Manejo de la evidencia digital con visión en normas internacionales aplicables por los primeros interventores y peritos forenses en Ecuador

Management of digital evidence with a view to applicable international standards by the first auditors and forensic experts in Ecuador

Fernando Mauricio De la Torre Muñoz[1]
Alejandro Xavier Puertas Realpe [2]
Christian Eduardo Burbano Peña[3]

Recibido: 25 de octubre de 2024
Aceptado: 10 noviembre de 2024
Publicado: 27 noviembre de 2024

Resumen

Este artículo tiene por objetivo, tomando por referente algunos elementos de los estándares internacionales (ISO) y los protocolos y procedimientos para el manejo de la evidencia digital (RFC), diseñar una herramienta metodológica que permita la estandarización de los procesos de observación, recolección, individualización, registro, sellado, traslado y tratamiento de la evidencia digital. En este sentido, se propone la creación de un instrumento que oriente a los primeros responsables como a los peritos forenses en el manejo inicial de la evidencia digital. Este tipo de directrices no está disponible en Ecuador, por lo que el instrumento contribuirá a que la evidencia se inserte en los principios de seguridad y legalidad, garantizando así su admisibilidad, credibilidad, confiabilidad, autenticidad y completitud ante las autoridades nacionales.

Palabras clave: especialista; evidencia digital**;** ISO**;** normas; RFC; responsable.

Abstract

The objective of this article is to design a methodological tool, taking as a reference some elements of the international standards (ISO) and the protocols and procedures for the handling of digital evidence (RFC), that allows the standardization of the processes of observation, collection, individualization, registration, sealing, transfer and treatment of digital evidence. In this sense, it is proposed the creation of an instrument to guide first responders and forensic experts in the initial handling of digital evidence. This type of guidelines is not available in Ecuador, so the instrument will help to ensure that the evidence is inserted in the principles of security and legality, thus ensuring its admissibility, credibility, reliability, authenticity and completeness before the national authorities.

Keywords: specialist; digital evidence**;** standards; ISO, RFC; manager.

1 Estudiante de la sexta cohorte de Criminalística, Isupol, fermaudelatorre@gmail.com 0009-0008-2433-9224
2 Estudiante de la sexta cohorte de Criminalística, Isupol, saint-alejandro@hotmail.com 0009-0006-2268-7001
3 Estudiante de la sexta cohorte de Criminalística, Isupol, Kriiizthburbano02@hotmail.com 0009-0002-1584-7290

Introducción

La primera labor de las diferentes unidades policiales en la escena del crimen consiste en preservar el lugar lo más intacto posible, evitar cualquier alteración, pérdida y manipulación de elementos físicos, biológicos y electrónicos: "[…] el contacto entre una persona, un lugar o una cosa implica un intercambio de materiales físicos, lo que permite a los investigadores utilizar estos indicios para reconstruir los hechos e identificar a los involucrados en un delito" (Locard 2010, p. 1).

Ecuador enfrenta un aumento en la delincuencia y el crimen, lo que ha generado una mayor carga laboral para el personal de la Policía Nacional del Ecuador (PNE). Los robos a personas, domicilios y vehículos, así como las extorsiones, secuestros, sicariatos, homicidios, entre otras modalidades delictivas, han evolucionado significativamente. Las organizaciones delictivas han incorporado tecnologías avanzadas para identificar a sus posibles víctimas, mejorar su comunicación, facilitar el lavado de dinero, realizar transacciones económicas, entre otras. La *tecnificación de la delincuencia* genera nuevas evidencias delictivas cuyo tratamiento, manejo y preservación garantiza una mayor efectividad de las investigaciones realizadas por la PNE (Castellanos 2017).

En este contexto, la PNE como entidad responsable de las investigaciones posdelito, ha desbordado su capacidad operativa debido al aumento de la actividad delictiva, por la complejidad de los casos y el débil sistema de administración de justicia. Esta situación ha obligado a la institución a desarrollar nuevas estrategias para enfrentar estos desafíos, mejorar sus procedimientos mediante la creación de protocolos de actuación, instaurar herramientas de gestión en situaciones de crisis, profesionalizar las labores investigativas, actualizar los conocimientos y capacitar a todo el personal policial (Policía Nacional 2022).

Una de las estrategias es la capacitación del personal, es decir, dotarlo de conocimientos que le permita contar y aplicar herramientas eficientes y eficaces que apunten a una mayor obtención de los indicios criminales. Por ejemplo, el primer interventor en una situación de crisis (América 2013) tiene una enorme responsabilidad ya que es la primer persona que entra en contacto con la escena del crimen y, por ende, debe poseer los conocimientos básicos para la protección de evidencias que vaya encontrando. Esta persona es la responsable de asegurar, proteger y preservar los indicios físicos y digitales (ISO/EC 27037 2012). Posee atribuciones legales y la facultad para actuar dentro de la cadena de custodia. En Ecuador las personas que cumplen esta labor son los peritos de inspección ocular técnica, agentes investigadores o de inteligencia y, personal del eje preventivo de la PNE.

Este artículo contiene y presenta una herramienta técnica y metodológica que servirá de guía en los procesos de observación, recolección, individualización, registro, sellado, traslado y tratamiento de la evidencia digital en el ámbito legal. Parte de los protocolos de la Organización Internacional de Normalización ISO/IEC 27037:2012 e ISO/IEC 27042:2016 y los Request for Comments (RFC) 3227, 4810 y 4998. Se busca estandarizar los procedimientos relacionados con el manejo de evidencia física y digital el cual incluye el levantamiento de la evidencia, el manejo adecuado de la cadena de custodia, ingreso al laboratorio forense y los objetos de pericia a realizarse considerando la normativa legal de Ecuador.

Marco teórico

Todo elemento físico, biológico o electrónico dentro de una escena del crimen es considerado un indicio[4] que debe ser localizado, fijado, levantado, rotulado y sellado. Este indicio se pueda transformar en una evidencia, entendida como: "Cualquier dato o información que pueda ser utilizado para determinar o demostrar la veracidad, que prueba un hecho realizado o bien que no se ha realizado" (Gómez- Agudelo 2020, p. 220-240). Esta evidencia ayudará en el proceso

4 Se denomina así a todo objeto, huella o elemento íntimamente relacionado con un probable hecho delictivo, cuyo estudio permite reconstruirlo, identificar a su autor o autores y establecer su comisión.

investigativo y, de suma importancia, para la resolución de un caso.

