivos susceptibles de contener evidencia. Una vez estos han sido identificados, deben ser copiados y protegidos para asegurar que no haya cambios que la puedan afectar, esto dada la alta volatilidad de los datos que se presenta en entornos virtuales, por lo que se indica tratar la escena de la siguiente manera:

- Determinar la ocurrencia del evento
- Examinar flujo de tráfico
- Reconstrucción de la sesión
- Reensamblar paquetes
- Extraer contenido de tráfico
- Examinar el paquete analizando el encabezado del protocolo

- Determinar el evento (intrusión, virus, escaneo, etc.)
- Escalar el evento

Basado en lo anterior, se debe tener claro el orden de volatilidad de la evidencia digital potencial y aplicar las prácticas establecidas por la RFC 3227 (2002), al momento de recolectar pruebas en el cloud computing, partiendo de lo más volátil a lo menos volátil, como se presenta a continuación:

- Registros, caché
- Tabla de enrutamiento, caché arp, tabla de procesos, estadísticas del kernel, memoria.
- Sistemas de archivos temporales
- Disco
- Registro remoto y datos de seguimiento que sean relevantes para el sistema en cuestión
- Configuración física, topología de red
- Medios de archivo

NIST 800-86

Guía para Integrar Técnicas Forenses en la Respuesta a Incidentes

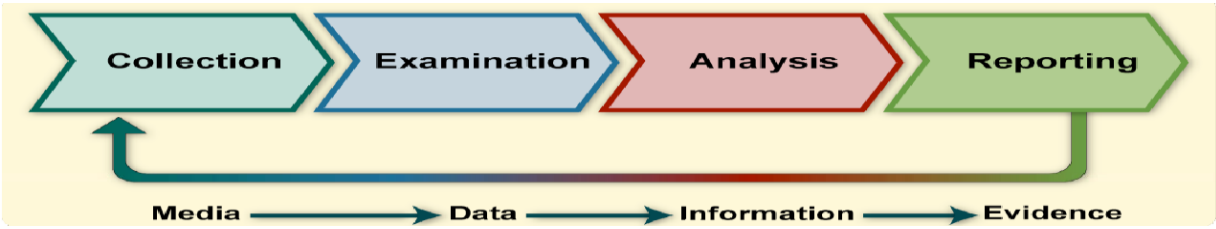
Según NIST (2006) se presenta la guía como punto de partida para desarrollar una capacidad forense junto con una amplia orientación proporcionada por asesores legales, funcionarios encargados de hacer cumplir la ley y la administración, la cual independientemente de la situación, comprende el proceso forense con las siguientes fases básicas:

- Recolección: consiste en identificar, etiquetar, registrar y adquirir datos de las posibles fuentes de datos relevantes, siguiendo directrices y procedimientos que preserven la integridad de los datos.

- Examen: implica el procesamiento forense de datos recolectados mediante métodos automatizados y manuales para evaluar y extraer datos de interés, preservando la integridad de los datos.
- Análisis: consiste en analizar los resultados del examen, utilizando métodos y técnicas legalmente justificables, para obtener información útil que responda a las preguntas que motivaron la realización de la recolección y el examen.
- Informes: en esta se informan los resultados del análisis, que incluye la descripción de las acciones utilizadas, la explicación de cómo se seleccionaron las herramientas y los procedimientos, así como la determinación de qué otras acciones deben realizarse.

Figura 4

Fases del Modelo NIST 800-86



Nota. Fases establecidas en el modelo NIS 800-86 para el manejo de la evidencia digital. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response (https://api.semanticscholar.org/CorpusID:64816814). En el dominio público.

ADFM

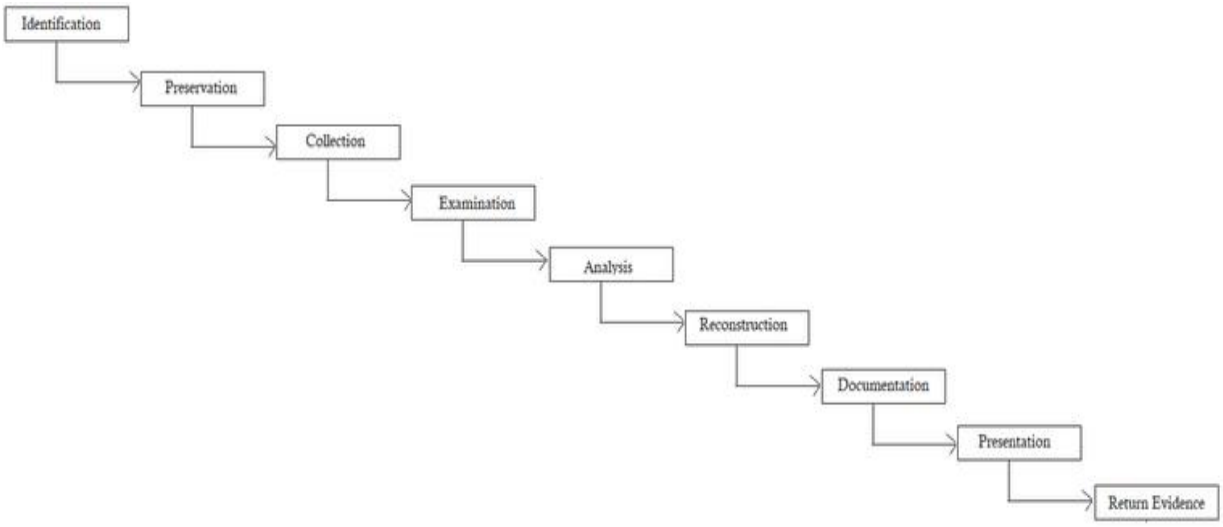
Modelo Forense Digital Abstracto

El modelo forense digital, es una herramienta para la investigación forense digital, la cual proporciona una forma clara y estructurada de proceder con evidencia particular, el cual consta de fases que les permiten a los investigadores aumentar la probabilidad de identificar y aportar evidencia digital para los diferentes procesos.

- Identificación: se identifican las pruebas que pueden estar en una computadora, servidor, teléfono móvil, servicio en la nube, etc.
- Preservación: se realiza para el mantenimiento de la integridad y la seguridad de las pruebas.
- Recolección: recolección de las pruebas y realización de un duplicado (imagen forense) de las pruebas principales.
- Examen: identificación de la información relevante y búsqueda de nuevos datos a partir de esta información.
- Análisis: vinculación de datos y recuperación e identificación de archivos dañados y eliminados.
- Reconstrucción: se construye un modelo de la evidencia o una situación en la que se encontró la evidencia.
- Documentación: el resultado o la información encontrada en las fases anteriores se registra en un documento (informe) que ayuda en los procedimientos legales.
- Presentación: el investigador desempeña el papel de presentador, proporcionando gráficos, informes y ayudas visuales para el proceso de investigación posterior.
- Devolución de evidencia: después de un examen completo, la evidencia que se utiliza para la investigación se devuelve al propietario original de la evidencia.

Figura 5

Fases del Modelo Forense Digital Abstracto



Nota. Fases del Modelo Forense Digital Abstracto para el manejo de evidencia digital. Geeksforgeeks, (2023), Modelo forense digital abstracto (https://www.geeksforgeeks.org/abstract-digital-forensic-model/). En el dominio público.

ISO 27037

Directrices para la Identificación, Recolección, Adquisición y Preservación de la Evidencia Digital

La norma internacional ISO 27037 (2012), proporciona pautas específicas para el manejo de la evidencia digital potencial; que se desarrollan en las etapas de identificación, recolección, adquisición y preservación de evidencia digital, buscando mantener su integridad, con una metodología aceptable para obtener pruebas digitales, que contribuyan a su admisibilidad en las acciones legales.

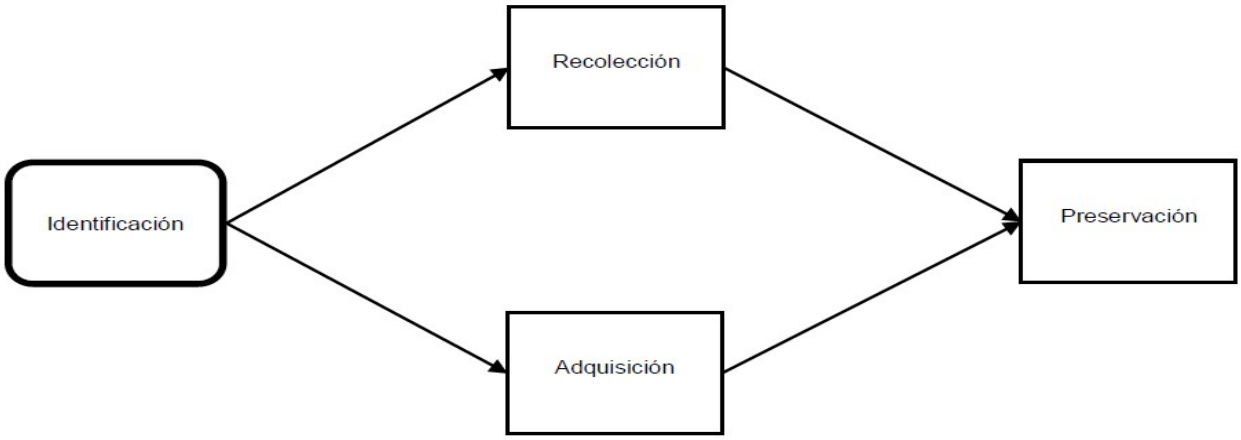
- Identificación: consiste en la búsqueda de reconocimiento y documentación de la evidencia digital potencial, en este proceso se deben identificar los dispositivos de

almacenamiento y de procesamiento digital que pueden contener potencial evidencia digital correspondiente al incidente.

- Recolección: etapa en el cual se recolectan los dispositivos que pueden contener evidencia digital potencial.
- Adquisición: implica realizar una copia exacta de la evidencia digital, así como la documentación de los métodos utilizados y las actividades realizadas.
- Preservación: en esta etapa la evidencia digital potencial se preserva para asegurar su utilidad en la investigación, buscando conservar los dispositivos digitales que pueden contenerla, este proceso de conservación debe iniciarse y mantenerse desde la identificación de los dispositivos digitales que contienen evidencia digital potencial.

Figura 6

Fases del Modelo ISO 27037:2012



Nota. Fases del *Modelo ISO 27037:2012* para el manejo de evidencia digital. Guía de Cadena de Custodia Digital, (2024), ISO 27037 (https://guiacadenadecustodiadigital.wordpress.com/iso-27037/). En el dominio público.

EDRM

Modelo de Referencia de Descubrimiento Electrónico

Según EDRM.NET (2023), el diagrama EDRM representa una visión conceptual del proceso de descubrimiento electrónico, no un modelo literal, lineal o en cascada, por lo que se pueden realizar algunos, pero no todos los pasos descritos en el diagrama, o se puede optar por los pasos en un orden diferente al de este.

