FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

"Diseño de una metodología de recolección de evidencia digital para análisis forense de unidades de disco duro, basada en la norma ISO/IEC 27037:2012"

Realizado por:

David Santiago Rosero Paredes

Director del proyecto:

Ing. Mónica Romero Pazmiño, Msc.

Como requisito para la obtención del título de:

MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

Quito, julio 2019

DECLARACIÓN JURAMENTADA

Yo, DAVID SANTIAGO ROSERO PAREDES, con cédula de ciudadanía1714952056, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

David Santiago Rosero Paredes

C.C.: 1714952056

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientandosus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

Ing. Mónica Romero Pazmiño

Magister en Evaluación y Auditoría de Sistemas.

CC: 0201615572

LOS PROFESORES INFORMANTES

Los Profesores informantes:

DIEGO RIOFRÍO LUZCANDO

LUIS FABIAN HURTADO VARGAS

Después de revisar el trabajo presentado lo han calificado

como apto para su defensa oral ante el tribunal examinador.

_____ _____

Ing. Diego Riofrío Luzcando, Dr Ing. Luis Fabián Hurtado Vargas, MsC

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____

DAVID SANTIAGO ROSERO PAREDES

C.C.: 1714952056

DEDICATORIA

Dedico el siguiente trabajo de investigación a Dios, sin él, no hubiese sido posible el desarrollo de la presente tesis, porque él da la sabiduría, el conocimiento y la inteligencia. A mis padres, por ser un apoyo incondicional, por infundirme valores éticos, morales, humanos y principios que fomentan el trabajo, el esfuerzo, la honestidad, la justicia y la responsabilidad. A mis hermanos, sobrinos y demás familia, porque siempre me apoyan, son una inspiración para superarme, obtener nuevos logros, por la pasión con la que hacen sus cosas y cumplen con sus objetivos. A mis amigos y compañeros del Servicio Nacional de Contratación Pública, con los cuales aprendo cada día algo nuevo profesionalmente y humanamente.

AGRADECIMIENTO

Un agradecimiento infinito a Dios, por ser mi guía en la presente investigación, por darme sabiduría y mantenerme motivado para cumplir este objetivo en mi formación profesional. A la docente Ing. Mónica Romero Pazmiño por su valiosa ayuda, paciencia, motivación, orientación y dirección durante todo el desarrollo de la investigación, además por su apreciable tiempo, experiencia y conocimientos impartidos en cada tutoría. A la Universidad Internacional SEK, institución altamente calificada para la formación de profesionales de excelencia.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tiene como propósito diseñar y difundir una metodología para manejo de evidencia digital contenida en unidades de almacenamiento, con énfasis en discos duros, basado en la Norma ISO/IEC 27037:2012, debido a que actualmente en Ecuador no se ha evidenciado un procedimiento normado o estandarizado para realizar actividades de manejo de evidencia digital por parte de los peritos informáticos calificados en el Consejo de la Judicatura, es por eso que se plantea una metodología orientada a la actuación pericial, dirigida a dispositivos actuales, con la cual se pretende mejorar la calidad de evidencia digital. Este trabajo inicia con el análisis de las metodologías de extracción de evidencia digital de discos duros en Argentina, España y Colombia. La metodología que se propone se basa en la Norma ISO/IEC 27037:2012 y en investigaciones provenientes de los países mencionados consta de seis fases que incluyen la ubicación, aseguramiento de la escena de los hechos, la identificación, recolección, preservación y análisis de la evidencia digital. Finalmente, se realiza una difusión a nivel nacional de la metodología a los peritos informáticos calificados en el Consejo de la Judicatura se tomó dos muestras de peritos informáticos, la primera para conocer los medios y herramientas que se utiliza actualmente en el manejo de evidencia digital, y la segunda muestra para la difusión de la metodología propuesta. Los resultados mediante un juicio de experto indican que la aplicación de la misma tiene ventajas competitivas respecto a otras metodologías; en otros resultados se muestra que la utilización de la metodología ayuda en la mejora de la calidad de evidencia digital para ser admitida en un proceso judicial por el hecho que cumple con los principios de relevancia, la confiabilidad y la suficiencia.

Palabras claves: Evidencia digital, Informática forense, discos duros, delitos informáticos, perito informático, cadena de custodia, Norma Internacional ISO 27037.

ABSTRACT

The purpose of this research is to design and disseminate a methodology for the management of digital evidence contained in storage units, with an emphasis on hard drives based on the ISO / IEC 27037: 2012 Standard because in Ecuador there is currently no evidence of a normed or standardized procedure for carrying out activities of digital evidence management by qualified computer experts in the Judicial Council, that is why the propose of a methodology oriented to expert performance, aimed at current devices, which aims to improve the quality of digital evidence. This work begins with the analysis of the methodologies for extracting digital evidence from hard drives in Argentina, Spain and Colombia. The methodology proposed based on ISO / IEC 27037: 2012 Standard and researching from the aforementioned countries consists of six phases that include the location, assurance of the scene of the events, the identification, collection, preservation and analysis of digital evidence. Finally, a national diffusion of the methodology is made to qualified computer experts in the Judicial Council, two samples of computer experts were taken the first to know the media and tools that are currently used in the management of digital evidence, and the second sample for the diffusion of the proposed methodology. The results through an expert judgment indicate that its application has competitive advantages over other methodologies; other results show that the use of the methodology helps in improving the quality of digital evidence to be admitted in a judicial process due to the fact that it complies with the principles of relevance, reliability and sufficiency.

Keywords: Digital evidence, Computer forensics, hard drives, computer crimes, computer expert, chain of custody, International Standard ISO 27037.

CAPÍTULO I

INTRODUCCIÓN

1.1PREFACIO

Actualmente en Ecuador no se ha evidenciado un manual, un procedimiento, un reglamento o norma sobre la recolección de evidencia digital confiable, es decir no se aplica ninguna norma o estándar fijo para extraer evidencia digital de dispositivos de almacenamiento como son las unidades de discos duros de ordenadores. Esto deriva que la calidad de la evidencia recolectada en muchos casos no sea la ideal.

Según una primera encuesta realizada para la presente investigación a una muestra de 27 peritos informáticos calificados en el Consejo de la Judicatura de Ecuador, se determinó que únicamente el 33% utiliza como preferencia aspectos de la norma ISO/IEC 27037:2012 para la fase de extracción de evidencia digital, es decir un 67% no utiliza ningún aspecto de la norma en mención. Se muestra en la siguiente tabla un extracto del análisis de la encuesta respecto al grado de utilización de las metodologías para extracción de evidencia digital en el país.

Tabla 1. Uso de metodologías de extracción de evidencia digital

Metodología / Grado Utilización	1	2	3	4	5
RFC 3227	12	1	4	2	8
ISO/IEC 27037:2012	6	2	6	4	9
UNE 71505	10	3	2	8	4
UNE 71506	10	4	1	10	2
ISO/IEC 27041:2015	8	1	8	8	2
ISO/IEC 27042:2015	8	3	8	4	4
ISO/IEC 27043:2015	10	1	8	6	2
UNE 197010:2015	10	3	6	6	2
ISO/IEC WD 27044	8	1	8	8	2
Otro Especifique: -------	16	1	4	2	4

Fuente: Encuesta a peritos informáticos, Elaboración: Autor

Como se puede ver en la tabla anterior, se valoró del 1 al 5 el grado de utilización de aspectos de las metodologías consideradas, por consiguiente, de los 27 peritos que

respondieron la encuesta, únicamente 9 valoraron en escala 5 la utilización de la Norma ISO/IEC 27037:2012.

Con una extracción de evidencia digital confiable y bien procesada, ésta puede ser aprovechada de la mejor manera posible para obtener calidad probatoria, precisión en el análisis, restauración del servicio y/o el costo de la recolección de la evidencia.

1.2PLANTEAMIENTO DEL PROBLEMA

Tanto en los delitos informáticos, como en las investigaciones de estos ilícitos se utiliza la tecnología. Por un lado, se emplean equipos informáticos para cometer delitos como son estafas, accesos ilegales a sistemas, falsificaciones documentales, amenazas y coacciones; delitos contra la intimidad y acoso, sabotaje informático, suplantación de identidad, delitos contra la propiedad intelectual, entre otros.

Por otro lado, en las investigaciones de los delitos mencionados, se utiliza también herramientas informáticas con el objeto de descubrir dichos ilícitos, mediante software especializado para el manejo de evidencia digital, de modo que sea posible presentar pruebas confiables ante la justicia. Las motivaciones de los delitos pueden ser múltiples, desde un robo de información hasta crímenes que implican homicidios.

Por consiguiente, es indispensable diseñar una metodología de informática forense basada en una norma especializada en identificación, recopilación, adquisición y preservación de la evidencia digital como es la ISO/IEC 27037:2012, la misma que presenta pautas para actividades específicas con el fin de que sea admisible en procesos judiciales.

Cabe destacar, la siguiente afirmación: “Los elementos claves que aportan credibilidad en la investigación son la metodología aplicada durante el proceso y la calificación de los individuos que actúan en el desarrollo de las tareas especificadas en la metodología” (Roatta, Casco, & Fogliato, 2017, p. 1).