En Ecuador la evidencia digital puede ser cualquier objeto que haya sido intervenido, u otra similar, extraído de un sistema informático. Por consiguiente, es entendida como: "La materia prima para los investigadores, donde la tecnología informática es parte fundamental del proceso. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad: Es volátil, es anónima, es duplicable, es alterable y modificable, es eliminable" (Martínez 2020, p. 29-39). Esta definición guarda estrecha relación con la guía publicada por el Department of Justice Computer Crime and Intellectual Property Section of United States.[5]

Esta guía permite inferir si la evidencia digital fue creada o generada por una persona o un dispositivo electrónico, es decir, si los documentos fueron creados en forma y formato electrónico y, ayuda a identificar el software que lo generó. Esta información es útil para los operadores de justicia[6] ya que suministra información sobre los hechos contenidos en la evidencia digital. Un ejemplo de ello son los dispositivos móviles del que es posible conocer su dueño, los mensajes de textos y los *logs files*[7] o registros telefónicos.

Ecuador necesita incursionar en estas discusiones, estándares y modelos internacionales que le permitan identificar, recolectar, adquirir y preservar evidencia digital. La evidencia debe tener valor probatorio. Las ISO[8] que debe aplicar el país son la *Information Technology Security Techniques Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/EC 27037 2012), así como la I*nformation Technology Security Techniques Guidelines for the analysis and interpretation of digital evidence* (DS/EN ISO/IEC 27042 2016).

Otras estándares que servirían de apoyo para la creación de un manual o instructivo que estandarice el manejo de la evidencia digital son los RFC conocidos por ser: "Documentos numerados que incluyen valoraciones, descripciones y definiciones de protocolos, conceptos, métodos y programas en línea" (NFON 2024). Para los fines de este artículo se pudo identificar los RFC 3227, 4810 y 4998.

Por otro lado, toda evidencia digital debe ser relevante, confiable y suficiente (Incibe 2014). Estos principios permiten que los procedimientos técnicos ayuden a preservar la información de la evidencia (Brandner 2007), así como también, "definir el procedimiento y el propósito general a fin de probar la existencia y validez de los datos" (Pordesch 2007) con el objetivo de que la evidencia no sea rechazada en alguna instancia jurídica procesal.

El primer responsable de la escena del crimen (o detectives especializados en la función de recolección [DEFR]) debe ser consciente de sus competencias, las cuales consisten en identificar, recolectar, consolidar y preservar la evidencia y contenido digital en una escena en la que se ha cometido una infracción. Esta persona no debe manipular la evidencia digital, excepto cuando prevea conseguir datos volátiles[9] o se efectúen operaciones urgentes debiendo documentar e informar al administrador de justicia el proceso realizado. Su técnica o metodología se fundamentaría con la RFC 3227.

Al contrario, el especialista en evidencia digital (o detectives especializados en la función de análisis y evaluación [DES]) es quien proporciona instrucciones específicas, ayuda con el análisis e interpretación y forja conclusiones de la evidencia digital. Según la ISO/EC 27037 2012 esta persona es quien: "[…] Da un grado de continuidad, validez, reproductividad y repetibilidad

5 Searching and seizing computers and obtaining electronic evidence in criminal investigations, https://www.combattingcybercrime.org/files/virtual-library/national-laws/searching-and-seizing-computers-and-obtaining-electronic-evidence-in-criminal-investigation.pdf

6 Los administradores de justicia en Ecuador desempeñan un rol fundamental en la aplicación imparcial de la ley, la protección de los derechos de los ciudadanos y la garantía de un sistema judicial efectivo y transparente.

7 Archivos que registran eventos y actividades importantes dentro de un sistema informático.

8 Es una organización no gubernamental con sede en Ginebra. Se trata de una red de organismos nacionales de normalización que elabora y publica normas internacionales. Desde su fundación en 1946, la ISO ha elaborado más de 20 000 normas internacionales y documentos relacionados.

9 Son aquellos datos que se almacenan en la memoria del sistema (por ejemplo, registros de sistema, caché, memoria RAM) y se pierden si el equipo se apaga o reinicia.

de la evidencia digital". Además, según Ochoa Arévalo (2018, p. 35-49): "Los especialistas en informática forense, no pueden bajar la guardia, ya que la evolución en este campo no puede medirse ni en años, ni en meses, sino en días".

La creación de una herramienta metodológica de este tipo es necesaria para el correcto manejo de la evidencia digital por parte de los DEFR y DES. Para ello, es necesario acoplar los procedimientos de acuerdo con la legislación nacional ya que, según la Constitución de la República del Ecuador, "las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria" (2018, artículo 76, literal 4). Corresponde a la PNE y a la Fiscalía General del Estado desarrollar todas las actividades pertinentes para la obtención de las pruebas de cargo y de descargo en un proceso penal, por tal razón, la generación de un manual estandarizaría el manejo de la evidencia digital de ambas instituciones basado en normas internacionales.

Metodología

Este artículo, a partir de una metodología cualitativa de tipo hermeneútica, contiene una propuesta técnica que permitiría estandarizar el levantamiento y tratamiento de la evidencia digital entre el personal de la PNE y Fiscalía General. Según Piña-Ferrer (2023), el enfoque cualitativo busca "[…] describir, explicar y predecir los espacios complejos en los que nos movemos", indagando el fenómeno, es decir, la evolución de los indicios que pueden ser materiales o digitales.

Según Maldonado (2016) el enfoque hermenéutico es el "arte de interpretar textos en la búsqueda de su verdadero sentido". Esto concuerda con lo expresado por Coreth (1972) en su libro titulado *Cuestiones fundamentales de la hermenéutica* quien destaca que la hermeneútica se basa en la interpretación de los textos. Entonces, es posible interpretar las ISO/IEC 27037:2012 y 27042:2016 y los RFC 3227, 4810 y 4998 desde las siguientes inquietudes: ¿Cuál es el procedimiento inicial que debe tener en cuenta el DEFR frente a una evidencia digital? ¿cómo llega a manos del DES la evidencia digital y cómo garantiza que esta no pierda sus características legales?[10]

Esta propuesta parte, entonces, del análisis de la información relevante que consta en las normas ISO/IEC 27037:2012 y 27042:2016 y los RFC 3227, 4810 y 4998. Partiendo que el derecho internacional y los acuerdos internacionales no pueden interferir con las disposiciones constitucionales, se busca estandarizar el levantamiento y tratamiento de los equipos computacionales, dispositivos de almacenamiento, dispositivos de red, dispositivos móviles, sistemas basados en la nube y tecnología exponencial. Por consiguiente, se presenta una investigación bibliográfica y documental.