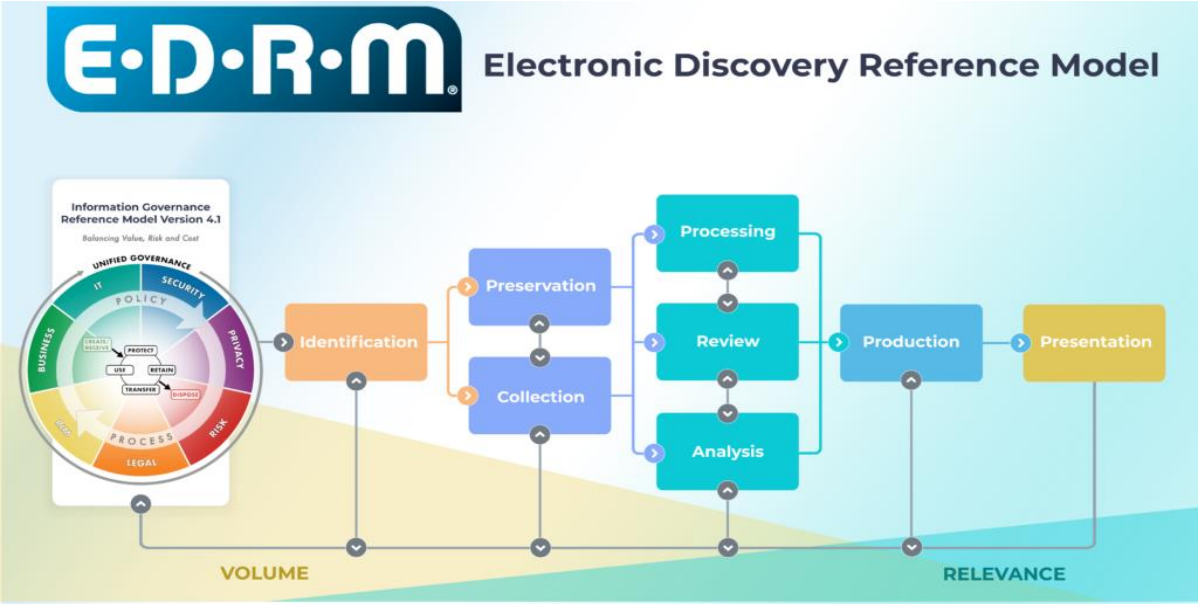
En este modelo, según EDRM (2020), el descubrimiento electrónico consta de varias etapas, que van desde la creación inicial de la ESI (información almacenada electrónicamente) hasta su disposición final, las cuales se presentan a continuación:

- Identificación: localizar fuentes potenciales de ESI y determinar su alcance, amplitud y profundidad.
- Preservación: garantizar que ESI esté protegido contra alteraciones o destrucción inapropiadas.
- Colección: recopilación de ESI para su uso posterior en el proceso de descubrimiento electrónico (procesamiento, revisión, etc.).
- Procesamiento: reducir el volumen de ESI y convertirlo, si es necesario, a formatos más adecuados para su revisión y análisis.
- Revisión: evaluación de ESI en cuanto a relevancia y privilegios.
- Análisis: evaluación de ESI en cuanto a contenido y contexto, incluidos patrones, temas, personas y debates clave.
- Producción: entregar ESI a otros en formas apropiadas y utilizando mecanismos de entrega apropiados.

- Presentación: mostrar ESI ante audiencias (en declaraciones, audiencias, juicios, etc.), especialmente en formas nativas y casi nativas, para obtener más información, validar hechos o posiciones existentes, o persuadir a una audiencia.

Figura 7

Fases del Modelo Simplificado EDRM 2.0



Nota. Fases del Modelo Simplificado EDRM 2.0 para el manejo de evidencia digital. EDRM (EDRM.NET), (2023). Modelo EDRM actual (https://edrm.net/edrm-model/current/). En el dominio público.

Propuesta de Buenas Prácticas

Actualmente, obtener evidencias digitales en los entornos de la nube se ha convertido en una tarea compleja, debido a las restricciones de los proveedores, ubicados en lugares diferentes a los de sus clientes, lo que dificulta la obtención de información para el análisis forense digital, produciendo demoras en el acceso, o la entrega de información incompleta, lo que impide garantizar la integridad de esta.

El análisis forense en entornos en la nube implica recolectar los recursos informáticos, tales como activos de red, servidores (físicos y virtuales), dispositivos de almacenamiento, aplicaciones, registros (logs) y cualquier otro servicio que contenga información, estos elementos se convierten en contenedores de evidencia digital potencial.

Según el modelo de servicio, podrán identificarse las dificultades a la hora de aplicar cloud forensics, las cuales estarán siempre asociadas al responsable de la gestión de los datos y el software, de conformidad con Fuentes, Fernando (2022) este indica que, en el caso del SaaS, o software como servicio, tanto el software como los datos están alojados permanentemente en la nube. El usuario accede a las aplicaciones en la nube, por lo que será el proveedor el responsable de gestionar tanto el software como los datos asociados y generados por él.

Es importante tener en cuenta las buenas prácticas establecidas por expertos y diferentes instituciones, así como organizaciones internacionales, en la recolección y garantía de integridad de evidencia digital, puesto que esto facilita la recopilación y creación de nuevas prácticas, las cuales pueden ajustarse a modelos de recolección de evidencia digital en el cloud computing, que aporten a procesos investigativos, mediante la aplicación de una metodología aceptable en la obtención de pruebas digitales, lo que contribuye a su admisibilidad en los diferentes estrados judiciales.

Tabla 8

Comparativo Fases de Modelos Buenas Prácticas para el Manejo de Evidencia Digital

Modelo	Fases			
	Identificar	Recolectar	Adquirir	Preservar
RFC 3227	X		X	X
NIST 800-86	X		X	X
ADFM	X	X		X
ISO 27037	X	X	X	X
EDRM 2.0	X	X		X

Nota. Comparativo de las fases que intervienen en la recolección y preservación de evidencia digital en el cloud computing, en los diferentes modelos de buenas prácticas.

Una vez realizado el análisis documental de las guías, manuales, y estándares de los diferentes organismos e instituciones aplicados a la recolección y preservación de la evidencia digital, se procede a diseñar la propuesta de buenas prácticas para la recolección y garantía de integridad de la evidencia digital en el cloud computing, de acuerdo con las recomendaciones y sugerencias impartidas en cada una de ellas, que aplican para la propuesta en mención, en la cual se plantea como base las fases comprometidas en la recolección y preservación de la evidencia digital que presentan cada uno de los modelos objeto de análisis, los cuales han sido aplicados a través del tiempo por expertos en la disciplina de informática forense, ya que son eficientes, producen resultados óptimos, cumplen con estándares en la materia, disminuyen los riesgos y aseguran que se recolecte y preserve la integridad de la evidencia digital de forma correcta.

Figura 8

Fases de Recolección y Preservación de Evidencia Digital Según Modelos de Buenas Prácticas

Nota. Comparativo de las fases de recolección y preservación de evidencia digital según modelos de buenas prácticas.

Esta propuesta busca convertirse es una buena práctica a tener en cuenta por expertos en informática forense, especialistas en el área de la informática, ciberseguridad, seguridad de la información, auxiliares de la justicia, técnicos, peritos, investigadores, abogados, fiscales, jueces, estudiantes y todo aquel que requiera recolectar y obtener evidencia digital, garantizando su integridad, de tal forma que esta sea admisible en un proceso legal, en cualquier rama del derecho (penal, civil, comercial, administrativo, laboral, disciplinario, tributario, entre otras).

Aunque en los modelos analizados, se puede identificar que en el proceso de recolección y garantía de integridad de la evidencia digital, se utilizan las fases de identificación, recolección, adquisición y preservación, en estos no se encuentra catalogada como fase la preparación, la cual se da antes de identificar la evidencia digital, la de obtención que se anexa en la fase de recolección, teniendo en cuenta que la información es susceptible de ser recolectada por un tercero, y la fase de documentación, que aunque es transversal a todas las fases, se consolida una vez se ha preservado la misma, buscando con la propuesta visibilizar la importancia de consolidar estas fases en el manejo de la evidencia digital en la nube.

Parte del imperativo de recolectar y preservar evidencia digital, después de presentarse un incidente informático, una conducta punible, o se tenga la necesidad de preservar un mensaje de datos en un proceso judicial, la cual puede ser aplicada teniendo en cuenta las legislaciones que se rigen en los diferentes países, se propone para esta buena práctica las fases de preparación, identificación, recolección y/u obtención, preservación y documentación, como se presenta a continuación:

- Preparación: es donde se determina el equipo y se reúnen las herramientas necesarias para el tratamiento de la evidencia digital en el lugar del incidente.
- Identificación: consiste en identificar y reconocer las fuentes de información que deben ser recolectadas y preservadas de acuerdo con el incidente o investigación.
- Recolección y/u obtención

Recolección: en esta se recolecta la información almacenada de los dispositivos electrónicos que podrían contener evidencia digital, lo cual es fundamental para garantizar que se recolecta toda la información relevante de manera adecuada para su posterior análisis.

Obtención: esta fase complementa la anterior, buscando obtener la evidencia digital directamente de los proveedores en las cuales se encuentra almacenada la información, ya sea mediante la activación del cumplimiento de contratos, o través de organismos de cooperación judicial.

- Preservación: en esta fase se garantiza que la información obtenida y recolectada no ha sufrido modificación.
- Documentación: fase en la cual se realiza el registro de la identificación, recolección y/ u obtención, y preservación de la evidencia digital.

Figura 9

Fases de la Propuesta de Buenas Prácticas en la Recolección y Garantía de Integridad de la Evidencia Digital en el Cloud Computing.

Nota. Fases de la propuesta de buenas prácticas.

Preparación

Antes de que un analista o investigador forense deba acceder a un sistema para la recolección de evidencia digital, su primera actividad debe ser la de tratar de conservar el sistema inalterado mediante técnicas de aislamiento, para que las evidencias no se volatilicen, esto será posible obteniendo copias inalteradas de la información del sistema, mediante el uso de herramientas de análisis forense previamente validadas.

En los entornos en la nube, se dificultad instalar o hacer uso de software de terceros, así como de mecanismos para adquirir evidencias sin alterarlas durante el proceso, por lo que no siempre es posible realizar la descarga rápida de grandes volúmenes de información, o aislar completamente un entorno cloud, lo que impedirá al analista o investigador forense tener acceso a éste.

Esto implica que, para poder realizar la recolección de evidencia digital en un entorno cloud, es necesario haberse preparado antes, lo que la convierte en una actividad proactiva, que se anticipa a la ocurrencia del incidente a investigar, por lo anterior se hace necesario además de contar con un plan de respuesta incidentes, tener herramientas de software y hardware previamente validadas y medios de almacenamiento sanitizados (borrado seguro) para garantizar la integridad de la información a almacenar.

Identificación

En esta fase se debe documentar la escena del incidente lo que debe incluir una descripción escrita, fotográfica o videográfica del lugar de recolección, el estado del dispositivo, el sistema o el servicio, sus características físicas, las cuales pueden incluir información de identificación (proveedor, marca, modelo, número de serie y cualquier otro tipo de particularidad que permita identificarlo y diferenciarlo de otro).

Al momento de determinar qué evidencias se deben recolectar u obtener, es fundamental tener en cuenta las posibles fuentes de evidencias en entornos en la nube y del evento que se quiere investigar. En el caso de las evidencias, habrá que diferenciar entre las que son accesibles por el cliente, y las que deberán ser suministradas por el proveedor de servicios en la nube:

Tabla 9

Evidencia Digital Potencial en la Nube

Fuente	Accesibilidad	Tipo
Red	Cliente	1. Logs de acceso a la red 2. Registro de transacciones, incluyendo información de cabeceras y contenidos de los mensajes enviados.
Usuarios	Cliente	1. Logs de herramientas de seguridad instaladas en los equipos de los usuarios finales. 2. Información de navegación y logs almacenados en los navegadores web. 3. Logs de acceso a la máquina. 4. Caché de aplicaciones.
Usuarios	Cliente	1. Cuentas de correo electrónico. 2. Cuentas de redes sociales. 3. Páginas web. 4. Cuentas de aplicaciones de mensajería instantánea. 5. Servicio de alojamiento de archivos.
Usuarios	Proveedor	1. Buzones de correo electrónico 2. Perfiles de redes sociales 3. Hosting de páginas web 4. Copias de seguridad
Infraestructura	Proveedor (SaaS y PaaS) o cliente (IaaS)	1. Logs de las herramientas de seguridad instaladas en el entorno. 2. Registros de acceso. 3. Registros de actividades en el sistema. 4. Logs de red generados. 5. Imágenes de memoria. 6. Snapshots del sistema virtualizado (Cliente o Proveedor dependiendo de si ofrece la funcionalidad con el servicio) 7. Registros de acceso al hipervisor (solo Proveedor) 8. Logs de acceso a la infraestructura sobre la que se despliegan los hipervisores (solo Proveedor).