1.2.1. Diagnóstico del problema

La calidad de la evidencia digital, es un aspecto fundamental en cualquier disputa legal o extrajudicial esencialmente dentro de un delito donde esté involucrado directa o indirectamente un equipo informático, porque aporta valor probatorio a la investigación.

Se entiende por evidencia digital, los datos generados por un equipo informático, si se considera un disco duro, la información queda registrada incluso luego de que haya sido formateado, es decir los datos almacenados en el disco pueden ser recuperados y procesados de forma correcta para que sean presentados como evidencia dentro de un proceso legal.

En los siguientes ejemplos conocidos a nivel mundial, se puede ver la importancia de la evidencia digital para descubrir delitos que se cometieron en diversas circunstancias:

En el año 2005, las pruebas digitales localizadas en un disco duro fueron de ayuda a los investigadores para encarcelar al asesino en serie BTK[1], un criminal que había esquivado a la policía desde 1974 y al cual se le atribuyen al menos 10 víctimas. (EFE, 2005, p.1).

Pruebas digitales encontradas en un celular llevó a la policía internacional[2] a dar con el paradero de los terroristas responsables de los atentados de Madrid, que resultó con la muerte de al menos 190 personas en el 2004. (Almeida, 2011, p.32)

En otro caso, en Norteamérica se recolectó pruebas digitales de las redes informáticas en las universidades y las instalaciones militares en la década de 1980 estas guiaron al descubrimiento del espionaje internacional, con el apoyo de un gobierno extranjero hostil a los Estados Unidos[3].

En la actualidad, los funcionarios de la ley que realizan actuación pericial tratan de extraer potencial evidencia digital de un mayor número de dispositivos, con mayor

[1] Dennis Lynn Rader es un asesino en serie estadounidense, su alias era Asesino BTK, letras correspondientes a Bind, Torture and Kill ('Atar, torturar y matar' en español).
[2] Documentos secretos de Estado- de Interpol, Europol, Guardia Civil-Servicios de Información- y de la Inteligencia española
[3] KGB sobornó a un ex agente de la CIA para que se infiltrara en el Congreso Norteamericano

capacidad de almacenamiento, los dispositivos informáticos que se pueden investigar en relación a un delito incluyen ordenadores, laptops, memorias flash, unidades de disco duro, dispositivos de almacenamiento externo, cámaras digitales, las consolas de videojuegos, los teléfonos celulares, Tablet, iPad, entre otros.

El contenido de datos en los dispositivos en mención puede ayudar como prueba en investigaciones criminales, en delitos como abuso sexual a menores de edad, al analizar una computadora de un sospechoso, se podría encontrar imágenes, indicios o pesquisas para encontrar al autor o autores del delito.

Todo lo indicado, es posible siempre y cuando la evidencia digital sea confiable, por consiguiente, existe la necesidad de seguir un estándar para la recolección de evidencia digital como la norma la ISO/IEC 27037:2012.

1.2.2. Pronóstico del Problema

En caso de no seguir con los procedimientos confiables en la recolección de evidencia digital en el país, en muchas ocasiones no se va a obtener la evidencia probatoria válida para presentar ante un juez, y por ende los delitos informáticos no van a poder ser resueltos, o en otros casos no van a ser válidas las operaciones con las que se ha recolectado la evidencia digital.

1.2.3. Control de Problema

Para poder conseguir procedimientos confiables en la recolección de evidencia digital, se ha considerado una metodología que siga estándares a nivel internacional, la misma está basada en la norma ISO/IEC 27037:2012 que es una guía para identificación, recolección, adquisición y preservación de potencial evidencia digital que tiene como objeto de brindar técnicas para dichas acciones, la cual serviría para mejorar la calidad probatoria, la confiabilidad en la recolección y manejo de la evidencia digital específicamente en dispositivos de unidades de discos duros de ordenadores.

1.2.4. Formulación del Problema

La recolección de evidencia digital en discos duros y en general en dispositivos de almacenamiento para la actuación pericial, es una actividad delicada y muchas veces se torna compleja, porque la evidencia para ser válida depende de los procedimientos realizados para dicha recopilación y preservación, para después ser analizados y posteriormente presentados en un proceso judicial.

1.3 OBJETIVOS

1.3.1 Objetivo general

Diseñar una metodología que incluya procedimientos para la recolección de evidencia digital contenida en unidades de discos duros, con base en la norma estándar ISO/IEC 27037:2012.

1.3.2 Objetivos específicos

- Identificar la situación actual de la utilización de métodos de extracción de evidencia digital de discos duros en Ecuador a través de una encuesta a peritos informáticos.
- Analizar la metodología de extracción de evidencia digital de discos duros en Ecuador y en algunos países como Argentina, España y Colombia.
- Diseñar una metodología basada en la norma estándar ISO/IEC 27037:2012 y en las mejores prácticas de identificación, extracción y preservación de evidencia digital de unidades de disco duro utilizadas en países como España, Argentina y Colombia que sea válida en procesos judiciales.
- Difundir la metodología propuesta basada en la norma internacional ISO/IEC 27037:2012 a los peritos informáticos calificados en el Consejo de la Judicatura.

1.4 JUSTIFICACIÓN

La presente investigación pretende dar a conocer una nueva metodología de recolección de evidencia digital de discos duros basada en el estándar ISO/IEC 27037:2012 y en las mejores prácticas de metodologías de informática forense destacadas a nivel iberoamericano; dicha metodología aspira ser competitiva respecto a las utilizadas en la región.

La metodología propuesta tiene como base la norma estándar ISO/IEC 27037:2012 la misma que maneja los principios que preservan la originalidad de la prueba, procesos auditables, procesos reproducibles, procesos defendibles de acuerdo a la tipología del dispositivo, procesos de identificación de la evidencia, recolección y/o adquisición de dispositivos o la información existente en los mismos, la preservación de la evidencia de manera íntegra. (López, 2012)

Cabe destacar que a más de diseñar una metodología de confianza como la que se plantea, se eligen métodos basados en buenas prácticas para que se garantice posteriormente que el análisis, la interpretación y la exposición de los informes con pruebas digitales sean íntegros, objetivos y transparentes. (Salmerón, 2017)

Esta norma utilizada en el diseño de la metodología, es aplicable a organizaciones que necesitan proteger, analizar y presentar evidencia digital potencial que puede provenir de diferentes tipos de dispositivos digitales, redes, bases de datos, etc.; los componentes clave que proporcionan credibilidad en la investigación son la metodología aplicada durante el proceso y los individuos calificados para realizar las tareas especificadas en la misma.

1.5 MARCO TEÓRICO

1.5.1 Principio de Intercambio de Locard

El principio manifiesta que "Siempre que dos elementos entran en contacto trasfieren parte del material que incorporan al otro objeto" (Rodríguez, 2018, p.55).

Figura 1. Principio de Intercambio de Locard
Fuente: (Rodríguez, 2018,p.55)

Este principio implica que "Todo contacto deja un rastro", es decir cuando ocurre un delito informático siempre se encontrará algún rastro o huella de quien fue el autor del delito, existen varios aplicativos de software y hardware utilizados para determinar el autor o la causa (Granda, 2015, p.18).

El objetivo es establecer el vínculo entre los tres elementos (escena de los hechos, victima, victimario) ya que el victimario se llevará material del lugar de los hechos y de la víctima; la víctima tendrá material del victimario y la escena de los hechos tendrá material de ambos (Iorio, 2015, p.56).

1.5.2 Evidencia Digital

Es un tipo de evidencia física, está compuesta de campos magnéticos y pulsos electrónicos que pueden ser recolectados y examinados con instrumentos y métodos especiales (Acurio, 2006, p.14).

De acuerdo con el HB: 171 2003 Guidelines for the Managment of IT Evidence, la evidencia digital es cualquier información que, por medio de intervención humana u otra semejante, ha sido extraída de un medio informático (Osorio, 2012). El documento establece también que la evidencia digital puede dividirse en tres categorías:

- Registros almacenados en el equipo de tecnología informática
- Registros generados por los equipos de tecnología informática
- Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática.

La evidencia digital tiene los siguientes elementos que la hacen un constante desafío para quienes la identifican e investigan:

- Volátil
- Anónima
- Es posible duplicarla
- Es alterable y modificable
- Susceptible de ser eliminada.

Algunos ejemplos que se consideran de la evidencia digital pueden ser: el último acceso a un archivo o aplicación, un log de un archivo, una cookie en un disco duro, la hora de encendido de un sistema, un proceso en ejecución, archivos temporales, por mencionar algunos (Ghosh, 2004).

Las fuentes de evidencia digital contienen elementos susceptibles de investigación, las mismas que resguardan información que generalmente se asocia al propietario del medio.