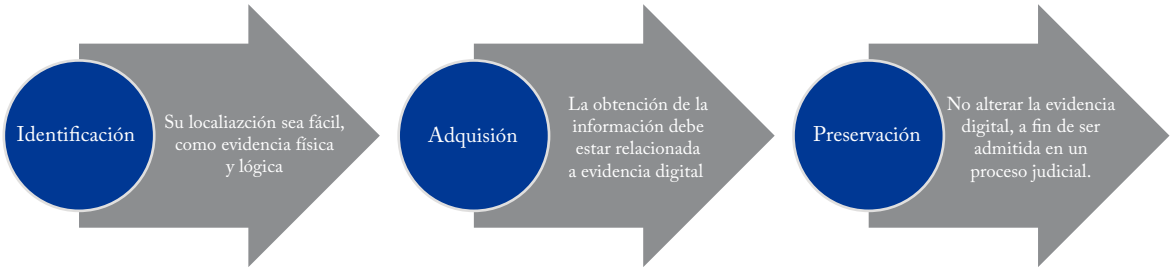
Esta propuesta parte de un muestreo por conveniencia debido a la facilidad de acceso que se tuvo a la población objeto de esta metodología que son los DEFR y DES. Los DEFR constan en los ejes preventivo, investigativo y de inteligencia de la PNE y son los actores iniciales que tienen acceso a la evidencia digital por ser los primeros que llegan a la escena del crimen. Por su parte, los DES son todos los peritos acreditados por el Consejo de la Judicatura que trabaja en el Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses. Los DES determinan el debido tratamiento de la evidencia digital.

Esta propuesta técnica se presenta en un diagrama de flujo que contiene los pasos para el levantamiento y tratamiento de la evidencia digital. De acuerdo con la Organización de Estados Americanos (OEA 2019) los países de América Latina y el Caribe necesitan un mejoramiento de los distintos elementos que intervienen en el tratamiento, adquisición y recopilación de la evidencia digital. Ecuador no es la excepción del caso.

10 Características legales de la evidencia digital: admisible, creíble, confiable, auténtica y completa.

Gráfico 1

Digital evidence management



Fuente: por los autores.

Elaboración: por los autores.

Análisis y discusión de resultados

ISO 27037: 2012 Guidelines for identification, collection, acquisition, and preservation of digital evidence (ISO 2012)[11]

Esta norma ofrece directrices para la comprobación de las pruebas digitales, la promoción de la gestión para la preservación y sostenimiento de los dispositivos de almacenamiento. La ISO sostiene que la evidencia debe ser obtenida mediante una metodología cuyo procedimiento sea auditable, como también, reproducido por otros peritos informáticos dando un mismo resultado. Por ende, el procedimiento (*Digital evidence management o* gestión de evidencia digital) sería defendido y demostrado dentro de una investigación. Además, esta norma se refiere actividades específicas para el potencial intercambio de evidencia digital entre jurisdicciones.

ISO 27042:2016 Guidelines for the analysis and interpretation of digital evidence (ISO 2016)[12]

Esta norma es útil para aclarar e investigar en los procesos judiciales el análisis fijo[13] y análisis en vivo[14] de la evidencia digital, recolectada en un hecho delictivo. Otorga continuidad, validez, reproducibilidad y repetibilidad a la evidencia, además, que define conceptos que ayudan al entendimiento de la situación forense. Esto facilita la intervención del DES quien puede desempeñarse como testigo dentro de un juicio. Otro elemento que destaca de esta ISO es que proporciona ayuda de los documentos que el DES debe presentar ante los tribunales anexados a su pericia de modo que se procura que no exista alguna objeción por parte de una autoridad competente. Aspectos como la alineación y el sustento de actividades de calidad están orientadas a la comisión de la evidencia digital.

RFC 3227 Directrices para la recolección de evidencias y su almacenamiento[15]

Este manual tiene por objetivo que el DEFR y el DES no pierdan información alojada dentro de una evidencia digital, en precisas circunstancias como al momento de extraer información cuando un dispositivo electrónico[16] se encuentre encendido o apagado de una red. Este manual también deja claro los principios de recolección de una evidencia, estos son: digital, digital potencial o digital legal. A continuación, se presentan los principios en la recolección de las evidencias:

11 ISO 27037:2012: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

12 ISO 27042:2016: https://tienda.aenor.com/norma-une-en-iso-iec-27042-2016-n0057471.

13 Es el reconocimiento de la evidencia digital potencial a fin de evaluar si se puede considerar evidencia digital, utilizando procedimientos que no la alteren.

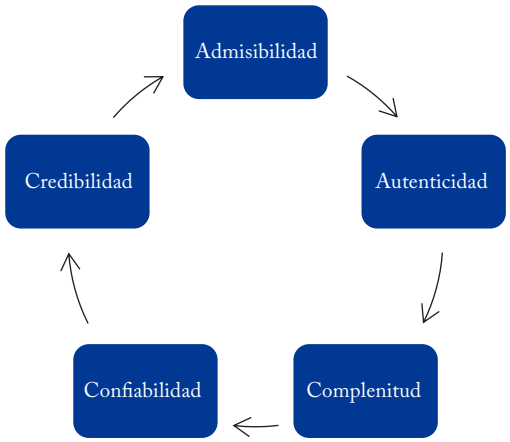
14 Es la comprobación de evidencias digitales potenciales en dispositivos como RAM, smartphones, redes de ordenador, entre otros.

15 RFC 3227: https://www.incibe.es/incibe-cert/blog/rfc3227

16 Ordenadores, impresoras, copiadoras, máquinas de escribir eléctricas o electrónicas, calculadoras de mesa o de bolsillo, teléfonos de todo tipo, terminales de faxes y otros productos de transmisión de sonido, imágenes u otra información por telecomunicación.

Gráfico 2

Principios de la recolección de evidencia digital



Fuente: Manual RFC 3227 para la recolección de evidencias y su almacenamiento.

Elaboración: por los autores.

Estos principios apuntan a que los procedimientos de recolección de la evidencia digital sean claros y estandarizados con el fin que, una vez completado el proceso, la evidencia sea válida y admisible ante una autoridad competente. De esta manera, se asegura el inicio de la cadena de custodia de los elementos recolectados en el lugar de los hechos o en la escena del crimen.

RFC 4810 Directrices para la preservación de la información (como objeto de estudio la creación y existencia de un archivo)[17]

Contiene las buenas prácticas para la recolección y almacenamiento de la información que garantizan su integridad en el menor tiempo posible, de modo que la evidencia conserve su valor. Este proceso es de gran apoyo para el DES en la presentación de su pericia pues asegura que la información no sea rechazada por la autoridad competente. Este RFC ofrece directrices para examinar, verificar, especificar características y validar cualquier tipo de archivo.[18] Un buen ejemplo es la verificación de la autenticidad de una firma digital, incluso, tiempo después de su creación.