Nota. Evidencia digital susceptible de ser recolectada y preservada en diferentes escenarios en la nube.

Recolección y/u obtención

Recolección

En esta fase se obtiene copia de la información que se presume puede estar vinculada con algún incidente, evitando al máximo modificar cualquier tipo de dato, para lo cual es necesario la realización de imágenes forenses (copias bit a bit) de los dispositivos, con herramientas y dispositivos previamente probados.

Este tipo de copia es imprescindible, porque permitirá recuperar archivos eliminados o particiones ocultas, arrojando como resultado una imagen de igual tamaño del dispositivo estudiado, la cual se debe verificar una vez terminado el proceso.

Con referencia a lo anterior, adicionalmente al momento de recolectar la información, se deben tener en cuenta las siguientes recomendaciones:

- Obtener una imagen forense del sistema o dispositivo lo más precisa posible.
- Priorizar la recolección sobre el análisis en caso de dudas.
- Minimizar los cambios en la información recopilada y eliminar agentes externos que puedan alterarla.
- Recoger información siguiendo el orden de volatilidad (de mayor a menor importancia y riesgo de pérdida).
- Realizar notas detalladas, incluyendo la descripción de fechas y horas.
- Respetar las políticas de privacidad y protección de datos personales, por lo que si es necesario se debe obtener autorización por escrito.

Todo este procedimiento debe llevarse a cabo mediante la utilización de guantes, bolsas antiestáticas o de Faraday, y contenedores adecuados para depositar los dispositivos o medios de

almacenamiento, que puedan ser afectados por ondas electromagnéticas, buscando con ello asegurar la integridad y evitar cambios accidentales o maliciosos en estos.

Obtención

Dado que en algunos casos puede presentarse la imposibilidad de recolectar la evidencia digital en el lugar del incidente, ya sea porque esta no se encuentra almacenada en los dispositivos del lugar, porque se requiera de autorizaciones o se deba remitir al proveedor del servicio, se hace necesario obtener dicha información a través de una solicitud de conservación por parte del usuario o por medio de una solicitud judicial a través de los canales establecidos para tal fin.

El aumento acelerado de la ciberdelincuencia y de la delincuencia transfronteriza, en espacios donde internet no tiene fronteras, el sistema de asistencia y cooperación judicial entre estados se tarda y está cargada de tramites, lo que provoca demoras en la obtención de la evidencia digital (pruebas electrónicas), según la guía práctica para la solicitud de pruebas electrónicas transfronterizas de UNDOC (2022). Además, han surgido problemas jurisdiccionales como resultado de la computación en la nube, lo que requiere que se examine cuidadosamente a qué lugar se envían las solicitudes de asistencia judicial recíproca para su ejecución.

Igualmente, la evidencia digital transita con rapidez por las fronteras, mientras que las solicitudes de asistencia judicial son lentas y engorrosas, especialmente si el profesional carece de la experiencia requerida en el proceso.

Ante estos desafíos gran número de países, entre ellos Colombia, el cual consciente de la necesidad de mejorar la coordinación y la cooperación entre los Estados, en marzo de 2020 se

adhirió al Convenio de Budapest, buscando fortalecer las capacidades nacionales, para prevenir, detectar, investigar y enjuiciar a la delincuencia organizada transnacional en el ciberespacio.

Según el informe explicativo del Consejo de Europa del convenio sobre la ciberdelincuencia (2001), este tiene como finalidad primordial: 1) armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos; 2) establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico, 3) establecer un régimen rápido y eficaz de cooperación internacional.

Para este tipo de investigaciones, se debe tener clara la información que se requiere, así como la entidad a la cual se debe hacerlo, para eso es necesario considerar la descripción de las definiciones legales del Convenio de Budapest, las cuales se relacionan a continuación:

Figura 10

Definiciones Legales con Respecto a Prueba Electrónica en el Convenio de Budapest

Convenio sobre la Ciberdelincuencia	
Datos informáticos (Artículo 1/b.)	Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función
Sistema informático (Artículo 1/a.)	Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa
Datos de abonado (Artículo 18/3)	Cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar: a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y el pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acordó de prestación de servicio
Datos de tráfico (Artículo 1/d.)	Todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente
Proveedor de servicios (Artículo 1/c.)	i. Toda la entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo

Nota. Estándar internacional de definiciones legales que proporciona el Convenio de Budapest. El Pacto - Programa de Asistencia contra el Crimen Transnacional Organizado. (2022). La prueba electrónica en el marco nacional y en el internacional en Latinoamérica, pág. 11 (https://www.elpaccto.eu/wp-content/uploads/2022/08/Publicacion-prueba-electronica-EL-PAcCTO.pdf). Copyright 2022 de *El Pacto.*

Es esencial determinar a dónde debe enviarse una solicitud de conservación. Un proveedor de servicios puede almacenar sus datos en distintas partes del mundo, pero esto no significa que la solicitud de conservación se deba enviar al lugar donde están almacenados los datos. La solicitud de conservación debe enviarse al lugar donde el proveedor de servicios tiene la custodia y el control de los datos, siendo necesario consultar las directrices para las fuerzas del orden establecidas por el proveedor de servicios, cuando proceda, para saber adónde debe enviarse la solicitud de conservación.

Tal como lo describe El PAcCTO (2022) en su publicación “La prueba electrónica en el marco nacional y el internacional en Latinoamérica”, como los datos son recopilados y almacenados por los proveedores de comunicaciones y servicios en línea, es esencial que las definiciones resulten en el marco de los datos específicos que son generados por los usuarios de los servicios.

Cuando se necesite legalmente datos para una investigación penal, las definiciones específicas permiten establecer tipos de datos relacionados con las categorías de datos de abonado, tráfico y contenido, definidos en el Convenio de Budapest. (El PAcCTO, 2022).

Figura 11

Tipos Específicos de Datos por Categoría, Definidos en el Convenio de Budapest

Categorías	Tipos de datos
Datos de abonado	1. Nombre completo 2. Nombre personalizado, apodo o nombre de inicio de sesión 3. ID de usuario 4. Números de teléfono 5. Correo electrónico 6. Fecha de nacimiento 7. Copia de DNI o pasaporte 8. Datos de facturación / Medios de pago 9. Fecha de inicio y finalización de la cuenta 10. Estado de la cuenta 11. Dirección IP de registro, incluidas fecha/hora 12. Dispositivos associados (incluído ID de dispositivo, IMEI, MAC) 13. Dirección y UDID cuando esté disponible) 14. Tipo de registro, copia de contrato, medio de verificación de identidad al momento del registro 15. Copias de documentos proporcionados por el suscriptor
Datos de tráfico	1. Registros de direcciones IP, incluidas fecha/hora 2. Registros de mensajes y registros de chat 3. Registro de actividad / archivos de registro, incluidas fecha / hora 4. Información de enrutamiento (dirección IP de origen, dirección IP de destino, número de puerto, navegador, encabezado de correo electrónico, ID de mensaje, volumen de transferencia de datos, origen o destino de cualquier mensaje electrónico enviado o recibido de la cuenta) 5. ID de la estación base, incluida la información geográfica y los datos de geolocalización
Datos de contenido	1. Contactos 2. Mensajes 3. Publicaciones 4. Archivos multimedia: videos, fotos, documentos 5. Fotos de perfil 6. Descarga de caja de correo electrónico 7. Descarga de contenido del dispositivo

Nota. Tipos de datos relacionados con las categorías de datos de abonado, tráfico y contenido, definidos en el Convenio de Budapest. El Pacto - Programa de Asistencia contra el Crimen Transnacional Organizado. (2022). La prueba electrónica en el marco nacional y en el internacional en Latinoamérica, pág. 12 (https://www.elpaccto.eu/wp-content/uploads/2022/08/Publicacion-prueba-electronica-EL-PAcCTO.pdf). Copyright 2022 de *El Pacto*.

Con los dispositivos en posesión, se debe realizar la obtención de la evidencia digital. Esto implica realizar una imagen forense de los datos almacenados en los dispositivos. Estas

copias se deben almacenar en un lugar seguro para su posterior análisis. La obtención se debe llevar a cabo de tal manera que no se altere ni dañe la información original.

Preservación

De acuerdo con la guía de buenas prácticas SWGDE Data Integrity Within Computer Forensics (2006), las pruebas digitales deben mantenerse de tal manera que se preserve la integridad de los datos, para lo cual el método aceptado para lograr esto, es la utilización de una función hash (MD5, SHA1, SHA256, SHA512, entre otras.), para autenticar la integridad de los archivos, esta función hash generará un valor matemático ya sea para un archivo individual o para una unidad completa.

El hash de los datos originales, conocido como hash de adquisición, debe realizarse cada que se recolecte evidencia digital, mínimo con dos funciones hash, esto permite identificar el acceso a la evidencia (archivo) o la alteración de un dato, ya que al darse esa acción el valor hash inicial cambiará drásticamente.

Al final de la recolección de la evidencia digital, y la creación de una imagen forense, esta debe ser sometida a un hash para demostrar que no se han producido alteraciones en los datos, de la misma forma, en caso de que se solicite la validación de este, se debe realizar un hashing utilizando las mismas funciones hash, ya sea para autenticar el archivo o la imagen forense, buscando con ello garantizar la integridad de los datos, como una representación verdadera y precisa de la evidencia original.

En esta etapa se debe garantizar que la información recolectada no se destruya o sea transformada, dando inicio el concepto de cadena de custodia, mediante un acta en la cual se debe realizar la descripción e identificación única de la evidencia, la fecha, hora de recolección, recepción y transferencia, dicho registro debe identificar completamente a cada persona que

tenga contacto con la evidencia, con su nombre, número de documento de identificación, cargo y firma.

Documentación

Conforme a lo indicado por IT Masters Mag. (2023) la documentación de los resultados implica la creación de informes técnicos detallados que describen los métodos utilizados, los datos recolectados, los análisis realizados y las conclusiones alcanzadas. Estos informes son fundamentales para registrar y respaldar científicamente los hallazgos obtenidos durante la investigación.

En aplicación de la norma ISO 27042 (2015), el contenido sugerido del informe debe tener como mínimo lo siguiente:

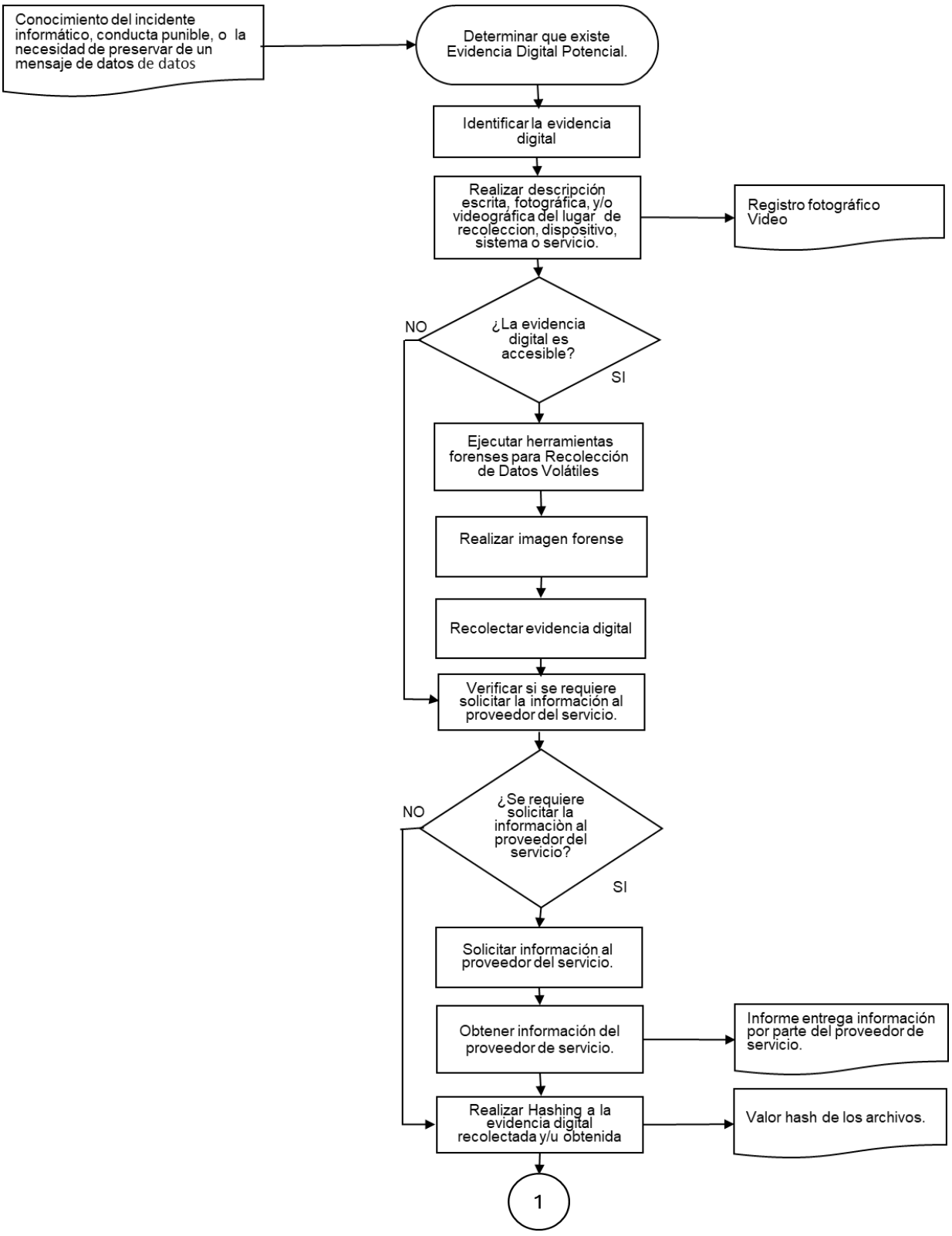
- una declaración clara de las cualificaciones o competencias del escritor para participar en la investigación, y elaborar el informe;
- una declaración clara de la información proporcionada al equipo de investigación antes de que comience la investigación (incluida la naturaleza del informe que se va a presentar);
- la naturaleza del incidente investigado;
- la hora y la duración del incidente;
- el lugar del incidente;
- el objetivo de la investigación;
- los miembros del equipo de investigación, y sus funciones y acciones;
- el momento y la duración de la investigación;
- el lugar de la investigación;
- detalles fácticos de las pruebas digitales encontradas durante la investigación;

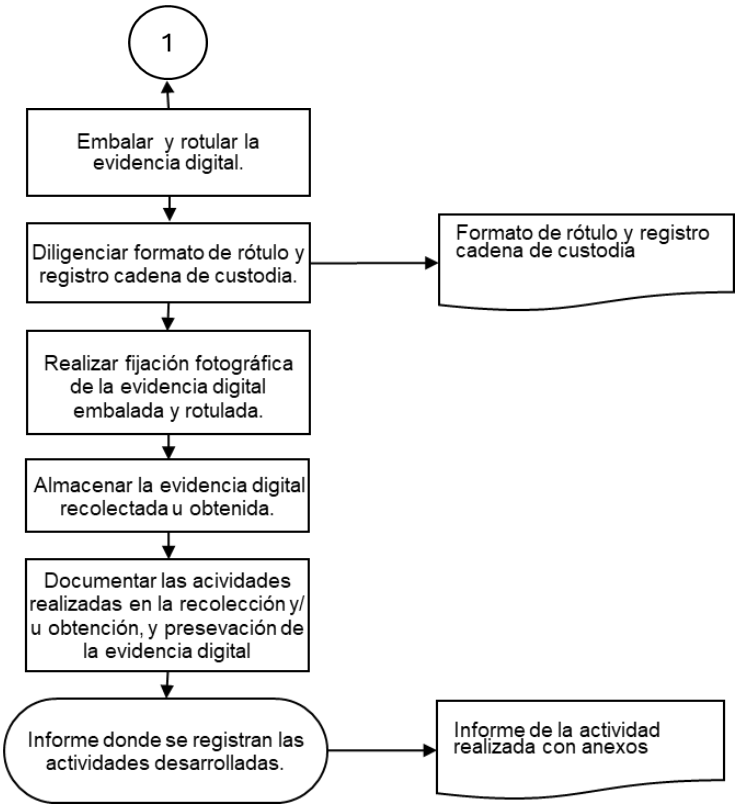
- cualquier daño a las posibles pruebas digitales que se haya observado durante la investigación y su impacto en las nuevas etapas de investigación;
- limitaciones de cualquier análisis realizado (por ejemplo, conjuntos de datos incompletos, limitaciones operativas o de tiempo); y
- una lista de los procesos utilizados, incluidas, en su caso, las herramientas utilizadas.

La documentación de los resultados garantiza la integridad de la evidencia digital, así como la transparencia, la reproducibilidad y la objetividad de la investigación forense digital, ya que, dando a conocer los descubrimientos realizados a las partes interesadas, se proporciona información que permite una argumentación valida, para el análisis crítico de las pruebas en el ámbito judicial.

Figura 12

Flujograma Recolección y Preservación de Evidencia Digital en el Cloud Computing





Nota. Flujograma que contiene los pasos para la recolección y preservación de evidencia digital en el cloud computing, según la propuesta de buenas prácticas.

Evaluación de la propuesta

En el desarrollo de evaluar la propuesta de buenas prácticas en la recolección de la evidencia digital y su aporte a garantizar la integridad de esta en el cloud computing, a través de expertos en la disciplina de informática forense, se implementó el instrumento de recolección de información tipo encuesta, el cual fue aplicado a personas que se desempeñan o se han desempeñado como peritos en informática forense a nivel internacional.

En la realización del instrumento de recolección de información, se buscó articular las preguntas con los modelos de buenas prácticas en la recolección y preservación de la evidencia digital, estructurando el cuestionario con el propósito principal de obtener una respuesta que aporte a la consecución del objetivo específico planteado.

Para la aplicación de este instrumento se contactó a expertos en la disciplina de informática forense, a los que se les informo sobre el trabajo de investigación que actualmente se está desarrollando, y se les solicitó la viabilidad de autorizar enviar el instrumento de recolección de información, con el propósito de evaluar la pertinencia y el aporte que da la “Propuesta de buenas prácticas en la recolección y garantía de integridad de la evidencia digital en el cloud computing”, como material de consulta y aplicación por parte de los peritos en informática forense.

Con esta autorización, se les compartió el link de la encuesta desarrollada en Google Forms, a través de los correos electrónicos suministrados por estos, obteniendo el desarrollo de 36 individuos de la muestra no probabilística planteada, instrumento que fue aplicado a expertos en informática forense ubicados en Argentina, Australia, Bolivia, Colombia, Ecuador, Estados Unidos, Guatemala, Honduras, México, Panamá, Perú, Portugal y República Dominicana, que ejercen en la actualidad cargos relacionados con peritaje informático y ciberseguridad.

Resultados de la Encuesta que Evaluó la Propuesta

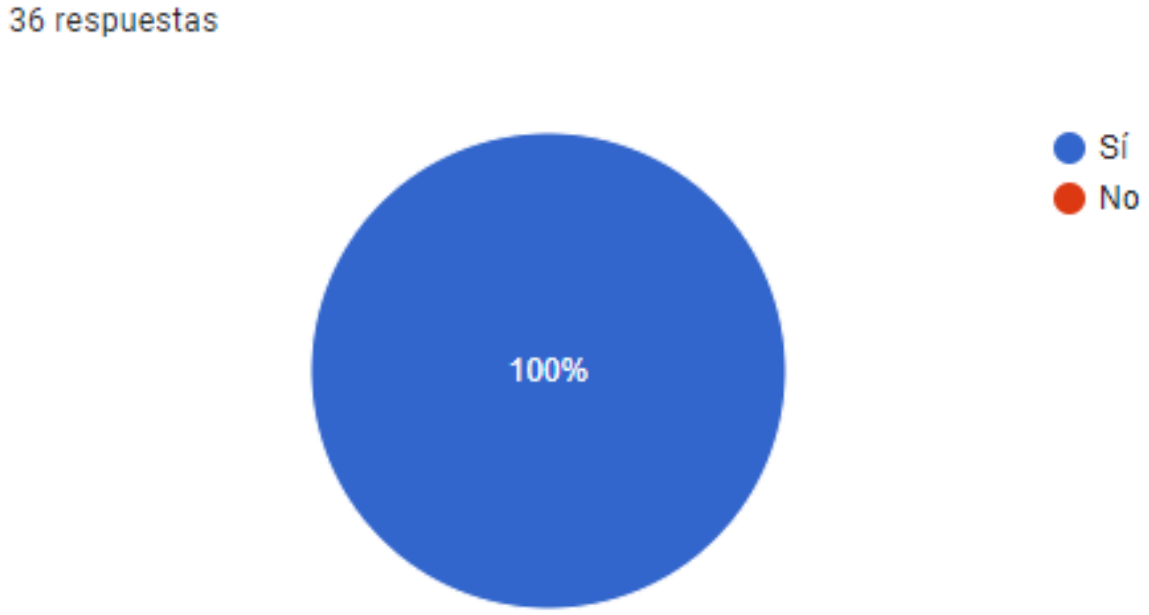
En respuesta a las preguntas establecidas en la encuesta, los expertos en informática forense dieron respuesta a cada uno de los interrogantes planteados, así:

1. ¿Trabaja o ha trabajado como perito en la disciplina de informática forense?

Se obtuvo que el 100% (36) de las personas encuestadas, contestaron que han trabajado o trabajan en un laboratorio de informática forense (fig. 13), con esta respuesta podemos ratificar que este instrumento de recolección de información fue dirigido a personal experto, por lo que se obtienen respuestas adecuadas que aportan significativamente a la presente propuesta.

Figura 13

Experiencia de los Expertos en la Disciplina de Informática Forense



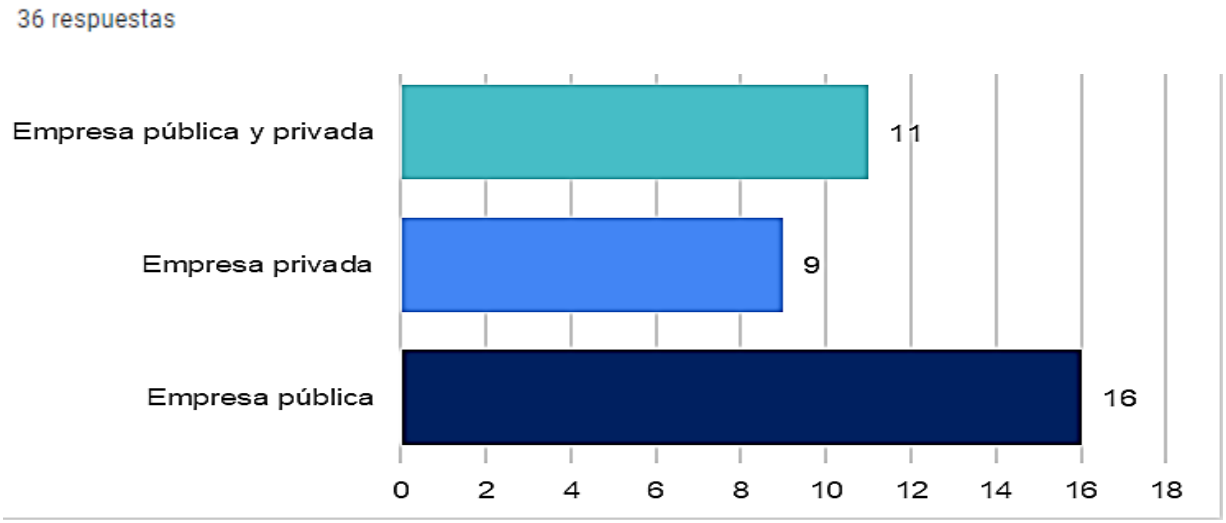
Nota. Respuesta de los encuestados, donde se identifica que el 100% tienen experiencia en informática forense.