Tabla 2. Fuentes de evidencia digital

Medio Digital	Recurso	Evidencia
Computadoras de Escritorio y Personales	Discos Rígidos Internos	-Archivos de Log -Cookies -Archivos ocultos -Navegación -Spool de impresión -Archivos temporales -Archivos de SWAP -Archivos comprimidos -Archivos ocultos -Archivos renombrados -Archivos protegidos con passwords
Dispositivo con control de acceso	Pen drive Tarjeta de proximidad Biometría	- Datos de identificación del usuario - Niveles de acceso - Permisos - Configuraciones
Cámaras digitales	Tarjeta de memoria	-Imágenes -Videos -Sonidos -Fecha y hora de grabación
Tarjetas de memoria	N/A	-Imágenes -Documentos o planillas -Fotos
Impresoras - Scanner	Tarjetas de memoria en scanner	-Documentos
Puntos de acceso de routers Wireless	N/A	- Archivos de configuración
Diskettes CD DVD	N/A	N/A
GPS - Celulares	Memoria interna del dispositivo celular Tarjeta de memoria	-SMS -WhatsApp -Telegram -Fotos -Emails -Videos -Notas de voz

Fuente: Investigación forense sobre medios digitales (Parada, 2018)

1.5.3 Informática Forense

Existen algunas definiciones de Informática Forense, las mismas que están relacionadas al manejo apropiado de la evidencia digital:

Es el proceso metodológico para la recolección, preservación y análisis de los datos digitales de un sistema de dispositivos de manera que pueda ser presentado y admitido en causas judiciales. (Rodríguez, 2011).

"La informática forense es una disciplina científica técnica legal que involucra métodos para identificar, preservar, analizar y presentar potencial evidencia digital, de manera que ésta sea legalmente aceptable en una causa judicial." (Igarza, Gioia, & Eterovic, 2018)

Las fases de la informática forense de manera general, se visualizan en la imagen siguiente conforme a un compendio de sus actividades principales.

Tabla 3. Fases de la informática forense

Identificación	-Levantamiento de información - Asegurar la escena
Validación y Preservación	-Copias de la evidencia -Cadena de custodia
Análisis	-Preparación para el análisis -Reconstrucción del ataque -Determinación del ataque -Identificación del atacante -Perfil del atacante -Evaluación del impacto
Documentación y Presentación De pruebas	-Registro del incidente -Informe técnico -Informe ejecutivo

Fuente: Fases de la Informática forense (Rivas, 2014a)

1.5.4 Perito Informático

Es un profesional experto y titulado, dotado de conocimientos legales, teóricos y prácticos especializados en informática y tecnologías de la información, capaz de asesorar o elevar un dictamen comprensible y a la vez técnico sobre un litigio o cualquier otra situación que se le requiera. (Navarro, 2016, p.25)

Los peritos informáticos actúan tanto en los ámbitos judicial y extrajudicial, sus áreas de conocimiento son amplias, y por ende deben estar constantemente actualizados tanto en aspectos metodológicos, tecnológicos y legales. El perito informático debe considerar sus limitaciones profesionales, puesto que es muy poco probable ser experto en todos los ámbitos y/o especialidades; no es suficiente tener los conocimientos técnicos, legales y prácticos, sino que debe garantizar que el resultado de su trabajo sea objetivo,

metódico, demostrable, reproducible, veraz, auditable, creíble, honesto y profesional (Navarro, 2016).

Es importante indicar que el perito informático forense, debe proceder de acuerdo a la normativa vigente de cada país, de tal forma que aplique métodos que certifiquen la legitimidad e integridad de la información procesada para que sea aceptada como válida en un tribunal (Puig, 2014).

Cabe señalar que, la representación del perito informático forense es requerida como auxiliar de la justicia para el dictamen de evidencias tecnológicas que faciliten al juez el esclarecimiento de un litigio. Además, los conocimientos de un perito informático forense son demandados por empresas, organizaciones y gobiernos para fortalecer la seguridad informática, se debe indicar también que son competencias del perito informático forense la auditoría de redes, el manejo de herramientas de hacking ético, gestión de incidentes, análisis y evaluación de vulnerabilidades, análisis de malware, análisis forense, entre otros (Navarro, 2016).

1.5.5 Crímenes y evidencia digital

Es importante indicar que la investigación de los diversos delitos y crímenes informáticos pueden obtenerse a través de varios tipos de evidencia digital que sirven como pruebas que pueden ser presentados ante un tribunal con la debida cadena de custodia.

Tabla 4. Crímenes y evidencia digital

Investigaciones de fraude computacional	
Datos de las cuentas de subastas en línea	Información de clientes
Contabilidad de software y archivos	Datos de tarjeta de crédito
Libreta de direcciones	Bases de datos
Calendario	Software de cámara digital
Registros de chat	Correos, notas y cartas
	Registros financieros de bienes
Investigación de Pornografía y Abuso Infantil	
Registro de chats	Imágenes
Software de cámara digital	Registro de actividad en internet.
Correos, notas y cartas	Archivos de video
Juegos	Usuario que creó el directorio y nombres de
Software de edición de gráficos	archivos de imágenes
Investigación de Intrusiones de Red	

Libreta de direcciones	Direcciones y nombres de usuario
Archivos de configuración	De protocolos de Internet
Correos, notas y cartas	Registros de chat
Programas ejecutables	Código fuente
Registro de actividad en Internet	Archivos de texto con nombres de usuario y contraseña

Investigación de Homicidios	
Libreta de direcciones	Registros médicos
Correos, notas y cartas	Números telefónicos
Registro de activos financieros	Diarios
Registros de actividad en Internet	Mapas
Documentos legales y testamentos	Fotos de la víctima o sospechoso
	Fotos de trofeos

Violencia Doméstica	
Libreta de direcciones	Registros financieros
Diarios	Registros telefónicos
Correos, notas y cartas	

Fraudes Financieros y Falsificación	
Libreta de direcciones	Registro de estados financieros
Calendario	Imágenes de firmas
Imágenes de moneda corriente	Registros de actividad en Internet
Imágenes de orden de pago y cheques	Software bancario en línea
Información de clientes	Imágenes de falsificación de monedas
Correos, notas y cartas	Registros del banco
Identificaciones falsas	Números de tarjetas de crédito

Amenazas de correo electrónico y acoso	
Libreta de direcciones	Registros de actividad en Internet
Diarios	Documentos legales
Correos, notas y cartas	Registros telefónicos
Registros de activos financieros	Víctimas
Imágenes	Mapas de ubicación

Investigación en Drogas	
Libreta de direcciones	Identificaciones falsas
Calendario	Registros de activos financieros
Bases de datos	Registros de actividad en Internet
Recipientes de droga	Imágenes de procedimientos de elaboración
Correos, notas y letras	

Piratería de Software	
Registros de chat	Números de serie de software
Correos, notas y cartas	Utilerías para crack de software
Archivos de imagen de licencias de software	Nombres de archivo y directorios creados por el usuario que clasifiquen el software propietario
Registros de actividad en internet	

Fraude en Telecomunicaciones	
Software de clonación	Correos, notas y letras
Bases de datos de clientes	Registros de activos financieros
Números de serie electrónicos	Registros de actividad en Internet
Números de identificación móvil	

Robo de Identidad	
Herramientas de hardware y software (Backdrops, lector/escritor de tarjetas de crédito, software de cámara digital, software de scanner)	Actividad en Internet relacionada con robo de identidad (correos y noticias, documentos borrados, pedidos en línea)

Plantillas de identificaciones (Actas de nacimiento, chequeras, licencias de conducir, firmas electrónicas, registro de vehículos)	Instrumentos de negocio (cheques, números de tarjetas de crédito, órdenes de pago, cheques personales)

Fuente: Estudio de Metodologías de Análisis Forense Digital (De León, 2009)

1.5.6 Delitos Informáticos en Ecuador

Se consideran según el COIP (Código Orgánico Integral Penal) (2014), como delitos informáticos los siguientes artículos entre los que enumeran y se detallan los más relevantes:

Tabla 5. Principales artículos sobre delitos informáticos de la ley ecuatoriana

Artículo COIP	Descripción General	Síntesis
Art. 103	Pornografía con utilización de niñas, niños o adolescentes	El individuo que promueva, divulgue o edite materiales visuales, informáticos, electrónicos de desnudos reales o simulados de niñas, niños o adolescentes en actitud sexual
Art. 104	Comercialización de pornografía con uso de niñas, niños o adolescentes	El individuo que anuncie, difunda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes
Art. 178	Violación a la intimidad	El individuo que, sin contar con la aprobación difunda datos personales, información contenida en soportes informáticos, por cualquier medio
Art. 190	Apropiación fraudulenta por medios electrónicos	El individuo que emplee encubiertamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la expropiación de un bien ajeno
Art. 191	Reprogramación o modificación de información de equipos terminales móviles	El individuo que cambie o modifique la información de identificación de los equipos terminales móviles
Art. 192	Intercambio, comercialización o compra de información de equipos terminales móviles	El individuo que comercie, mercantilice o adquiera bases de datos que contengan información de identificación de dispositivos móviles.
Art. 193	Reemplazo de identificación de terminales móviles	El individuo que sustituya las etiquetas de fabricación de los terminales móviles de identificación de dichos equipos con información de identificación falsa o distinta a la original
Art. 194	Comercialización ilícita de terminales móviles	El individuo que comercie equipos móviles con transgresión de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente
Art. 229	Revelación ilegal de base de datos	El individuo que, devele información registrada, contenida en ficheros, archivos, bases de datos; materializando voluntaria o deliberadamente la violación del secreto, la intimidad y la privacidad de las personas

Art. 230	Interceptación ilegal de datos	El individuo que, sin orden judicial previa, en provecho propio o de un tercero, obstruya, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
Art. 231	Transferencia electrónica de activo patrimonial	El individuo que, con ímpetu de lucro, trastorne, maneje o cambie el funcionamiento de un programa o sistema informático o telemático o mensaje de datos, para procurarse la transmisión o incautación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero
Art. 232	Ataque a la integridad de sistemas informáticos	El individuo que arruine, inutilice, suprima, estropee, trastorne, suspenda, trabe, ocasione mal funcionamiento, actuación no deseada o elimine datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen
Art. 233	Delitos contra la información pública reservada legalmente.	La persona que arruine o invalide información clasificada de conformidad con la Ley
Art. 234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	La persona que sin consentimiento intervenga en un sistema informático o sistema telemático o de telecomunicaciones, para utilizar ilegalmente el acceso obtenido, alterar un portal web, desviar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos.