RFC 4998 Directrices para la preservación de la información (como objeto de probar la existencia y validez de información)[19]

Este instrumento contiene los lineamientos de preservación de los datos, lo cual incluye las firmas electrónicas, así como la validez de la evidencia digital durante un período determinado. De esta manera el DES puede sustentar ante la autoridad competente la presencia de la información en la evidencia digital (legal) y demostrar su validez. El instrumento también define los tipos de archivos y establece los requisitos que debe cumplir una evidencia digital.

Propuesta metodológica para los DEFR

En el inicio de un procedimiento en el cual sea necesaria la actuación policial, es primordial que las diferentes unidades sean despachadas mediante el operador del SIS ECU 911 quien se encarga de recibir el llamado de auxilio por parte de la ciudadanía y, dependiendo del tipo de emergencia, despacha las unidades que sean necesarias. La unidad designada avanza hasta el sitio del suceso. Es allí cuando entra en escena el DEFR quien debe cumplir con lo siguiente:

- **Observación y valoración del lugar:** el DEFR, en el sitio del suceso, debe analizar el tipo de escena y establecer el método idóneo para la protección del lugar y preservación de la mayor cantidad de indicios.
- **Identificación de riesgos iniciales:** el DEFR deberá verificar las posibles amenazas de seguridad a las que se encuentran expuestos los equipos que intervienen. Por ejemplo, los artefactos sospechosos, el tendido eléctrico colapsado, las estructuras fracturadas, entre otros. Deberá mitigar cualquier amenaza solicitando la intervención de las instituciones correspondientes.

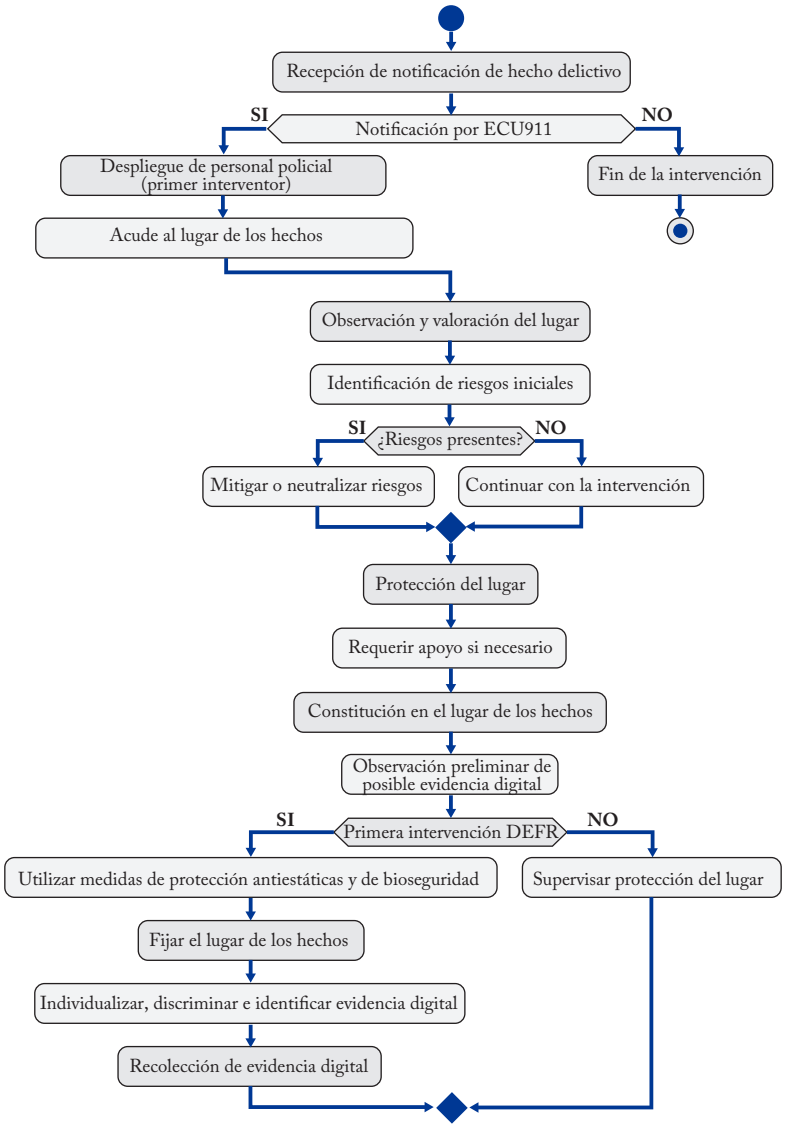
17 RFC 4810: https://datatracker.ietf.org/doc/html/rfc4810

18 Los sistemas de archivos o arquitectura de ficheros son la forma en la que los sistemas operativos organizan la información y la indexan en las particiones de almacenamiento para acceder a ella de forma eficiente, tanto para leer como para escribir.

19 RFC 4998: https://datatracker.ietf.org/doc/html/rfc4998

Gráfico 3

Diagrama de flujo del procedimiento inicial del DEFR



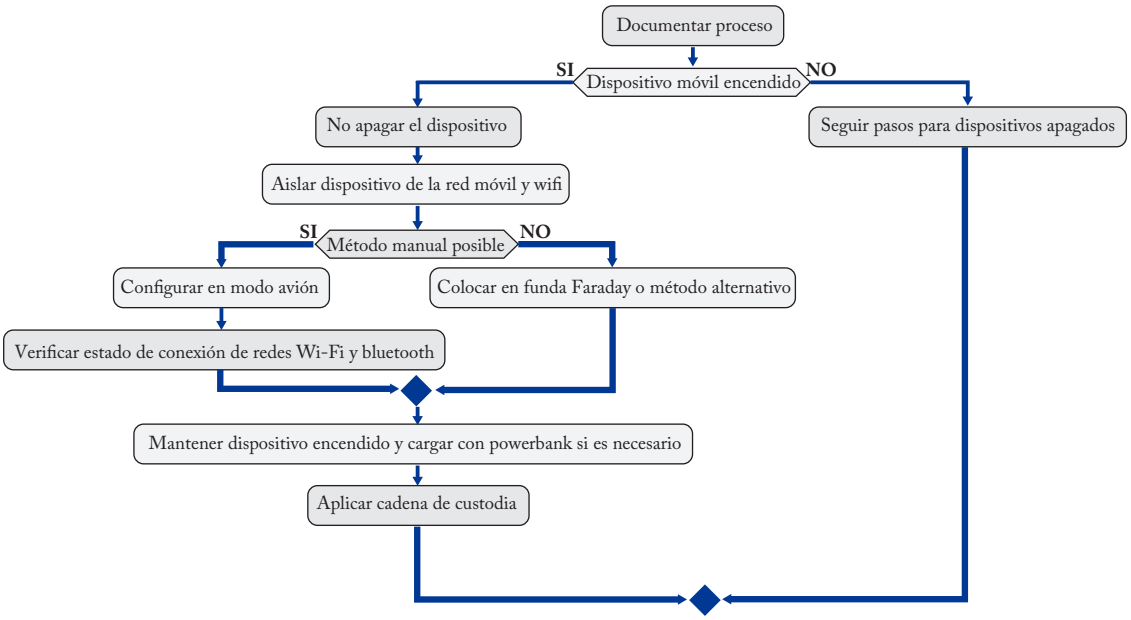
Fuente: procedimiento inicial del DEFR

Elaboración: por los autores.