2. ¿En qué tipo de institución o empresa?

Se obtuvo que, de las 36 personas encuestadas, 16 han trabajado como peritos en la disciplina de informática forense en el sector público, 9 en el sector privado y 11 en ambos sectores. (fig. 14).

Figura 14

Tipo de Empresa en Donde Trabajan los Peritos



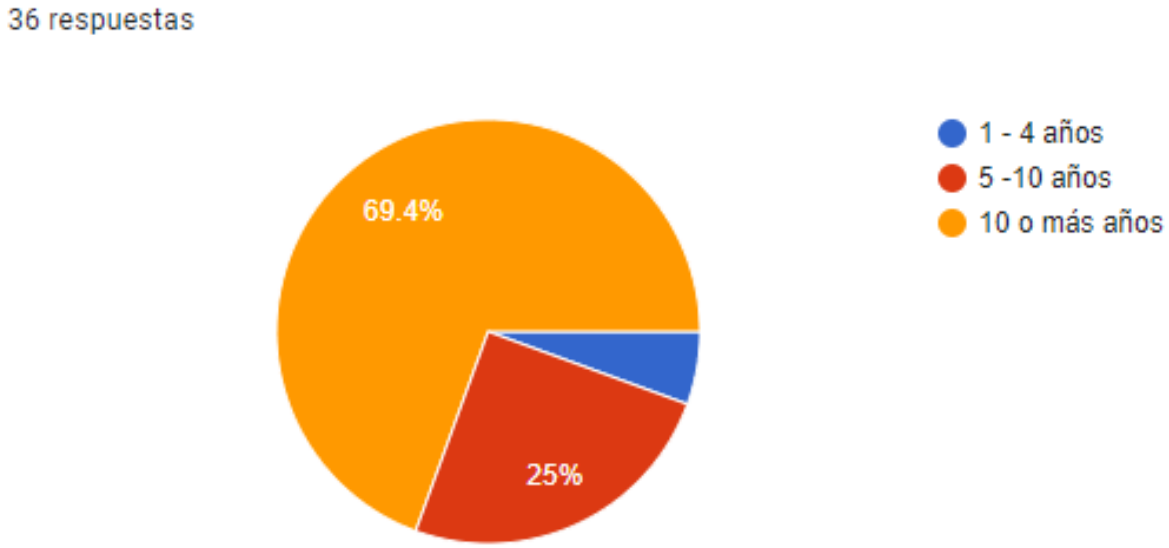
Nota. Respuesta de los encuestados, donde se evidencia que en mayor porcentaje los expertos trabajan, o ha trabajado en empresas del sector público.

3. ¿Cuántos años lleva ejerciendo como perito en la disciplina de informática forense?

Frente a esta pregunta el 5.6% (2) de los encuestados, contesto que lleva de 1 - 4 años, el 25% (9) entre 5 - 10 años, y el 69.4% (25) 10 o más años. (fig. 15), constatando que este personal cuenta con la experiencia necesaria para dar respuesta a los interrogantes y aportar a la propuesta.

Figura 15

Años que los Peritos Llevan Ejerciendo la Disciplina de Informática Forense



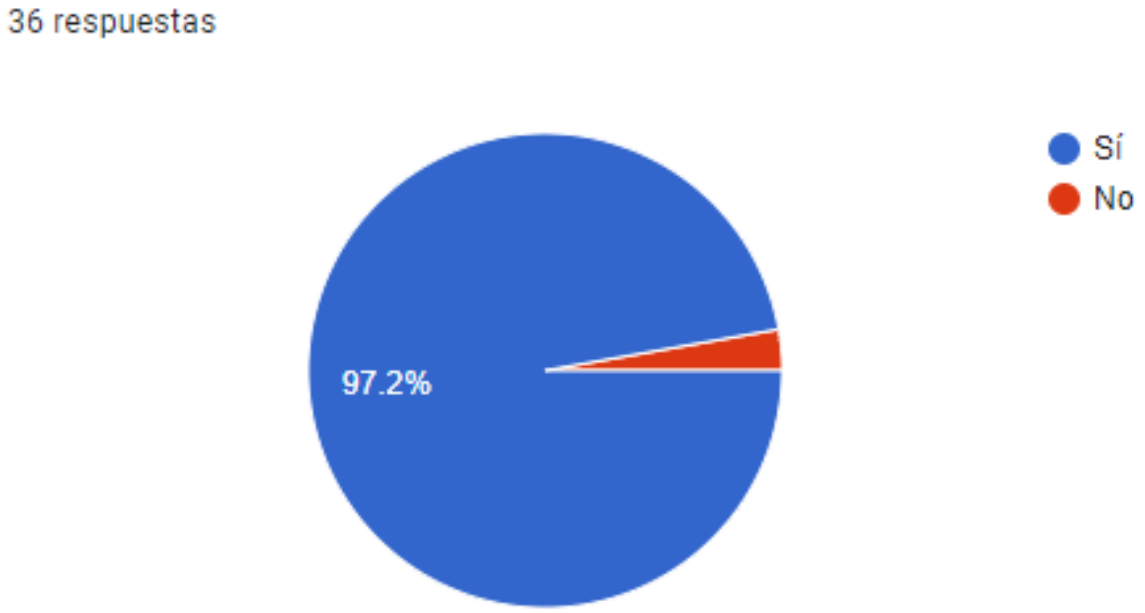
Nota. Respuesta de los encuestados, donde se refleja que el 69.4% (25), lleva ejerciendo como perito en la disciplina de informática forense 10 o más años.

4. ¿Dentro de las funciones desempeñadas como perito, ha realizado la recolección de evidencia digital en el cloud computing?

En respuesta a esta pregunta se obtuvo que el 97.2 % (35) de los encuestados han recolectado evidencia digital en el cloud computing, mientras que el 2.8% (1) no. (fig. 16), ratificando de esta forma, que el personal encuestado, es el idóneo para consultarle sobre la necesidad de implementar esta buena práctica, así como las herramientas que se utilizan para realizar un trabajo adecuado, de acuerdo normas y estándares internacionales.

Figura 16

Peritos que han Realizado la Recolección de Evidencia Digital en el Cloud Computing.



Nota. Respuesta de los encuestados, donde se refleja que el 97.2 % (35), han recolectado evidencia digital en el cloud computing.

5. ¿En los casos en los cuales se ha desempeñado como perito, que tipo de evidencia digital potencial ha requerido recolectar u obtener en el cloud computing?

Frente a esta pregunta el 86 % (31) de 36 de los encuestados, contestaron que como perito, el tipo de evidencia digital potencial que ha requerido recolectar u obtener en el cloud computing, han sido imágenes, vídeos, audios, ubicaciones, historial de navegación, el 52.8% (19) de 36, Snapshots de sistemas virtualizados / Máquinas virtuales, el 63.9% (23) de 36, Copias de seguridad, el 72.2% (26) de 36, Cuentas de aplicaciones de mensajería instantánea, el 72.2% (26) de 36, Páginas web / Hosting, el 94% (35) de 36, Cuentas de correo electrónico / Buzones de correo electrónico, el 75 % (27) de 36, Logs (registros) de herramientas de seguridad, información de navegadores web, de acceso a la red, máquinas, e hipervisor,

actividades en el sistema, transacciones, etc., el 80.6% (29) de 36, Servicio de alojamiento de archivos (Drive, One Drive, Dropbox, otros) (fig. 17), lo que permite evidenciar la gran cantidad de información que se encuentra en el cloud computing, susceptible de recolectar y preservar.

Figura 17

Evidencia Digital Potencial que ha Requerido Recolectar u Obtener el Perito en el Cloud Computing

Nota. Respuesta de los encuestados, donde se puede apreciar que el 94% (35), que en los casos en los cuales se ha desempeñado como perito, ha requerido recolectar u obtener cuentas de correo electrónico /buzones de correo electrónico, en el cloud computing.

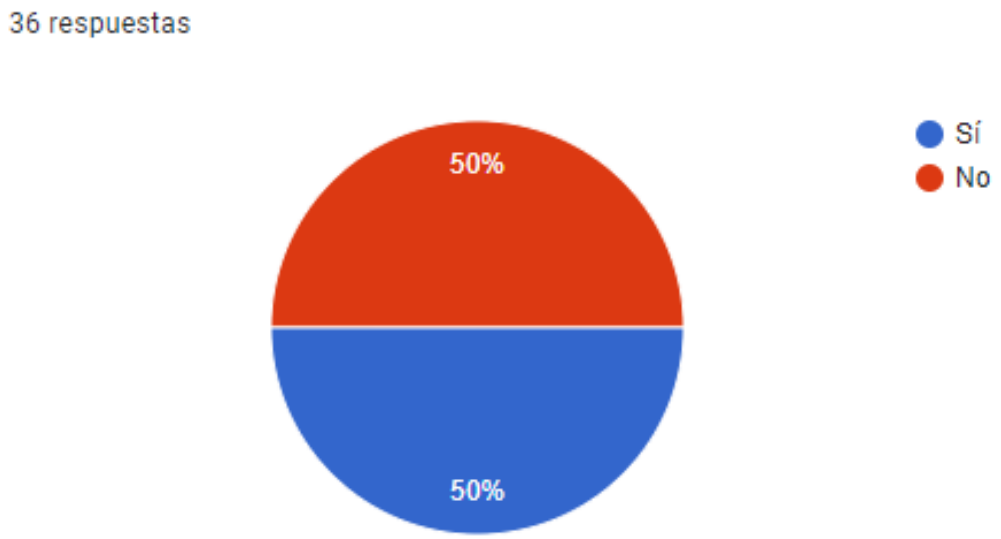
6. ¿En la institución o empresa en la cual se desempeña, o desempeñó, poseen un procedimiento estandarizado para la recolección y garantía de integridad (preservación) de la evidencia digital en el cloud computing?

En respuesta a esta pregunta el 50 % (18) indica que en la institución o empresa en la cual se desempeña o desempeñó como perito, poseen un procedimiento estandarizado para la recolección y garantía de integridad de la evidencia digital en el cloud computing, mientras que

el otro 50% (18) indico que no. (fig. 18), aquí podemos ver la necesidad que existe de estandarizar procedimientos y buenas prácticas en la recolección y preservación de evidencia digital, ya que el 50% de los encuestados manifestó no seguir un procedimiento estandarizado para tal fin.

Figura 18

Empresas que Poseen Procedimientos Estandarizados para la Recolección y Garantía de Integridad de la Evidencia Digital en el Cloud Computing



Nota. Respuesta de los encuestados, donde se puede evidenciar que solo en el 50% de las empresas donde laboran los expertos, existe un procedimiento estandarizado para la recolección y garantía de integridad (preservación) de la evidencia digital en el cloud computing.