Fuente: (COIP, 2014), Elaboración: Autor

1.5.7 Normativa de actuación pericial COIP y Ley de Comercio Electrónico

En el Código Orgánico Integral Penal (COIP), así como también en la Ley de Comercio Electrónico de Ecuador (2002), constan artículos en la normativa legal, que orientan a los peritos informáticos a seguir los principios y procedimientos para que la actuación pericial informática, además algunas consideraciones para tomar en cuenta con el fin de que la prueba sea admisible, se presenta a continuación, un extracto de los principales apartados relacionados a la investigación.

Tabla 6. Normativa legal relacionada a la actuación pericial en Ecuador

Artículo COIP	Síntesis
Art. 500	Hace referencia al contenido digital; se indican las reglas que se deben seguir: El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses; cuando se encuentre almacenado en sistemas y memorias volátiles, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido; de la misma forma cuando se encuentre almacenado en medios no volátiles; se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.
Art. 453	Trata de la prueba que tiene por finalidad llevar al juzgador al convencimiento de los hechos y la responsabilidad de la persona procesada.
Art. 292	Se refiere a la alteración de evidencias y elementos de prueba, cuando se destruya vestigios, evidencias materiales u otros elementos de prueba para la investigación de una infracción.
Art. 456	Hace relación a la cadena de custodia, en la que se indica que se aplicará a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad; la cual inicia en el lugar donde se recauda el elemento de prueba y finaliza por orden de la autoridad competente.
Art. 272	Hace referencia al fraude procesal, respecto a cuando la persona que con el fin de inducir a engaño al juez, oculte los instrumentos o pruebas, cambie el estado de las cosas, lugares o personas, antes o durante un procedimiento penal.

Fuente: COIP Elaboración autor(COIP, 2014)

Se informa también la normativa legal indicada en la Ley de Comercio Electrónico (2002), referente a la información original, práctica y valoración de la prueba para ser presentada por los peritos informáticos en el país.

Tabla 7. Normativa de la ley de comercio electrónico referente a la gestión de la prueba electrónica

Artículo Ley de Comercio Electrónico	Descripción
Art. 7	Hace referencia a la información original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos, cuando se encuentre almacenado en medios no volátiles; se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.
Art. 54	Se trata sobre la práctica de la prueba; indica que al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático en caso de ser requeridos; en caso de

	impugnación del certificado o la firma electrónica por cualesquiera de las partes, el juez ordenará a la entidad de certificación remitir los certificados; será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley.
Art. 55	Contempla la valoración de la prueba, la misma que será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, para la valoración de las pruebas, el juez competente deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

Fuente: (LEY DE COMERCIO ELECTRONICO, 2002) Elaboración autor

1.6 ESTADO DEL ARTE

ANTECEDENTES

Es importante en el presente estudio, indagar las metodologías que utilizan países como Argentina, España y Colombia; en estos países se ha evidenciado que utilizan procesos que siguen normas estándar para la recolección de evidencia digital en dispositivos de almacenamiento; a continuación, se detallan aspectos generales, ventajas, desventajas, parámetros como preservación de la evidencia, herramientas y casos de estudio de cada uno de los países en mención.

1.6.1 METODOLOGÍAS DE EXTRACCIÓN DE EVIDENCIA DIGITAL

1.6.1.1 Metodología de Extracción de Evidencia Digital en Argentina

Aspectos generales metodología en Argentina

La metodología utilizada en Argentina está basada en la Guía de obtención, conservación y tratamiento de evidencia digital de la Procuración General de la Nación Argentina publicada en marzo de 2016, tiene como fundamento los lineamientos para la identificación, recolección, obtención y preservación de la evidencia digital de forma tal que pueda ser presentada como evidencia válida en un proceso judicial; junto con otros documentos sobre guías de buenas prácticas para evidencia digital, computación forense, guía para recolectar y archivar evidencia RFC 3227, guía de obtención, preservación y tratamiento de evidencia digital (Armilla, Panizzi, Eterovic, & Torres, 2017a).

La metodología que utiliza Argentina tiene como objeto cumplir los tres principios de manejo de la evidencia digital establecidos en la norma estándar ISO 27037 que son la relevancia, la confiabilidad y la suficiencia (Semprini, 2016a).

Ventajas de la metodología en Argentina

- Cuenta con una guía para la obtención, preservación y tratamiento de evidencia digital para su presentación en procesos judiciales.
- Se aplican métodos confiables para que las evidencias no se alteren a lo largo del proceso.
- Los informáticos forenses basan sus investigaciones periciales en normas y guías de buenas prácticas como RFC e ISO, entre otras(Armilla et al., 2017a).

Desventajas de la metodología en Argentina

- La falta de capacitación del personal que interviene en la recolección de dispositivos tecnológicos abre la posibilidad de que se omita o no se considere el secuestro de todos los dispositivos en el lugar de los hechos para garantizar la suficiencia de la evidencia.
- Nunca existe una pericia informática igual a otra, varían en el escenario, las pruebas y la modalidad que han sido obtenidas; y las partes que intervienen en la investigación (Semprini, 2016a).

Preservación de la prueba en la metodología Argentina

La preservación se constituye de una serie de procedimientos y herramientas para la conservación de evidencia digital original, a lo largo de todo el ciclo de vida pericial, desde la identificación, adquisición o recolección, análisis hasta la presentación de resultados técnicos a tribunales de la justicia (Igarza et al., 2018).

Las recomendaciones indicadas en el documento mencionado, son utilizadas a nivel nacional e internacional para confiscar, examinar y preservar evidencia digital que

deben ser tomadas en consideración por los operadores judiciales (Armilla, Panizzi, Eterovic, & Torres, 2017b).

En la etapa de preservación de la prueba es muy importante mantener la cadena de custodia registrando todas las operaciones realizadas sobre la evidencia digital y resguardando de manera segura los elementos confiscados utilizando etiquetas de seguridad (Igarza et al., 2018).

Metodología empleada en Argentina

Referente a la metodología implementada en Argentina, se basa en principios fundamentales de la evidencia digital para garantizar su admisibilidad, asimismo es un proceso reproducible, tomando en consideración que se cuente con la prueba original.

La metodología está basada en la guía de tratamiento de evidencia digital antes mencionada, además con los protocolos, procedimientos y con el apoyo de las herramientas correctas, la metodología transita el ciclo de vida de la evidencia mostrada en la siguiente ilustración:

Figura 2. Ciclo de vida de la evidencia digital

Fuente: Metodología desarrollada por Rodney Mckemmish (Gómez, 2014).

El presente estudio se centra en la recolección de evidencia digital, por lo que se toma en cuenta un conjunto de buenas prácticas, que tienen como propósito no solo suministrar una guía para auxiliar a la ley, sino contribuir a la investigación de la seguridad informática e informática forense, tanto en escenas de crímenes como en incidentes (Armilla et al., 2017a).

El conjunto de buenas prácticas para la recolección de la evidencia digital en la Argentina, propuesto Por Nicolás Armilla, Marisa Panizzi, Jorge Eterovic y Luis Torres (2017), consta de siete etapas que son las siguientes:

- **Evaluación de escena**

El perito informático debe tomar toda precaución que garantice la seguridad de las pruebas de potencial evidencia digital.

- **Herramientas y equipamientos**

Según el problema a analizar, se utilizan las herramientas, para que se asegure la eficacia y eficiencia que se debe estimar en estos procesos donde la libertad de las personas puede estar en riesgo.

- **Dispositivos electrónicos**

Por lo general, los dispositivos electrónicos descritos para informática forense se aplican a computadoras y dispositivos en general.

- **Recolección**

Respecto a la recolección de potencial evidencia digital, ésta debe de manejarse cuidadosamente, de tal forma que preserve su valor probatorio.

- **Almacenamiento y transporte**

Las actividades que se realicen en esta etapa no deben modificar los datos almacenados en un ordenador u otros dispositivos, se debe precautelar al empaquetar, trasladar y recolectar evidencia digital.

- **Análisis**

Corresponde a una variedad de técnicas que se encargan de extraer información relevante, importante y valiosa de dispositivos de la manera menos intrusiva posible de tal forma que no altere el estado de los mismos.