- **Protección del lugar:** el DEFR puede delimitar el sitio del suceso y restringir el acceso con la finalidad de proteger la escena y evitar la contaminación de la misma. Así también, la de resguardar los indicios.
- **Requerir apoyo si es necesario:** el DEFR deberá establecer, de acuerdo a las necesidades del hecho, cuáles son las unidades especializadas o de apoyo necesarias para el tratamiento y procesamiento de la escena.

Gráfico 4

Diagrama de flujo de la actuación del DEFR en dispositivos móviles



Fuente: la actuación del DEFR en dispositivos móviles.

Elaboración: por los autores.

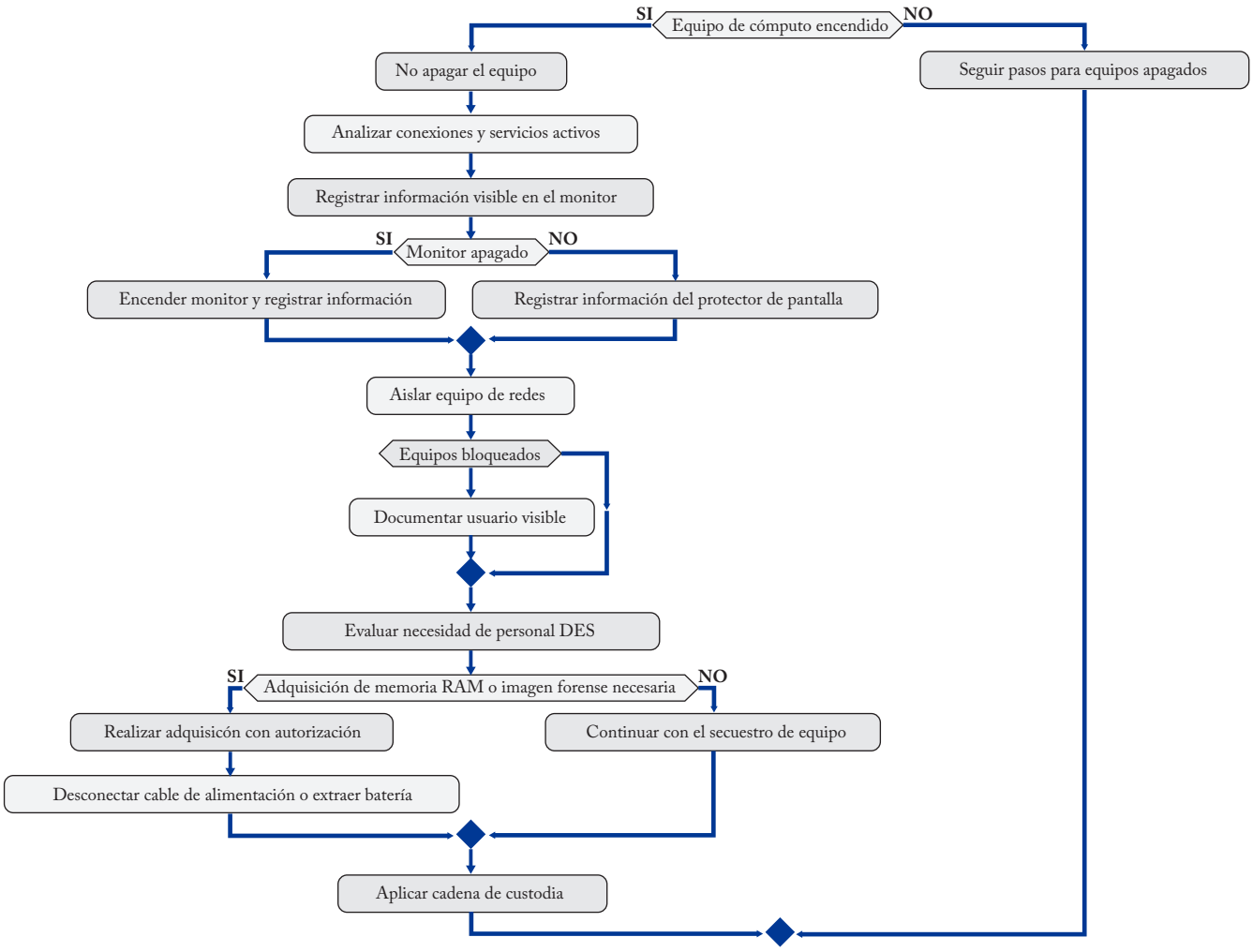
- **Constitución en el lugar de los hechos:** efectuados los procedimientos anteriores, el DEFR se posiciona en el sitio del suceso y establece los posibles indicios a ser levantados. Entre esos debe identificar los indicios de naturaleza digital que son los más propensos a desaparecer por sus características volátiles. Localizados estos indicios, utilizará las medidas de protección antiestática y bioseguridad para proteger el dispositivo y, fijará el lugar donde se encuentra el indicio que debe ser individualizado. Posterior a ello, realizará la recolección, además que levantará la documentación respectiva.

Si bien, el procedimiento brinda en líneas generales las directrices que debe realizar el DEFR en la escena del crimen, para realizar el adecuado manejo de los equipos digitales o tecnológicos, debe tomar en consideración una serie de detalles para la obtención de la información que reposa en los dispositivos. Entre estos detalles se encuentra:

- Determinar si el dispositivo móvil se encuentra encendido o apagado ya que de esto dependerá el tipo de procedimiento que deba realizar.
- Si el dispositivo móvil está apagado, deberá fijar el lugar en dónde se encontró. El DEFR no debe manipular o intentar encender el dispositivo. Se realizará la fijación fotográfica del indicio para individualizarlo, levantarlo y trasladarlo en un contenedor adecuado.
- Si el dispositivo móvil se encuentra encendido, deberá evitar al máximo su manipulación y tendrá prioridad para su tratamiento ya que la información contenida es demasiado volátil. No debe intentar apagarlo, al contrario, propenderá a que permanezca encendido utilizando un *powerbank*. Debe verificarse que las conexiones wifi y bluetooth se encuentren deshabilitadas, de ser posible se colocará el dispositivo en modo avión y

Gráfico 5

Diagrama de flujo de la actuación del DEFR en ordenadores



Fuente: la actuación del DEFR en ordenadores.