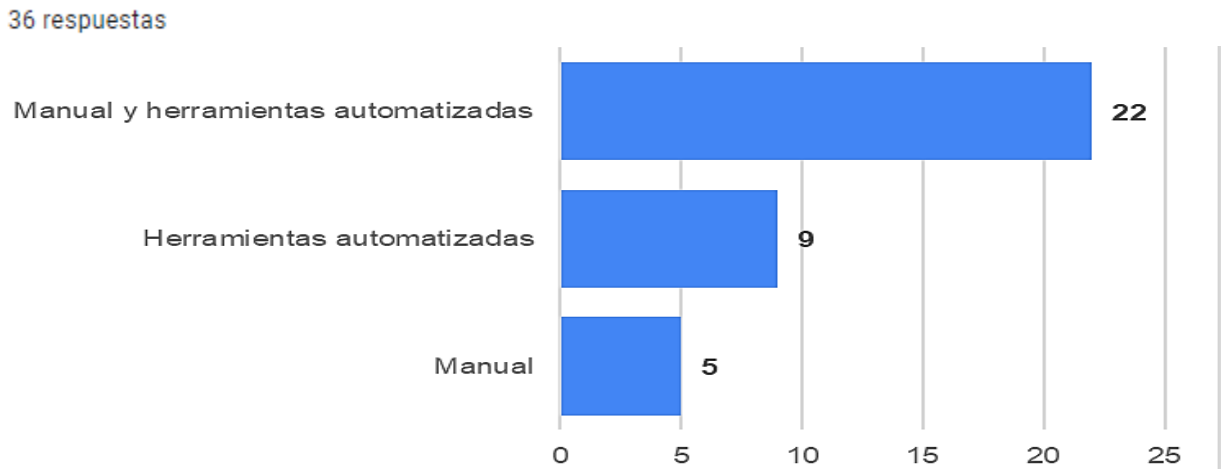
7. ¿De qué manera realiza la aplicación de procedimientos para la recolección de evidencia digital en el cloud computing?

De las 36 personas encuestadas, 14% (5) manifestaron aplicar procedimientos manuales para la recolección de evidencia digital en el cloud computing, 25% (9)que utilizan herramientas automatizadas, y 61% (22) aplican tanto procedimientos manuales, como herramientas

automatizadas (fig. 19), en esta respuesta se puede identificar que los expertos en informática forense, de acuerdo a sus necesidades, utilizan tanto procedimientos manuales como herramientas automatizadas para la recolección de evidencia digital en el cloud computing, por lo que la buena práctica que se propone aplica para ambos escenarios.

Figura 19

Procedimientos Aplicados por los Peritos en la Recolección de Evidencia Digital en el Cloud Computing



Nota. Respuesta de los encuestados, donde se puede apreciar que y 61% (22). Aplican procedimientos manuales y herramientas automatizadas para la recolección de evidencia digital en el cloud computing.

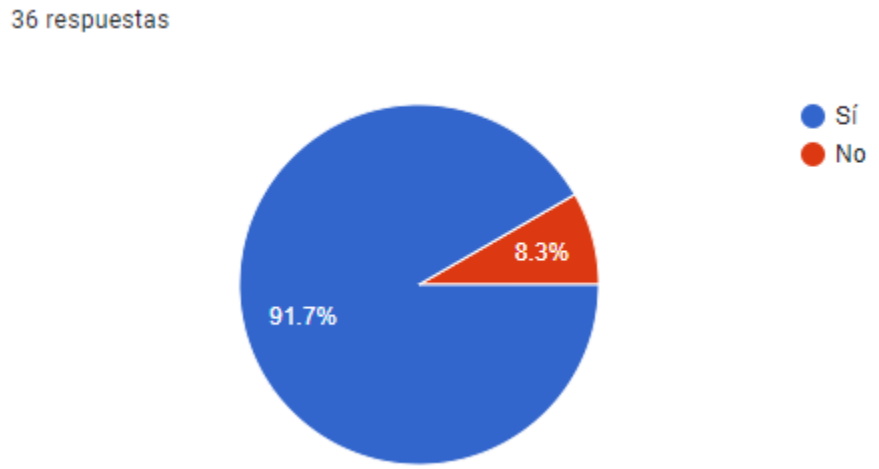
8. ¿En la actualidad conoce herramientas en el mercado que permitan la recolección de la evidencia digital en el cloud computing?

En respuesta a esta pregunta el 91.7 % (33) de los encuestados indica que conoce herramientas en el mercado que permiten la recolección de la evidencia digital en el cloud computing, mientras que el 8.3% (3) indico que no las conoce. (fig. 20), ante esta respuesta nos encontramos con un gran porcentaje de expertos familiarizados con herramientas para la

recolección de evidencia digital en el cloud computing, mientras que un menor porcentaje no las conoce, los cuales se convierten en público objetivo para la aplicación de la presente propuesta.

Figura 20

Conocimiento del Perito de Herramientas para la Recolección de la Evidencia Digital en el Cloud Computing



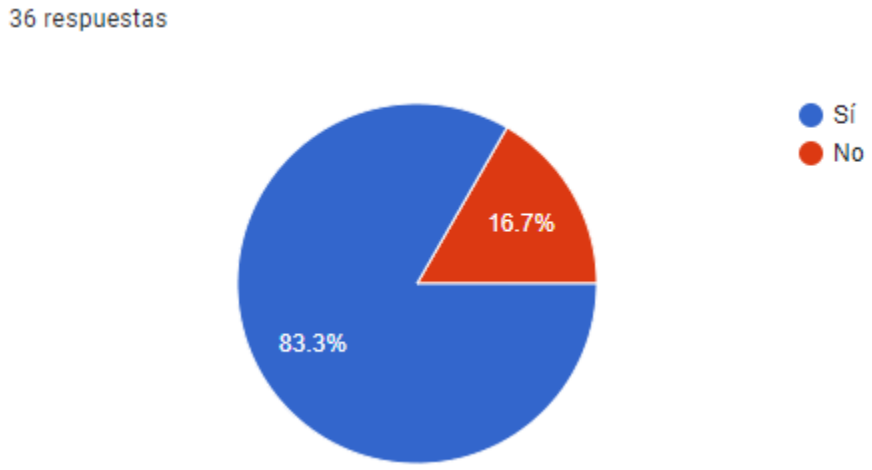
Nota. Respuesta de los encuestados, donde se refleja que el 91.7 % (33) indica que conoce herramientas en el mercado que permiten la recolección de la evidencia digital en el cloud computing.

9. ¿Ha utilizado alguna herramienta para recolectar evidencia digital en el cloud computing?

En respuesta a esta pregunta el 83.3 % (30) de los encuestados manifestó haber utilizado herramientas para recolectar evidencia digital en el cloud computing, mientras que el 16,7 % (6) manifestó que no las ha utilizado. (fig. 21), en esta respuesta se identifica nuevamente la experiencia de los expertos encuestados, los cuales en mayor porcentaje han utilizado herramientas para la recolección de evidencia digital en el cloud computing, una razón más para poner a su consideración la aplicación de la buena práctica propuesta.

Figura 21

Utilización de Herramientas por parte del Perito para Recolectar Evidencia Digital en el Cloud Computing



Nota. Respuesta de los encuestados, donde se puede evidenciar que la mayoría, el 83.3 % (30) manifestó haber utilizado herramientas para recolectar evidencia digital en el cloud computing.

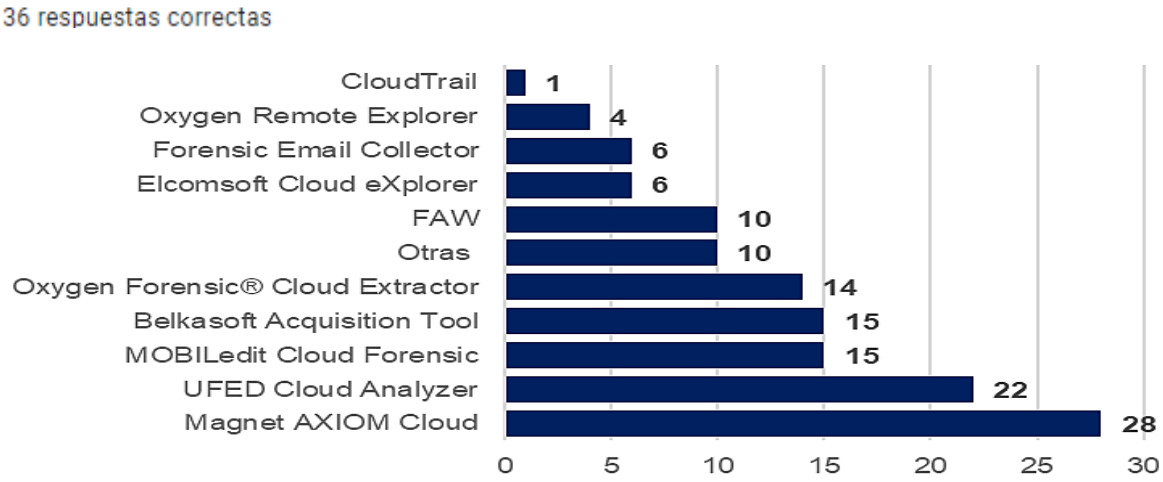
10. ¿De las herramientas que se encuentran en el mercado, cuales ha utilizado para recolectar la evidencia digital en el cloud computing?

De las 36 personas encuestadas , 1 contesto utilizar la herramienta CloudTrail, 4 contestaron Oxygen Remote Explorer, 6 contestaron Forensic Email Collector, 6 contestaron Elcomsoft Cloud eXplorer, 10 contestaron FAW, 10 más contestaron Otras , 14 contestaron Oxygen Forensic® Cloud Extractor, 15 contestaron Belkasoft Acquisition Tool, 15 contestaron MOBILedit Cloud Forensic, 22 contestaron UFED Cloud Analyzer, y 28 contestaron Magnet AXIOM Cloud, (fig. 22), en esta respuesta podemos identificar que existen diferentes herramientas de software en el mercado, así como el variado conocimiento de los expertos de cada una de ellas, lo cual independiente de la herramienta que se utilice, se ajusta a la aplicación

de la propuesta de buenas prácticas para la recolección de evidencia digital en el cloud computing.

Figura 22

Herramientas Utilizadas por los Peritos para Recolectar Evidencia Digital en el Cloud Computing



Nota. Respuesta de los encuestados, donde se puede apreciar que, la herramienta del mercado que más utilizan para recolectar la evidencia digital en el cloud computing es Magnet AXION Cloud.
Con referencia a las 10 personas que manifestaron utilizar otras herramientas para recolectar evidencia digital en el cloud computing, estas indicaron las siguientes: X1 forensic, Pandora, XRY Cloud, Cellebrite inseyets módulo cloud, Invictus Microsoft Extractor Suite, Hawke powershell module, y Self made scripting in Pyton.

11. ¿Desde su experiencia, considera viable la aplicación de modelos de buenas prácticas para la recolección y garantía de integridad (preservación) de evidencia digital, en el cloud computing?

Como respuesta se obtuvo que el 100 % (36) de los encuestados, contestaron que es viable la aplicación de modelos de buenas prácticas para la recolección y garantía de integridad (preservación) de evidencia digital, en el cloud computing (fig. 23), lo que fortalece la presente

propuesta, ya que expertos en la disciplina, ven viable la aplicación de buenas prácticas para recolección de la evidencia digital, asegurando su integridad y preservación.

Figura 23

Viabilidad de la Aplicación de Modelos de Buenas Prácticas por parte de los Peritos

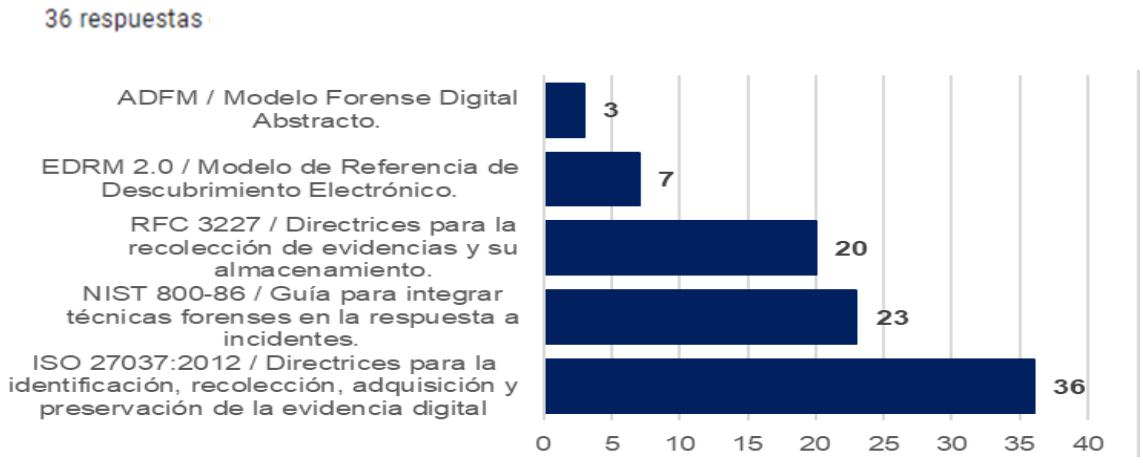
Nota. Respuesta de los encuestados, donde se puede apreciar que el 100% (36), ve viable la aplicación de modelos de buenas prácticas para la recolección y garantía de integridad (preservación) de evidencia digital, en el cloud computing.