- **Reporte**

Se refieren a información que describe los detalles específicos de un asunto particular escritos con una terminología determinada.

Cada fase indicada plantea métodos y herramientas, las primeras se refieren a las acciones que debe realizar el perito informático en cada fase y las herramientas apuntan a lo referente al software y elementos que se requieren para llevar a cabo las prácticas en cada fase(Armilla et al., 2017b).

Herramientas utilizadas para análisis forense en la metodología Argentina

En Argentina se utilizan herramientas para el manejo de evidencia digital de software de uso gratuito para sistema operativo Windows, también open source cuando se trata de Linux, y además software propietario, todo depende del tipo de análisis forense que se realiza y la plataforma a analizar.

Entre las cuales se encuentran bloqueadores de escritura como *write blocker*; bloqueadores por hardware como FastBloc, Tableau; de Imagen Forense licenciados como: EnCase, *FTK, IEF, DEFT*; entre otras herramientas open source que por lo general se utiliza en Linux como son: RegRipper, Forensic Registry Editor *(FRED), CAINE, KALI LINUX* entre las más conocidas. (Semprini, 2016, pp. 95).

Caso de estudio de la metodología Argentina

El caso que fue escogido consiste en la recepción de un email, que contiene una presunta intimidación que recibe un usuario final en un ordenador con sistema operativo Windows 10, la cual se encontró conectada a la energía eléctrica.

Para el análisis de la supuesta amenaza, se considera la aplicación de un conjunto de procedimientos para la recolección de evidencia digital en Argentina. El mismo que consta de siete fases.

Las etapas contemplan herramientas que se adaptan a investigaciones y casos relacionados de tipo tecnológico, social y cultural, como son: fraudes, violencia doméstica, acoso vía redes sociales y/o correo electrónico, homicidios, pornografía infantil, delincuencia organizada, entre otros delitos (Armilla et al., 2017).

Tabla 8. Aplicación de mejores prácticas de evidencia digital en Argentina

Etapas	Prácticas	Herramientas
Evaluación de la escena	-Preservación del ordenador -Aislar el ordenador de personas extrañas a la investigación	-Cámara fotográfica -Cinta del lugar de los hechos -Guantes
Herramientas y equipamientos	-Renovación de herramientas y equipamientos afines a la informática forense	-Cámara fotográfica, cinta del lugar del crimen, guantes, instrumentales no magnéticos, libreta de notas, cajas de cartón, registros, etiquetas, marcador y bolso antiestático -Conocimientos sobre Windows 10, hardware, periféricos, redes y seguridad informática. -Aplicaciones para hacer copias bit a bit, para analizar el estado del sistema y para generar imágenes forenses
Dispositivos electrónicos	-Evitar pérdida de información volátil -Interés primordial por Windows 10, mails, historial de internet y log	-Conocimiento sobre Windows 10 -Conocimiento sobre hardware -Conocimiento sobre periféricos
Recolección	-Rotular, documentar, marcar, fotografiar, filmar y titular la computadora -Especificar todos los cables del ordenador -Comprobar registro para ver si se suprimió algún dato	-Guantes -Instrumentos no magnéticos

Almacenamiento y transporte	-Procedimiento de embalaje de computadora -Procedimiento de transporte de computadora -Procedimiento de almacenaje de la computadora -Cadena de custodia	-Libreta de notas -Cajas de cartón -Guantes -Registros de inventario de pruebas -Etiquetas adhesivas de pruebas -Bolso antiestático -Marcador permanente
Análisis	-Copia bit a bit del sistema operativo Windows 10 -Estrategia forense (concentrarse en los mails maliciosos) -Situar datos en listado de la evidencia digital	-Conocimiento en Windows 10 -Programas para examinar procesos -Programas para examinar el estado del sistema -Programa para hacer copias bit a bit -Programas para generar imágenes esenciales y para poder examinarlas
Reporte	-Generación de reporte técnico -Conclusiones alcanzadas	-Conocimiento en Windows 10 -Conocimiento en seguridad informática -Conocimiento en redes

Fuente: XXIII Congreso Argentino de Ciencias de la Computación (Armilla et al., 2017)

1.6.1.2 Metodología de extracción de evidencia digital en España

Aspectos Generales de la Metodología en España

La metodología de análisis forense digital en España se fundamenta en normas y estándares, como la norma Internacional ISO 27037, la RFC 3227, las UNE 71505 y UNE 71506.

Las normas indicadas recomiendan el seguimiento de unos procedimientos determinados de actuación y la utilización de unas herramientas técnicas por parte del perito informático, con el objetivo de evitar la contaminación de las evidencias recolectadas con cualquier evento que pueda inducir su invalidez probatoria (García, 2015).

Las evidencias digitales se alojan en dispositivos como discos duros de ordenadores de puestos de trabajo, en servidores de correo electrónico, en teléfonos móviles, entre otros. Proporcionar la evidencia digital como medio de prueba en un proceso, es un derecho que contempla la Constitución Española en el artículo 24.2. Acorde a éste, “todos tienen derecho a utilizar los medios de prueba pertinentes para su defensa” (Velázquez, 2016).

Ventajas de la metodología en España

- Ofrece las directrices y orientación para tratar el manejo de la evidencia digital concernientes a la identificación, recolección, adquisición y preservación de la misma.

- Se utiliza aspectos de la norma ISO/IEC 27037:2012, como uno de los estándares en el ámbito pericial, en el cual se proporciona orientación para dispositivos de almacenamiento, entre los cuales están los discos duros que son el motivo de la presente investigación.

- La metodología en España es un compendio de aplicación de normas y estándares que aportan solidez y garantías en todo el proceso, no dando lugar a interpretaciones laxas, errores o inadvertencias graves (Rivas, 2014b).

Desventajas de la metodología en España

- Las aplicaciones y herramientas utilizadas en las mejores prácticas de recolección de evidencias digitales utilizadas en esta metodología, puede variar con el transcurso del tiempo, teniendo en cuenta que la evolución del software es constante.

Preservación de la prueba en la metodología de España

España cuenta como estándar en el tratamiento de evidencia digital la norma ISO/IEC 27037:2012 que presenta pautas para la identificación, recolección, adquisición y preservación de la evidencia digital. Dicha norma se aplica en cumplimiento de las leyes nacionales de cada jurisdicción. El contenido de la norma abarca técnicas, recomendaciones y funciones, que deben tomarse en cuenta cuando se trata la evidencia digital. Estos refuerzan su autenticidad e integridad, coadyuvando a que se admita como medio de prueba (Velázquez, 2016).

Para la preservación de la prueba se utilizan principios, recomendaciones y directrices necesarias de las normas UNE 71505, que contiene principios generales, buenas prácticas para gestión de evidencias electrónicas y formatos de intercambio de evidencias que permiten asegurar su contenido; asimismo de la norma UNE 71506 que complementa el estándar anterior, incluye técnicas para el análisis forense, incluyendo la preservación, adquisición, documentación, análisis y presentación de evidencias electrónicas (García, 2015).

Metodología empleada en España

La metodología en España, se fundamenta en cinco fases: Identificación del incidente, Recopilación de evidencias, Preservación de la evidencia, Análisis de la evidencia, Documentación y presentación de los resultados.

- La Identificación sintetiza la escena donde se ha producido el incidente que requiere un análisis forense.
- La recopilación explica cómo identificar y recolectar las evidencias.
- En la fase de preservación se explica cómo proteger las mencionadas evidencias asegurando la cadena de custodia.
- Se establecen recomendaciones y buenas prácticas sobre el análisis de las evidencias.
- Se cimienta en los informes que se debe presentar tanto técnico como ejecutivo (Navarro, 2016).

Herramientas utilizadas para análisis forense en la metodología de España

Para recuperación y tratamiento de discos: *PhotoRec, Scalpel, NTFS Recovery, Recovery RS, Recuva, RaidReconstructor, Resoration, FreeRecover, R-Studio, IEF, Bulk Extractor Viewer, CNWrecovery, GuyMager, GParted, UnBlock.*

Para análisis del sistema de Ficheros: *AnalizeMFT, INDXParse, MFT Tools, MFT Parser, Prefetch Parser, FileAssassin, WinHex.*

Para análisis del registro de Windows: *RegRipper, Windows Registry Recovery, Shellbag Forensics, Registry Decoder.*

Para recuperación de contraseñas en Windows: *Ntpasswd, Pwdump7, SAMInside, Ophcrack, Lophtcrack, ChromePass.*

Para utilidades de análisis de Red: *Wireshark, NetworkMiner, Netwitness Investigator, Network Appliance Forensic, Xplico, Snort, Splunk, AlientVault, Firebug.*

Para análisis de amenazas y vulnerabilidades: *PDF Tools, PDFStreamDumper, SWF Mastah, Captura BAT, Regshot, LordPE, OllyDbg, Jsunpack-n, OfficeMalScanner, SAS ClamWin, Xteg, ProcessHacker.*

Utilidades de análisis de dispositivos móviles y *tablets: iPhone: iPhoneBrowser, iPhone Analizer, iPhone-Dataprotection, SpyPhone; Android: Android-locdump, androguard, Viaforensics, Osaf, Santoku.*

Distribuciones software para el análisis forense digital: *Live DVD/USB/CD desarrolladas GNU/Linux, Kali, Backtrack, Santoku, Deft, Caine, Hélix, Autopsy, Volatility, Access FTK Imager, QPhotorec, Testdisk, Foremost, Nessus, Wireshark, Nmap* (Navarro, 2016).