Elaboración: por los autores.

para su traslado deberá utilizar fundas Faraday.[20]

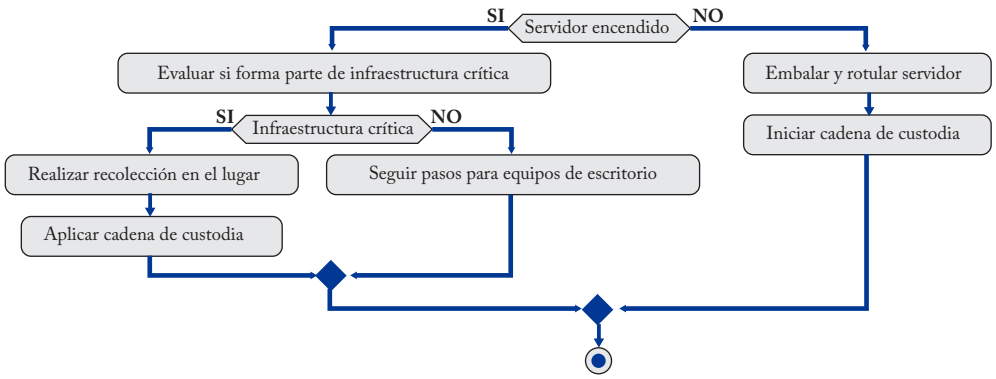
Si se trata de equipos de computación también debe considerar para su tratamiento si está encendido o no. En caso de no estar encendido deberá fijar, levantar y trasladarlo con la documentación pertinente, por el contrario, si está encendido deberán tomar en cuenta las siguientes consideraciones: no apagar el equipo, aislar el dispositivo de conexiones y servicios, respaldar la información que está en el monitor e intentar mantenerlo encendido. Si el equipo se encuentra bloqueado, se debe fijar el usuario. Realizados estos procedimientos el DEFR solicitará la presencia de un DES para el manejo técnico de los equipos.

El personal DES tomará las medidas de seguridad necesarias para que la información que consta en los equipos informáticos o digitales esté segura y no sea objeto de ninguna manipulación.

20 Funda Faraday: es un elemento en forma de caja y que crean un campo electromagnético nulo, protegiendo por tanto su interior de cualquier campo eléctrico estático.

Gráfico 6

Diagrama de flujo de la actuación del DEFR en servidores



Fuente: la actuación del DEFR en servidores.

Elaboración: por los autores.

Obtendrá la memoria RAM del dispositivo o a su vez, una imagen forense de la información del equipo para lo cual, deberá contar con la autorización judicial correspondiente, aplicar las normas de manejo de la información y respetar la cadena de custodia. Así, garantiza que la información obtenida tenga eficacia probatoria dentro de un proceso judicial.

En el caso que en una escena de un delito se encuentren servidores informáticos, el DES verificará si el equipo está encendido o apagado. En caso que esté apagado, lo fijará, embalará y rotulará para su respectivo traslado hasta el centro de acopio de indicio. Si, por el contrario, el servidor informático se encuentra encendido, el DES evaluará si este forma parte de una estructura crítica antes de realizar cualquier procedimiento. Si determina que forma parte de una estructura crítica, realizará la extracción de la información en el sitio e iniciará la cadena de custodia respectiva para salvaguardar la información. Si el servidor no forma parte de una estructura crítica, se fijará, embalará, rotulará y trasladará al centro de acopio de indicios.

Propuesta metodológica para los DES

A continuación, consta una propuesta metodológica de los pasos que debe seguir el DES tomando por ejemplo un dispositivo móvil. Para cada tratamiento, sea de equipos computacionales, dispositivos de almacenamiento, dispositivos de red, sistemas basados en la nube y tecnología exponencial, el procedimiento es amplio. Esta propuesta procura que no se pierda las características técnicas[21] y legales[22] de la evidencia digital desde el DES.

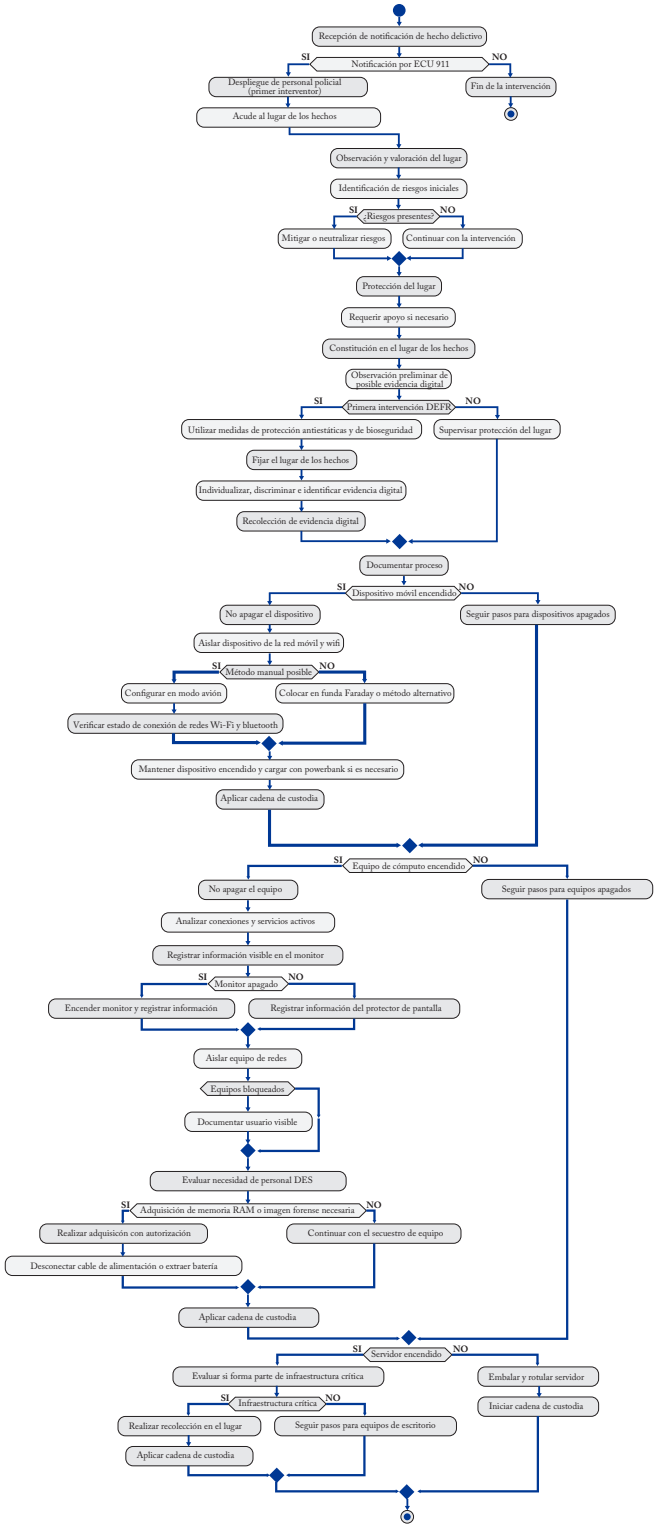
El DES debe contar con un laboratorio que tenga el equipamiento necesario para desempeñar su trabajo, esto es, herramientas de software y hardware, tecnología y herramientas físicas indispensables para el tratamiento de la evidencia digital. Así mismo, debe ejecutar tres actividades esenciales: la recolección, el tratamiento y análisis de la evidencia digital. Para esto se diseñó una propuesta de procedimiento que a continuación se detalla:

21 Características técnicas de la evidencia digital: volátil, anónima, duplicable, alterable y eliminable.

22 Características legales de la evidencia digital: admisible, creíble, confiable, auténtica y completa.

Gráfico 7

Diagrama de flujo total de la actuación del DEFR

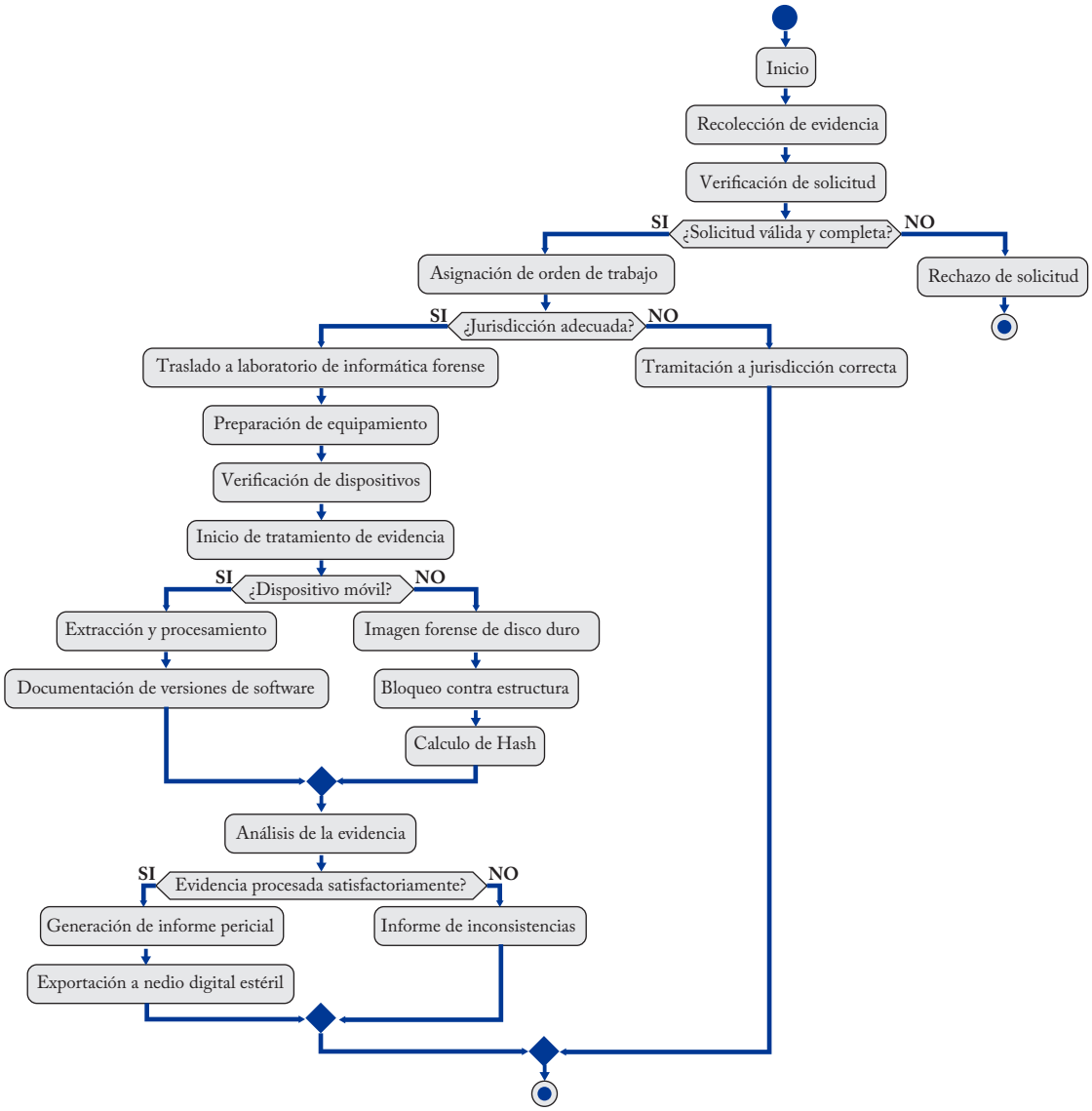


Fuente: la actuación del DEFR.

Elaboración: por los autores.

Gráfico 8

Diagrama de flujo del procedimiento inicial del DES y pasos a seguir en un dispositivo móvil



Fuente: procedimiento inicial del DES.

Elaboración: por los autores.

- Una vez que la evidencia se encuentra en el centro de acopio,[23] el DES debe verificar la documentación en la cual consta el pedido de la pericia solicitado por la autoridad competente. Esta documentación debe contener una descripción clara del objeto de la pericia.

23 Centro de acopio. - Es el lugar que cumple la función de reunir indicios, muestras, materiales y otros, para mantener la integridad y naturaleza de éstos.

- Si la solicitud no contiene las formalidades necesarias, se procede a rechazar la misma, indicando los motivos del rechazo y se remitirá mediante oficio a la autoridad solicitante.
- Si la solicitud de pericia está completa y es válida, la misma se asigna a un perito acreditado de la jurisdicción. El DES una vez que ha tomado posesión de la evidencia digital, traslada la misma hasta el laboratorio de informática forense donde preparará el equipo. Realiza la verificación completa del dispositivo tomando en cuenta todas sus características de manera que sea individualizado y comienza con el tratamiento de la evidencia digital.
- Si se trata de un dispositivo que contiene evidencia digital, el DES se centra en identificar, adquirir, procesar, analizar y presentar la información ante un estrado judicial. Para esto, debe especificar el tipo de software y hardware, la versión utilizada para la extracción de la información e indicar si se trata de una extracción bit a bit o de una extracción lógica.
- La evidencia digital debe ser tratada de manera rigurosa conforme a los estándares legales y tecnológicos vigentes. Una vez tratada, se realiza un informe detallado de las actividades desarrolladas y se pasa la información obtenida a un medio estéril. Se indica si existió alguna inconsistencia durante la pericia. Por último, la evidencia deberá ser entregada mediante una cadena de custodia (nuevamente) al centro de acopio. Así termina este procedimiento.