12. ¿Qué modelos de buenas prácticas para la recolección y preservación de la evidencia digital, conoce?

Frente a esta pregunta el 100% (36) de los encuestados contesto que conoce el modelo ISO 27037:2012, el 63.9% (23) conoce el modelo NIST 800-86, el 55% (20) el modelo RFC 3227, el 19.4% (7) el modelo EDRM 2.0, y el 8.3% el modelo ADFM (fig. 24), frente a esta respuesta se identifica que el modelo de buenas prácticas más conocido por expertos en la disciplina de informática forense , es el modelo ISO 27037:2012, lo que da valor a la buena práctica propuesta, ya que esta complementa las fases de este modelo.

Figura 24

Modelos de Buenas Prácticas Conocidos por los Peritos, para la Recolección y Preservación de la Evidencia Digital



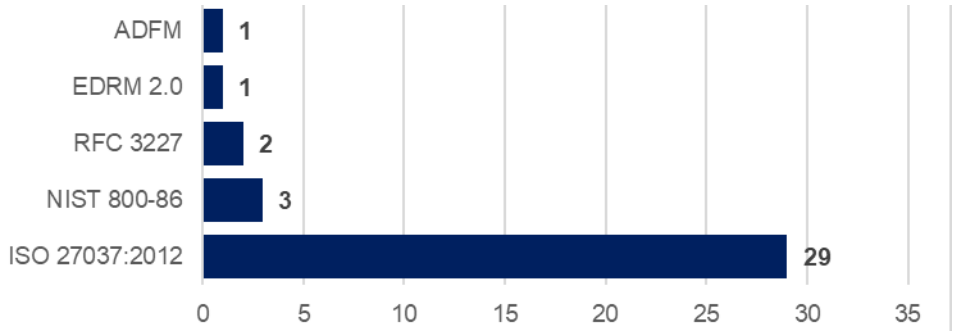
Nota. Respuesta de los encuestados, donde se refleja que el 100% (36), conoce el modelo ISO 27037:2012.

13. ¿Teniendo en cuenta las fases de modelos de buenas prácticas para la recolección y preservación de la evidencia digital conocidos, cual considera el más apropiado?

Frente a esta pregunta el 2.8% (1) de los encuestados, contesto que considera más apropiado el modelo ADFM, el 2.8% (1), el modelo EDRM 2.0, el 5.6% (2), el modelo RFC 3227, el 8.3% (3), el modelo NIST 800-86, y el 80.6% (29) el modelo ISO 27037:2012 (fig. 25)., donde se puede evidenciar que los expertos, consideran más apropiado las fases del modelo ISO 27037:2012, lo que va en la misma dirección de la propuesta , en la que se fortalecen esas fases, con las de planeación y documentación, así como el fortalecimiento de la fase de recolección, en donde se anexa la obtención, lo que aporta a una mejor la recolección y preservación de la evidencia digital en el cloud computing.

Figura 25

Modelo de Buenas Prácticas, Considerado más Apropiado para la Recolección y Preservación de la Evidencia Digital



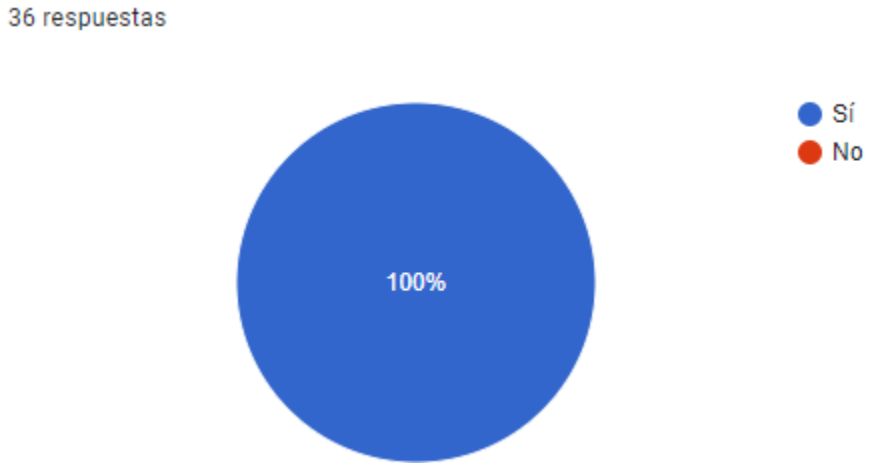
Nota. Respuesta de los encuestados, donde se puede evidencia que el 80.6% (29), teniendo en cuenta las fases de modelos de buenas prácticas para la recolección y preservación de la evidencia digital conocidos, considera como más apropiado el modelo ISO 27037:2012.

14. ¿Conoce los procedimientos establecidos para garantizar la integridad y preservación de evidencia digital en cumplimiento al protocolo de cadena de custodia?

En respuesta a esta pregunta, el 100% (36) de los encuestados, indica que conoce los procedimientos establecidos para garantizar la integridad y preservación de evidencia digital, en cumplimiento al protocolo de cadena de custodia (fig. 26), en esta respuesta se identifica la experiencia de los expertos en el manejo de la cadena de custodia, lo que en la evaluación de la propuesta se ve aplicado en la implementación de una buena práctica en la recolección y garantía de integridad de la evidencia digital en el cloud computing.

Figura 26

Conocimiento por parte de los Peritos, de los Procedimientos y Protocolo de Cadena de Custodia, para Garantizar la Integridad y Preservación de Evidencia Digital



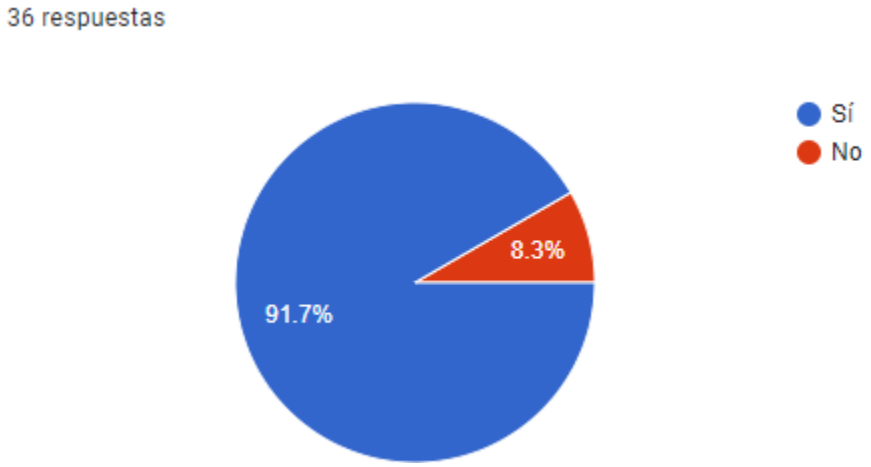
Nota. Respuesta de los encuestados, donde se puede evidenciar que el 100% (36), indica que conoce los procedimientos establecidos para garantizar la integridad y preservación de evidencia digital, en cumplimiento al protocolo de cadena de custodia.

15. ¿En su concepto la propuesta de buenas prácticas en mención aporta a garantizar la integridad de la evidencia digital en el cloud computing?

En respuesta a esta pregunta el 91.7 % (33) indica que la propuesta de buenas prácticas en mención aporta a garantizar la integridad de la evidencia digital en el cloud computing, mientras que el 8.3 % (3) indico que no. (fig. 27), los expertos consultados basados en su experiencia, en un alto porcentaje indican que la propuesta presentada aporta a garantizar la integridad de la evidencia digital en el cloud computing, evidenciando así que se cumplen con los objetivos de la propuesta.

Figura 27

Aporte de la Propuesta de Buenas Prácticas para Garantizar la Integridad de la Evidencia Digital en el Cloud Computing



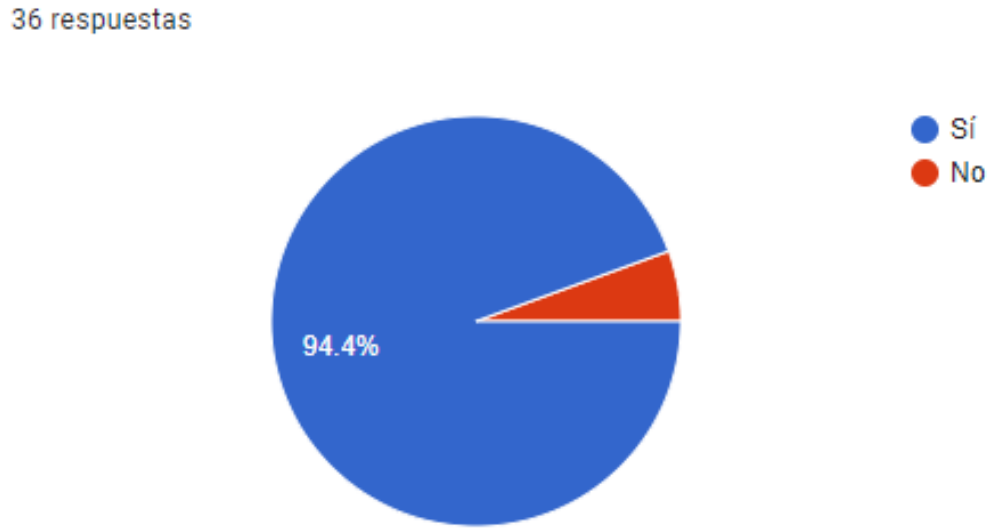
Nota. Respuesta de los encuestados, donde se refleja que el 91.7 % (33), indica que la propuesta de buenas prácticas aporta a garantizar la integridad de la evidencia digital en el cloud computing.

16. ¿Aplicaría la propuesta de buenas prácticas en mención para recolectar y garantizar la integridad de la evidencia digital en el cloud computing?

En respuesta a esta pregunta el 94.4 % (34) de los encuestados, indica que aplicaría la propuesta de buenas prácticas en mención para recolectar y garantizar la integridad de la evidencia digital en el cloud computing, mientras que el 5.6 % (2) indico que no. (fig. 28), basados en la anterior respuesta, se puede inferir que la propuesta es aprobada por un gran porcentaje de expertos, los cuales aplicarían en escenarios relacionados con el cloud computing, lo que la convierte en una buena práctica para implementar y replicar.

Figura 28

Aplicación de la Propuesta de Buenas Prácticas por parte de los Peritos, para Recolectar y Garantizar la Integridad de la Evidencia Digital en el Cloud Computing



Nota. Respuesta de los encuestados, donde se evidencia que el 94.4 % (34), aplicaría la propuesta de buenas prácticas, para recolectar y garantizar la integridad de la evidencia digital en el cloud computing.

Conclusiones

El análisis de las publicaciones, documentos, normas, manuales, guías, libros y los artículos relacionados con las buenas prácticas en el manejo de la evidencia digital, así como la transformación tecnológica de sus medios de almacenamiento, nos permiten conocer los procedimientos utilizados a nivel internacional, para garantizar la recolección y preservación de la evidencia digital en el cloud computing.

Las mejores prácticas relacionadas con la recolección y preservación de la evidencia digital, ayuda a los interesados en la disciplina de informática forense, ha adquirir nuevos conocimientos, que aportan al fortalecimiento de la disciplina en la aplicación de estándares y normas, que minimizan los riesgos que se puedan presentar al obtener evidencia digital en la nube.