Caso de estudio de la metodología en España

Se eligió el caso realizado en *INCIDE Digital Data, S.L.,* es una empresa especializada en el tratamiento e investigación de la información digital. Se anonimiza el caso, no se utilizarán nombres propios, fechas concretas ni lugares. El Cliente explicó a INCIDE que había sido denunciado por su Empresa por irregularidades detectadas en las cuentas de la compañía. En concreto, por alteración de los precios en las facturas con un proveedor con el que él se encargaba de gestionar los pedidos. La Empresa aportó cinco ordenadores que habían sido asignados al Cliente durante su periodo laboral.

El cliente solicitó los servicios de la empresa de investigación de información digital INCIDE para que realice el peritaje con el fin de que su abogado tuviera el máximo de información posible para encarar la defensa.

Los objetivos que determinó el juez de instrucción para el análisis de los discos proporcionados pertenecientes a los cinco ordenadores que aportó la Empresa son:

- Extraer todos los ficheros que, en su nombre, contengan una denominación específica *PALABRA_A o PALABRA_B*.
- Extraer todos los correos electrónicos enviados o recibidos entre *DIRECCION_1 y DIRECCION_2*.
- Verificar que los correos electrónicos extraídos son íntegros.
- Extraer todos los ficheros eliminados entre *FECHA_INICIAL y FECHA_FINAL.*

Respecto al análisis forense digital, específicamente adquirir y autenticar se procede como primer paso a tomar posesión de los dispositivos que se van a analizar, en este caso la empresa aportó cinco equipos de sobremesa con un disco duro cada uno; se extrajo los discos duros y se realizaron dos copias de cada disco, los discos duros originales fueron depositados ante un notario junto con una memoria *USB* que contenía unas fotografías realizadas durante el proceso de clonación de los discos en donde también se puede ver en el resultado del cálculo del hash.

En referencia a examinar y recolectar, se realizó una pequeña descripción del dispositivo, respecto a los discos duros se registró el tamaño del disco, número de particiones, sistema operativo y sistema de ficheros, así como los usuarios del equipo y fechas relevantes como la instalación y de último uso por parte de los usuarios; lo indicado es posible obtener con las herramientas *The Sleuth Kit y Regripper*.

Para cumplir con los objetivos planteados, se realizan las siguientes acciones:

- Listado de todos los archivos del sistema de ficheros con la herramienta *find*.
- Listado de todos los archivos y directorios del equipo, actuales y borrados recientemente, con la herramienta fls de The Sleuth Kit.

- Búsqueda de gestores de correo electrónico y/o webmail (cliente de correo electrónico al que se accede desde el navegador de Internet).
- Extracción de las cadenas del disco con la herramienta strings.
- Extracción de la timeline o línea temporal de los equipos con las herramientas tsk_gettimes y mactime de The Sleuth Kit.
- Carving: recuperar el máximo de ficheros y directorios eliminados con las herramientas TestDisk y PhotoRec.
- Extracción de un listado de todos los ficheros contenidos en la papelera de reciclaje.

En relación con el análisis de los datos, las hipótesis que se tienen que probar o desmentir son los objetivos establecidos en el proceso judicial, la información obtenida sirve también para redactar el informe pericial.

En atención al primer objetivo que consiste en extraer todos los ficheros que, en su denominación contengan el nombre *PALABRA_A o PALABRA_B*, se utilizó la lista de ficheros *allocated* del disco para realizar una búsqueda ciega mediante palabras clave, siendo las dos indicadas por el Cliente que debían figurar en el nombre del fichero.

Para verificar si existen ficheros eliminados que se conservan en el disco y que contienen las palabras *PALABRA_A o PALABRA_B* en el nombre, se procedió con una búsqueda en el listado de ficheros extraído con la herramienta *fls* de *The Sleuth Kit*.

Para cumplir otro objetivo que es extraer todos los correos electrónicos enviados o recibidos entre *DIRECCIÓN_1 (Cliente) y DIRECCIÓN_2 (Proveedor)*, la Empresa quiere que se demuestre cómo se llevaron a cabo las irregularidades entre el Cliente y el proveedor.

En este caso no se encontraron indicios en los ficheros temporales de Internet, sin embargo, se encontró gestores de correo electrónico *Microsoft Outlook* en los equipos que utilizan sistema operativo Windows, y el gestor de correo *Evolution* en los equipos que utilizaban sistema operativo *Ubuntu*.

Los buzones encontrados estaban asociados a una única dirección de correo electrónico, el correo corporativo del Cliente *(DIRECCIÓN_1)*, por consiguiente, las

búsquedas realizadas son de la dirección de correo electrónico *DIRECCIÓN_2* con la herramienta *grep*.

Se obtuvo como resultado que en los Disco 01 y Disco 02 la única coincidencia de la palabra *DIRECCIÓN_2* fue en la agenda de contactos; en el Disco 03 no se encontró ninguna coincidencia de la palabra *DIRECCIÓN_2*; en el Disco 04 se encontraron coincidencias en la agenda de contactos, en la bandeja de entrada y en la bandeja de correos eliminados. En la recuperación de estos correos se ha usado la herramienta *undbx* que extrae correos de las bases de datos de Outlook. Finalmente, en el Disco 05 se encontraron coincidencias en la agenda de contactos y en las bandejas de entrada y de salida, no obstante, el comportamiento de *Evolution* no fue el esperado, pues los correos no se podían abrir y aislar de forma individual, por lo que se creó una herramienta por parte del investigador.

Se aprovechó el script creado para separar los correos del Disco 05 para buscar correos electrónicos eliminados en las cadenas del disco, como resultado se encontraron correos enviados y/o recibidos entre *DIRECCIÓN_1 y DIRECCIÓN_2* en los Discos 01, 02, 04 y 05, en el Disco 03 no se encontró ninguna coincidencia de la palabra *DIRECCIÓN_2.* Se pudo verificar además que todos los correos son íntegros, es decir no se han detectado alteraciones. El Cliente solicita recuperar los ficheros eliminados entre *FECHA_INICIAL y FECHA_FINAL*. Para extraer los correos se ha utilizado las herramientas *TestDisk y PhotoRec*.

La información recopilada en las fases anteriores se presenta en un informe de resultados, cabe indicar que la fase de documentación se mantiene durante todo el caso, el perito registra todo el procedimiento y los resultados obtenidos, los mismos que va a presentar detalladamente tomando en cuenta todos los hechos.

Es importante indicar que, en todas las fases de la investigación, es de obligado cumplimiento seguir las buenas prácticas forenses, en las que se constituyen los principios de integridad, auditabilidad, experticia, formación adecuada y legalidad.

Para garantizar estos principios, se establece la cadena de custodia para asegurar que los datos no han sido modificados, y así poder presentar de forma clara y detallada, las pruebas en un proceso legal.(Taribó, 2016).

1.6.1.3 Metodología de extracción de evidencia digital en Colombia

Aspectos Generales en la Metodología de Colombia

En Colombia, desde el año 2004 empezó a funcionar la Dirección de Investigación Criminal e Interpol (DIJIN), con el objetivo de brindar apoyo a las acciones indagatorias e investigativas forenses desarrolladas por la Policía Nacional colombiana dedicadas específicamente a los medios informáticos, además en la Contraloría General de la Nación de Colombia en el mismo año crea su propio laboratorio de informática forense. Asimismo, en el mismo año, la Fiscalía General de Colombia publicó el manual de procedimientos del sistema de Cadena de Custodia con el propósito de preservar la evidencia de tal forma que pueda ser aceptada en un proceso judicial.(Lasso, 2017)

El peritaje informático en Colombia cuenta con cinco fases:

- Planificación que define lo que se desea conocer
- Recuperación de la información existente.
- Análisis de los datos en el que se busca la información mediante software forense.
- Desarrollo del informe pericial el cual mostrará los hallazgos de la investigación, y finalmente
- Fase de sustentación del informe pericial que es la comparecencia del perito ante el juez para dar a conocer el trabajo realizado (Lasso, 2017).

Para garantizar la validez probatoria de la evidencia digital en Colombia, según su legislación se debe tomar en consideración los criterios de autenticidad, confiabilidad, suficiencia y conformidad con las leyes y reglas de la administración de justicia, lo cual da lugar a la admisibilidad de prueba (Álvarez, Rivera, & Morales, 2012).

Ventajas en la Metodología de Colombia

1. La Fiscalía General de la República de Colombia, cuenta con el Manual de Procedimientos del Sistema de Cadena de Custodia, el cual contiene los métodos y normas para asegurar las características originales de la evidencia digital.

2. En la recolección de evidencia digital, Colombia considera las buenas prácticas basados en el RFC 3227 pautas para la colección de evidencias y su acopio en el que se destaca el principio de orden con el que debe ser recolectada la evidencia digital iniciando con la información más volátil hasta finalizar recolectando la información menos volátil.