Conclusiones

Se obtuvo un panorama de los aspectos que permiten el levantamiento y tratamiento de la evidencia digital, al igual del trabajo que debería desempeñar el DEFR y el DES en el marco de los desafíos y delitos relacionados con los avances tecnológicos. Teniendo presente esa necesidad, este artículo elaboró un instrumento o modelo con metodología técnica que, basada en normas internacionales como las ISO y los RFC, ofrece directrices de cómo se debe realizar la observación, recolección, individualización, registro, sellado, traslado y tratamiento de la evidencia digital con el fin de asegurar el esclarecimiento de un hecho.

Es necesario que los DEFR desde el eje preventivo, investigativo e inteligencia de la PNE, se guíen de este instrumento y resguarden las características principales y legales de la evidencia con base en las normas ISO y RFC aquí analizadas. La evidencia tendrá por principios fundamentales la admisibilidad, autenticidad, completitud, confiabilidad y credibilidad.

Los pasos o procedimientos que se proponen en el presente artículo buscan instaurar el buen manejo de la evidencia digital como parte de las buenas prácticas profesionales. La propuesta permite a los DES brindar el tratamiento correcto de la evidencia digital para que esta sea admisible, creíble, confiable, auténtica y completa ante los tribunales de justicia. Con esto, no existirían vacíos legales que puedan incurrir en la nulidad de una sentencia o que las pericias sean anuladas.

Recomendaciones

- Presentar los resultados de este artículo a los peritos de informática forense y personal jurídico de Ecuador con el fin de que pongan en práctica el manejo y el tratamiento de la evidencia digital conforme a la metodología que aquí se presenta. Esto permitiría asegurar que los procedimientos empleados cumplan con los estándares internacionales y normas nacionales y, se mantenga con la integridad de la información. Además, la implementación de estas prácticas ayudará a mejorar la precisión y fiabilidad en la recolección y análisis de datos digitales. Finalmente, la colaboración entre el DEFR y el DES contribuirá a la actualización constante para que la evidencia digital no pierda relevancia, confiabilidad y suficiencia.
- Realizar capacitaciones al personal policial que cumpliría la función del DEFR y DES desde el eje preventivo, investigativo e inteligencia. Estas capacitaciones deben enfocarse en procedimientos actualizados para la identificación, recolección, adquisición y preservación de la evidencia digital, garantizando así el cumplimiento de los estándares internacionales. Además, es crucial que el entrenamiento incluya escenarios prácticos y estudios de caso para mejorar la comprensión y aplicación de las técnicas.
- Analizar la posibilidad de crear diversos protocolos conforme a la evidencia digital tratada o analizada, de esta manera, se implementarían capacitaciones hacia los DES. Estas capacitaciones asegurarán que los peritos informáticos forenses se mantengan al día con los últimos avances tecnológicos y métodos de análisis. Además, el intercambio de conocimientos entre los especialistas permitirá desarrollar y mejorar el campo profesional con estrategias más efectivas, con protocolos y metodología novedosas. Finalmente, la formación continua del DES contribuirá a que no exista duda razonable de la evidencia digital ante la autoridad competente.

Bibliografía

America, Usaid del Pueblo de los Estados Unidos de America. 2013. *Sistema de Comando de Incidentes.* Acceso el 27 de mayo de 2024. https://www.gob.mx/cms/uploads/attachment/file/228836/Curso_Basico_SCI_material_de_referencia.pdf.

Asamblea Nacional. 2008. *Constitución de la República del Ecuador.* Montecristi: Registro Oficial, 91-92.

Brandner, Carlos Wallace & Ralf Ulrich Pordesch. 2007. *Requisitos del servicio de archivo a largo plazo.* Manuales de archivo y conservacion de la información digital. Darmstadt, Alemania: Sociedad de Internet.

Castellanos, Bayron José. 2017. *Dialnet.* Acceso el 27 de mayo de 2024. https://dialnet.unirioja.es/servlet/articulo?codigo=6704741.

Coreth, Emerich. 1972. *Cuestiones fundamentales de hermenéutica*, 1ª ed. Traducido por Manuel Balasch. Barcelona: Herder Editorial.

DS/EN ISO/IEC 27042. 2016. *Tecnologías de la información - Técnicas de seguridad - Lineamientos para el análisis e interpretación de la evidencia digital.* Ginebra: Secretaría Central de ISO.

Gómez- Agudelo, Dany Steven. 2020. *Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano.* Artículo científico, Ratio Juris.

Incibe, Asier. 2014. *Plan de recuperación, transformación y resiliencia.* Directrices para la recopilación de evidencias y su almacenamiento, España: S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A.

ISO/EC 27037. 2012. *Tecnología de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales.* Ginebra: Secretaría Central de ISO.

Locard, Edmond. 2010. *Manual de técnica policíaca.* Barcelona: Maxtor.

Maldonado, Ricardo Oñate. 2016. El método hermenéutico en la investigación cualitativa. *ResearchGate* (University of Concepción), 1-10.

Martínez, Jesús, Francisco Cano y Franco Rodríguez. 2020. *Adaptación española del Inventario de Estrategias de Afrontamiento.* Sevilla.

NFON. 2024. Request por comments. Acceso el 4 de mayo de 2024. https://n9.cl/rbz9kd

Organizacion de los Estados Americanos. 2019. *Consideraciones de Ciberseguridad del proceso democratico para la América Latina y el Caribe.* Santiago de Chile: 1 - 68.

Piña-Ferrer, LenysSenovia. 2023. El enfoque cualitativo: una alternativa compleja dentro del mundo de la investigación. *Revista Arbitrada Interdisciplinaria KOINONIA*, 1-3.

Policía Nacional, Sistema Especializado Integral de Investigación Medicina Legal y Ciencias Forenses de la Policía Nacional del Ecuador. 2022. *Manual de Procedimientos Investigativos Fiscalía - Policía Judicial.* Policía Nacional del Ecuador, Quito: Sistema Especializado Integral de Investigación Medicina Legal y Ciencias Forenses de la Policía Nacional del Ecuador, 1-184.

Pordesch, Tobias Gondrom & Ralf Brandner-Ulrich. 2007. *Sintxis del registro de pruebas (ERS).* Manual de Sintaxis del registro de pruebas (ERS), Alemania: Sociedad de Internet.