El diseñó de esta buena práctica para la recolección y preservación de la evidencia digital en el cloud computing, permite a los encargados de garantizar la integridad de esta, establecer procedimientos estandarizados que la salvaguardan, aplicando y cumpliendo con los protocolos de cadena de custodia, lo cual es requerido por las autoridades administrativas y judiciales para validar su autenticidad.

Las cinco fases que componen esta propuesta, dan a conocer las buenas prácticas que se deben aplicar para el manejo de la evidencia digital en la nube, las cuales buscan mejorar el proceso de planeación, identificación, recolección u obtención, preservación y documentación de la evidencia digital en el cloud computing, así como servir de herramienta para que todas las personas relacionadas con esta , garanticen la calidad en los proceso de recolección y garantía de integridad de la evidencia digital, lo que permitirá que esta sea aceptada y valorada en los diferentes procesos judiciales como prueba.

La propuesta de buenas prácticas en la recolección y garantía de integridad de la evidencia digital en el cloud computing, una vez evaluada por parte de expertos en la disciplina de informática forense, permite su aplicabilidad y se convierte en material de consulta, tanto de peritos, como de interesados en la materia.

Recomendaciones

Debido a la diversidad que tiene la evidencia digital, es necesario tener en cuenta las buenas prácticas establecidas para el manejo de esta de acuerdo a sus características y los diferentes medios de almacenamiento digital en los cuales se encuentren, por lo cual estas deben actualizarse permanentemente, teniendo en cuenta los cambios tecnológicos que se presenten con referencia a la recolección, almacenamiento, y preservación de evidencia digital, entre los que se encuentran el uso de la inteligencia artificial, el blockchain y la criptografía cuántica.

Referencias Bibliográficas

Abdellah Akilal, M-Tahar Kechadi, (2022). An improved forensic-by-design framework for cloud computing with systems engineering standard compliance, Forensic Science International: Digital Investigation, Volume 40. https://www.sciencedirect.com/science/article/pii/S2666281721002407

AWS, (2024). ¿Qué es AWS CloudTrail? https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

B. Dhake, H. Limaye and D. Motwani, (2022). "Cloud Forensics: Threat Assessment and Proposed Mitigations," 2022 International Conference for Advancement in Technology (ICONAT), pp. 1-6. https://ieeexplore.ieee.org/document/9725922

Belkasoft. (2024) Belkasoft Acquisition Tool. https://belkasoft.com/es/bat

Bernal, Cesar A. (2010). Metodología de la investigación. Tercera edición. https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci %C3% B3n-F.G.-Arias-2012-pdf.pdf

Cellebrite. (2024). Analizador de nubes UFED. https://cellebrite.com/en/ufed-cloud-analyzer-5/

Consejo de Europa. (2001). Informe explicativo del convenio sobre la ciberdelincuencia. https://rm.coe.int/16802fa403

DAFF. (2004). Guidelines on the Use and Control of Electronic Records for Statutory Compliance

https://www.agriculture.gov.au/sites/default/files/sitecollectiondocuments/aqis/exporting/meat/elmer3/index/methods-microbiological-test-meat/Guidelines_Use_and_Control_of_Electro nic_Records_for_Stat_Comp_Ver1Read_in_conjunction_with_AMN200701_.doc

EDRM (EDRM.NET). (2020). Modelo EDRM. https://edrm.net/edrm-model/current/

EDRM (EDRM.NET). (2023). Modelo EDRM actual https://edrm.net/wiki/edrm-model/

El Pacto - Programa de Asistencia contra el Crimen Transnacional Organizado. (2022). La prueba electrónica en el marco nacional y en el internacional en Latinoamérica. https://www.elpaccto.eu/wp-content/uploads/2022/08/Publicacion-prueba-electronica-EL-PAcCTO.pdf

Fuentes, Fernando. (2022). Análisis forense en cloud: ¿qué es y en qué consiste? https://www.arsys.es/blog/analisis-forense-cloud

Garner. Costello, Katie. (2020). La guía del CIO para la nube distribuida. https://www.gartner.es/es/articulos/la-guia-del-cio-para-la-nube-distribuida

Garner. Costello, Katie. (2021). Gartner predice el futuro de las infraestructuras de Cloud y Edge Computing. https://www.gartner.es/es/articulos/gartner-predice-el-futuro-de-las infraestructuras-de-cloud-y-edge-computing

Geeksforgeeks. (2023). Modelo forense digital abstracto. https://www.geeksforgeeks.org/abstract-digital-forensic-model/

Guevara Patiño, Ragnhild, (2016). El estado del arte en la investigación: ¿análisis de los conocimientos acumulados o indagación por nuevos sentidos?, Revista Folios, núm. 44, julio-diciembre, 2016, pp. 165-179, Universidad Pedagógica Nacional, Bogotá, Colombia. https://www.redalyc.org/pdf/3459/345945922011.pdf

Herman M, Iorga M, Salim AM, Jackson RH, Hurst MR, Leo RA, Mishra AK, Landreville NM, Wang Y (2022). Arquitectura de referencia forense de computación en la nube del NIST. (Instituto Nacional de Estándares y Tecnología, Gaithersburg, MD), Publicación especial del NIST (SP) 800-201 ipd. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-201.ipd.pdf

Ibermatica. (2020). No todas las nubes son iguales, descubre que servicio te conviene más. https://www.ibermatica365.com/no-todas-las-nubes-son-iguales-descubre-que-servicio-te-conviene-mas/

INCIBE. (2014). RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento. https://www.incibe.es/incibe-cert/blog/rfc3227

INTERPOL. (2021). Guidelines for digital forensics first responders, best practices for search and seizure of electronic and digital evidence. https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf

Ismsforum, (2023). Guía de ISMS Fórum, Antes, durante y después de ir a la Nube, Respuesta ante Incidentes https://www.ismsforum.es/backoffice/ckfinder/userfiles/files/guia-incidencias-nube-2023

1678875623.pdf

Ismsforum. (2018). CLOUD AUDIT & FORENSICS. https://www.ismsforum.es/ficheros/descargas/cloudauditforensics2018v41544463021.pdf

ISO 9000. (2015). Sistemas de gestión de la calidad — Fundamentos y vocabulario. https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:es

ISO/CEI 27000. (2018). Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Visión general y vocabulario. https://www.iso.org

ISO/CEI 27001. (2022). Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información-Requisitos. https://www.iso.org

ISO/CEI 27002. (2022). Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información. https://www.iso.org

ISO/CEI 27005. (2022). Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de los riesgos de seguridad de la información. https://www.iso.org

ISO/CEI 27017. (2015). Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube. https://www.iso.org

ISO/CEI 27037. (2012). Directrices para la identificación, recolección, adquisición y preservación de evidencia digital.

https://www.iso.org

ISO/CEI 27042. (2015). Tecnología de la información. Técnicas de seguridad. Directrices para el análisis y la interpretación de las evidencias electrónicas. https://www.iso.org

IT Masters Mag. (2023). Análisis forense digital ¿Cómo se realiza? Técnicas, pasos y mejores prácticas. https://www.itmastersmag.com/noticias-analisis/como-se-realiza-un-analisis-forense-digital-tecnicas-pasos-y-mejores-practicas/

Karen Kent and S. Chevalier and Timothy Grance and Hung Dang, (2006), Guide to Integrating Forensic Techniques into Incident Response. https://api.semanticscholar.org/CorpusID:64816814

López, Pedro Luís. (2004). Población muestra y muestreo. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1815-02762004000100012

Magnet Forensic. (2024). AXIOM Cloud https://www.magnetforensics.com/resources/axiom-cloud/#

Metaspike, (2024). Forensic Email Collector https://www.metaspike.com/forensic-email-collector/#intro

MINTIC, (2016) Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. https://www.mintic.gov.co/gestionti/615/articles5482_G21_Gestion_Incidentes.pdf

MOBILedit. (2024). Cloud Forensic https://www.mobiledit.com/cloud-forensic

Network Working Group, D. Brezinski, (2002). Request for Comments: 3227 (RFC3227), Directrices para la recopilación y el archivo de pruebas. https://www.ietf.org/rfc/rfc3227.txt

NIST. (2020). NISTIR 8006. NIST Cloud Computing Forensic Science Challenges https://csrc.nist.gov/publications/detail/nistir/8006/final

NIST. (2011). NIST SP 800-145, The NIST Definition of Cloud Computing. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

NIST. (2011). Guide to Security for Full Virtualization Technologies. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=907776

NIST. (2006). NIST 800-86. Guide to Integrating ForensicTechniques into Incident Response. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Normas Internacionales de Austrália, (2003). HB:171, Guidelines for the Management of IT Evidence. https://www.saiglobal.com/pdftemp/previews/osh/as/misc/handbook/hb171.pdf

Oficina de las Naciones Unidas Contra la Droga y el Delito - UNODC. (2022). Guía práctica para la solicitud de pruebas electrónicas transfronterizas. https://sherloc.unodc.org/cld/uploads/res/st/evidence/practical-guide_html/22-00094_Practical_Guide_S_ebook_Final.pdf

Organización de las Naciones Unidas para la Alimentación y la Agricultura (FAO). (2014). Plantilla de Buenas Prácticas. https://www.fao.org/3/as547s/as547s.pdf

Oxygen Forensics. (2024), Explorador remoto.

https://oxygenforensics.com/en/products/oxygen-remote-explorer/

Oxygen Forensics. (2024), Oxygen Forensic® Cloud Extractor. https://oxygenforensics.com/es/resources/oxygen-forensic-cloud-extractor/

Paba B., Carmelina, Paba A., Zuany, Rodríguez D, Ubaldo, (2014), Guía Práctica para la presentación de informes de investigación y artículos científicos (Normas APA). https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/70094

Palomo, L. E., & Guillet, S. M. (2021). EVIDENCIA DIGITAL DE LA NUBE. EL APORTE PROBATORIO EN SANTIAGO DEL ESTERO. Difusiones, 21(21), 59–75. http://ediciones.ucse.edu.ar/ojsucse/index.php/difusiones/article/view/394

Quecedo, Rosario; Castaño Carlos, (2002). Introducción a la metodología de investigación cualitativa. Revista de Psico didáctica, núm. 14, pp. 5-39. Universidad del País Vasco/Euskal Herriko Unibertsitatea Vitoria-Gazteis, España. https://www.redalyc.org/articulo.oa?id=17501402

Salesforce. (2022). Cloud Computing: Aplicaciones en un solo lugar. https://www.salesforce.com/mx/cloudcomputing/#:~:text=De%20una%20manera%20simple%2C%20la,computadora%20personal%20o%20servidor%20local.

Senado de la República de Colombia, (1999. Ley 527, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Semprini, G., Nilles, G., & Silva, G. (2021). Metodología de obtención de Evidencia en la Nube. Electronic Journal of SADIO (EJS), 20(1), 102-116.

https://publicaciones.sadio.org.ar/index.php/EJS/article/view/187

Scientific Working Group on Digital Evidence. (2006). SWGDE Data Integrity Within Computer Forensics. https://www.swgde.org/documents/published-complete-listing

Scientific Working Group on Digital Evidence. (2020). SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers. https://www.swgde.org/documents/published-by-committee/forensics

Tamayo, Carla; Silva S., Irene. Universidad católica los ángeles de Chimbote. (2022). Técnicas e instrumentos de recolección de datos. https://www.postgradoune.edu.pe/pdf/documentos-academicos/ciencias-de-la-educacion/23.pdf

Vargas, Ana Cecilia y Castro Mattei, Alonso. (2007). Sistemas de gestión de seguridad de la información [en línea]. San José Costa Rica: Universidad de Costa Rica, s.f. [citado el 22-04-16]. http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

Vella, Mark & Colombo, Christian. (2022). D-Cloud-Collector: Admissible Forensic Evidence from Mobile Cloud Storage. https://www.researchgate.net/publication/361043416_D-Cloud-Collector_Admissible_Forensic_Evidence_from Mobile_Cloud_Storage