3. Toma en consideración aspectos de la norma estándar ISO 27037, la misma que está dirigida a dispositivos actuales como medios de almacenamiento y elementos externos, sistemas críticos (alta disponibilidad), computadoras y dispositivos conectados en red, dispositivos móviles, y sistema de CCTV; la norma en mención está orientada a la extracción, identificación y secuestro de la evidencia digital.(Mesa, 2015).

Desventajas en la Metodología de Colombia

1. Cabe mencionar que la evidencia digital es frágil, debido a que puede ser objeto de manipulación y modificación; esto deriva que se dificulte la recolección y análisis de la misma.

2. Se evidencian falencias encontradas para el análisis de pruebas digitales, debido a los altos costos, existen falta de equipos y tecnologías idóneas para su estudio y peritaje de las pruebas documentales y medios informáticos (Jaramillo & Torres, 2016).

Preservación de la prueba en la Metodología en Colombia

En Colombia, para que la evidencia digital sea válida en procesos judiciales, debe ser preservada en su autenticidad, confiabilidad, integridad y tiene que ser repetitible. La evidencia debe tener las características siguientes:

- Admisibilidad: Debe cumplir las normas legales del país donde se ejecute el caso.
- Auténtico: Se debe comprobar que la evidencia es genuina.
- Completo: Debe comprobar todas las hipótesis que el investigador muestra en el tribunal.
- Fiable: No debe haber duda de su legitimidad y autenticidad.
- Creíble: Debería entenderse y ser fidedigna para el tribunal (Guerrero & Sanchez, 2013).

Parte de las fases del peritaje informático es la preservación de la prueba, es decir de los datos adquiridos, para su validación se inicia con la cadena de custodia, asegurando que se conserve la integridad de la información, a través de medidas estrictas de seguridad, por medio de la elaboración de una copia exacta de la información que posiblemente contenga la evidencia digital.(Lasso, 2017).

Metodología empleada en Colombia

El manual de procedimientos para Cadena de Custodia, está dirigida tanto a servidores públicos como privados o particulares, con el fin de que el material de prueba o evidencia sean aseguradas. Además, conserven las características originales y registro de las modificaciones que sufran dichos elementos, desde su recolección hasta su disposición final. El manual mencionado tiene como objetivo general unificar los criterios de funcionamiento del sistema de cadena de custodia, mediante estandarización de los métodos de trabajo y el mejoramiento del servicio en la administración de justicia en el ámbito penal (Iguarán, 2004).

La metodología está explicada por diagramas de todo el proceso del sistema de cadena de custodia, en los que se indica en primera instancia la fase de verificación y confirmación de un acto criminal, en esa fase nos muestra si existen elementos de prueba o evidencia que requiera su recolección o si es un bien a incautar.

Se identifica además si la evidencia requiere un análisis, en este caso se lo envía al laboratorio forense, en caso que no requiera un estudio se lo remite al almacén de

evidencias; si el elemento es analizado y resulta positivo, es almacenado como Elemento de Material Probatorio (EMP); dicha evidencia puede ser requerida judicialmente.

La evidencia puede ser de un delito informático, en ese caso el juez que lleve el caso debe dictaminar un peritaje informático a los equipos resguardados, se debe tomar en cuenta que la cadena de custodia no presente ninguna falencia por parte del personal que decomisó y aseguró los elementos de prueba o evidencias, con el fin de que la contraparte no tenga argumentos válidos para pronunciar que la cadena de custodia haya sido rota, interrumpida, contaminada o alterada ante el tribunal (Iguarán, 2004).

Es necesario también tomar en cuenta que existen dos fases de la cadena de custodia que son vulnerables, la primera es la fase de extracción y preservación de la evidencia que es la que está más propensa para cometer errores por la pericia que conlleva dichas acciones, la segunda fase también vulnerable es el transporte adecuado, entrega controlada y la individualización en la que puede existir errores en los procesos.

En Colombia con el fin de no dar cabida a pronunciamientos de la parte contraria en un proceso judicial, para recibir la evidencia tecnológica se debe efectuar mediante notario con el fin de que puntualice paso a paso los procedimientos de recolección, descripción y demás procesos que certifiquen la idoneidad y protección de la información en los equipos, así como también el proceso de copias de discos duros y memorias, asimismo, efectuando la entrega oficial de la llave pública de encriptación de la información mediante el algoritmo hash u otro si se requiere dado la cantidad de archivos almacenados en el ordenador (Ramírez & Castro, 2018).

La metodología de Análisis Forense Digital en Colombia también toma en consideración para su aplicación en los procedimientos para Cadena de Custodia algunos aspectos de la norma ISO/IEC 27037 la cual establece los principios:

- Identificación: Reconocimiento inicial de donde se encuentra la evidencia digital.
- Recolección: La acción que realiza el perito informático y procede a trasladarla al laboratorio, en el cual se debe tomar en consideración los recursos informáticos y tiempo disponibles; el proceso debe documentarse y sustentarse adecuadamente en caso que deba defenderse en un caso judicial.

- Adquisición: Es un proceso que debe seguirse por parte del perito, el cual debe realizar una copia exacta del contenido físico o lógico de los objetos involucrados en la investigación.

- Preservación: Se refiere a que la evidencia digital debe conservar su integridad durante todo el proceso (Jaramillo & Torres, 2016).

Herramientas utilizadas para análisis forense en Colombia

Las herramientas que se utilizan son:

- *EnCase*, *KeyLogger*, *Autopsy*, *HashMyFiles* para el manejo de evidencia digital.
- *EnCase*: se utiliza para recolección de evidencia digital.
- *KeyLogger*: se utiliza para monitorear el uso de las computadoras, eventos realizados por el teclado, imágenes visualizadas, controlar remotamente un computador.
- *Autopsy*: se utiliza para analizar los discos duros y *Smartphone* de manera eficiente.
- *HashMyFiles*: se utiliza para encriptar todo tipo de archivo para verificar la identidad y autenticidad de un archivo.
- *Nmap*: se utiliza para escanear computadoras y redes enteras, se evidencia los servicios que se ejecutan en un ordenador y se identifica el sistema operativo.
- *Wireshark*: se utiliza para detectar todo el tráfico de red
- *FTK*: se utiliza como herramienta estándar en software forense de computadoras.

Caso de estudio en Colombia

El caso seleccionado se trata de una empresa de Colombia que se dedica a la venta al por mayor de ropa femenina, que se ve aquejada en la entereza y confidencialidad de su información y probablemente en la solidez de sus finanzas, debido a que en los primeros días del mes de noviembre de 2013 le intentaron hacer un fraude por la suma de doscientos millones de pesos en mercancía a través de Internet.

El requerimiento es investigar el origen del incidente, posibles delincuentes, herramientas utilizadas, daños ocasionados, fallas que permitieron el ilícito y correcciones a corto plazo.

En la investigación forense, se verificó que la empresa de ropa femenina que se le va a denominar, empresa A recibe un correo de uno de sus clientes, representante legal de la compañía a quien se le denominará cliente X, donde solicita doscientos cincuenta millones de pesos en mercancía y adjunta como soporte el recibo de consignación bancaria correspondiente al pago del negocio (Arnedo, 2014).

El cliente X solicita se envíe la mercadería a una dirección física, la cual se notó no estaba entre las que usaban normalmente, pero se argumentó que hubo una ampliación de sedes. Lo indicado genera sospecha, debido a que los directivos de la compañía del cliente X acostumbran a socializar con sus proveedores cualquier cambio que afecte su lógica de negocio y hasta el momento no había llegado información de nueva sede o traslado alguno.

Por tanto, se llama a la compañía que realizó la compra, es decir la empresa X, procedimiento que se hace para validar la transacción. No obstante, se descubre que esta empresa no ha solicitado mercancía alguna y por ende no ha hecho envío alguno. Luego, se verifican las transacciones bancarias y evidentemente no existe ingreso por esa cuantía. Por consiguiente, se desvirtúa la legalidad del recibo de entrega que llegó adjunto al correo electrónico. Se verifica la dirección donde se debería enviar la mercancía, por parte del personal de la empresa X en la ciudad donde se ubican, específicamente la ciudad de Montería, y se descubre que el sitio corresponde a un local alquilado, el cual se encuentra desocupado.

Se encontraron novedades en la consecución de este delito: La empresa A no cuenta con servidor de correo propio. Utilizan el servicio de correo gratuito para sus negocios. Tienen un solo email donde manejan sus negocios, denominado xxx@hotmail.com.

Entre las evidencias digitales adquiridas en la consecución de este delito se tiene el mensaje de correo electrónico donde llegó el mensaje fraudulento, y el archivo adjunto en formato PDF, donde se soporta la transacción bancaria fraudulenta.

Se revisa el correo electrónico donde llegó el correo fraudulento. Se verifica su autenticidad y se observa que tiene un nombre similar al original, con un cambio casi imperceptible. El correo de la empresa X es empresax@xxxxxxx.com y el utilizado para el fraude es empresax.@xxxxxxxx.com. Se analiza su cabecera y se determina que provienen de una IP en particular] (Arnedo, 2014)

Se rastrea la dirección IP en mención para ver su procedencia a través del portal es.geoipview.com, el cual arroja una dirección de un servidor del proveedor gratuito xxxmail en los Estados Unidos, con lo cual se comprueba que el estafador no utilizó un servicio corporativo rastreable.

Posteriormente se procede a descargar el archivo adjunto que llegó en el correo electrónico fraudulento y se sacan dos copias. Este archivo tiene formato PDF. El archivo en mención previo al análisis se hizo un resumen hash y se sacaron dos copias de seguridad, son validadas posteriormente dichas copias por hash.

Para el análisis se ejecutará el software *Exiftool*, el cual será utilizado para el análisis de metadatos en el documento descargado.

Una vez obtenidos los metadatos indica en el campo Autor: XXXXL., además fecha de elaboración: noviembre 8 de 2013.

Se solicita información a la compañía X con relación al usuario extraído, se nos informa que ese usuario corresponde al empleado XXXXL., quien es un empleado activo de la empresa. Los directivos de la empresa se reúnen con dicho empleado y le solicitan explicación de los hechos, no obstante, él niega todo lo que le exponen.

En este caso desde la ciudad de Montería donde tiene la sede la empresa X y ya en la compañía se identifica el computador asignado al empleado investigado. El

ordenador tiene el sistema operativo Windows 7 instalado, este se encuentra encendido. Se realiza un volcado de memoria con el software *DumpIT*.

Se realiza dos copias al disco duro con el aplicativo *FTK Imager*, y se hace un hash a cada uno. Se ratifican los resultados y las copias quedan correctas. Se realiza el análisis al equipo donde se revisa la imagen del disco, se hace el montaje respectivo de una de las imágenes y se procede a hacer una búsqueda por nombre, tratando primero que todo de localizar un documento de nombre documento1.pdf.

Se ubica en el disco montado con la imagen del disco duro del empleado sospechoso y evidentemente se muestra un único archivo con ese nombre. Como siguiente acción se procede a abrirlo, y ciertamente coincide con el archivo utilizado como prueba para efectuar el fraude. Se confirma nuevamente con el software *Exiftool* arrojando los mismos resultados.

Ahora se utiliza el volcado de memoria realizado al computador del empleado XXXXL. Esto se realiza en el equipo que se utiliza en la investigación forense, con el software *FTK Imager*. La herramienta en mención abre una interfaz tipo editor binario (hexadecimal), lo cual permite proceder a buscar en memoria el nombre documento1.pdf, para ver si el empleado XXXXL., estaba trabajando en ese documento al momento de llegar a su oficina; efectivamente se encuentran indicios de haber trabajado con el documento documento1.pdf.

Se concluye que el empleado XXXXL., pretendía estafar a la empresa A tratando de obtener de ella una suma considerable en mercancías, aprovechándose de datos obtenidos en la empresa X donde labora (Arnedo, 2014).

Las Herramientas de software que se utilizaron en este caso, se detallan a continuación:

Tabla 9. Herramientas de software utilizadas en caso de estudio Colombia

Software	Tipo	Interfaz	Facilidad de uso	Funcionalidad	Recomendado
Geolocalizador ONLINE: es.geoipview.com	GPS, Localización	WEB	Fácil	Objetivo exitoso	Si
Exiftool	Extracción Metadatos	Consola	Difícil	Objetivo exitoso	Si
DumpIT	Volcado Memoria	Consola	Fácil	Objetivo exitoso	Si
Ftk Imager	Suite (Copias a imagen, Volcado Memoria, Editor Hexadecimal, entre otras)	GUI	Algo difícil	Objetivo exitoso	Si

Fuente: Herramientas de análisis forense en la Investigación de delitos informáticos (Arnedo, 2014)

1.6.2 COMPARATIVA DE LAS METODOLOGÍAS ESTUDIADAS

Respecto a las metodologías de informática forense para tratamiento de evidencias digitales estudiadas de España, Argentina y Colombia, se realizó un resumen comparativo en el que se muestran los siguientes parámetros:

Tabla 10. Comparativa de Metodologías en Argentina, España y Colombia

Parámetros / País	España	Argentina	Colombia
Nombre Metodología	Buenas Prácticas de RFC 3227 UNE 71505 UNE 71506 e ISO 27037	Guía de Buenas Prácticas Basada en la Metodología de Rodney Mckemmish e ISO 27037	Metodología de mejores prácticas Basada en el Manual de Procedimientos del Sistema de Cadena de Custodia e ISO 27037 / Framework
Caso de Estudio	Cliente denunciado por fraude electrónico solicita intervención de INCIDE	Recepción de un correo electrónico con una presunta intimidación que recibe un usuario final	Intento de Fraude en mercancía a través de Internet
Ventajas	1. Ofrece las directrices y orientación para tratar el manejo de la evidencia digital. 2. Se utiliza la norma ISO 27037 como estándar. 3. La metodología en España	1. Cuenta con una guía para la obtención, preservación y tratamiento de evidencia digital para	1. La Fiscalía General de la República de Colombia, cuenta con el Manual de Procedimientos del

	aplica normas y estándares que aportan seguridad y garantías en todo el proceso.	presentación en procesos judiciales.	Sistema de Cadena de Custodia. 2. En la recolección de evidencia digital, Colombia considera las buenas prácticas basados en el RFC 3227. 3. Toma en consideración aspectos de la norma estándar ISO 27037, la misma que está dirigida a dispositivos; la norma en mención está orientada a la extracción, identificación y secuestro de la evidencia digital (Mesa, 2015).
Desventajas	1. Las aplicaciones y herramientas utilizadas en las mejores prácticas de recolección de evidencias digitales utilizadas en esta metodología, puede variar con el transcurso del tiempo, teniendo en cuenta que la evolución del software es constante.	1. La falta de capacitación del personal que interviene en la recolección de dispositivos tecnológicos abre la posibilidad de que se omita o no se considere el secuestro de todos los dispositivos en el lugar de los hechos para garantizar la suficiencia de la evidencia. 2. Nunca existe una pericia informática igual a otra, varían en el escenario, las pruebas y la modalidad que han sido obtenidas; y las partes que intervienen en la investigación.	1. La evidencia digital es frágil, puede ser objeto de manipulación y modificación, puede dificultar la recolección de la evidencia, convirtiendo así en una desventaja para el sistema judicial. 2. Se verifica falencias para la extracción y análisis de pruebas digitales por falta de equipos y tecnologías idóneas para su estudio y peritaje informático, el costo real para contar con la estructura adecuada a utilizar en temas forenses, son altos lo que nos da una razón clara de la falta de los mismos.
Software Utilizado	Para análisis de red más habituales son Snort, Nmap, Wireshark, Xplico; Para tratamiento de discos se utilizan Dcdd3, Mount Manager, Guymager; Herramientas para el tratamiento de memoria Volatility, Memoryze, RedLine; Herramientas para el análisis de aplicaciones OllyDbg, OfficeMalScanner, Radare, Process explorer, PDFStreamDumper;	En Argentina se utilizan herramientas útiles para el manejo de evidencia digital, entre las cuales se encuentran EnCase, FTK, IEF, RegRipper, Forensic Registry Editor (FRED), cabe indicar que dichas herramientas aportan a garantizar el	EnCase, KeyLogger, Autopsy, HashMyFiles. EnCase, se usa para recolección de evidencia digital. KeyLogger, sirve para monitorear el uso de las computadoras, eventos realizados por el teclado, imágenes visualizadas, controlar remotamente un computador.

	Además, se utilizan Suites de aplicaciones DEFT, ForLEx, CAINE, Autopsy	principio de la suficiencia.	Autopsy, que sirve para analizar los discos duros y Smartphone de manera eficiente. *HashMyFiles*, es una herramienta que permite encriptar todo tipo de archivo para verificar la identidad y autenticidad de un archivo. *Nmap*, para escanear computadoras y redes enteras, se evidencia los servicios que se ejecutan en un ordenador y se identifica el sistema operativo.

Fuente: Autor

CAPÍTULO II

MÉTODO

2.1 TIPO DE ESTUDIO

La investigación utilizada en el presente estudio es una metodología mixta es decir de dos tipos: cualitativa mediante una entrevista a un experto[4] en el tema de informática forense y el análisis de las diversas metodologías que se usan en informática forense; y se complementa con investigación cuantitativa a través de la encuesta desarrollada para analizar el estado actual de las metodologías de extracción de evidencia digital en Ecuador, se realizó a peritos calificados en el Consejo de la Judicatura, en donde se ha difundido previamente la metodología propuesta en esta tesis con base en la Norma ISO/IEC 27037:2012 y en buenas prácticas de las metodologías utilizadas en España, Argentina y Colombia.

La propuesta de metodología es resultado de un estudio exploratorio que consiste en conocer sobre el tema del manejo de evidencia digital a nivel nacional e internacional, con el objetivo de encontrar todo lo relacionado a las mejores prácticas, utilización de normas, estándares y uso de herramientas para identificación, recolección, preservación, análisis y presentación de evidencia digital válida en un proceso judicial.

2.2 MÉTODO

En la presente investigación se utiliza el método inductivo – deductivo; se parte de un conocimiento general de extracción de evidencia digital a nivel iberoamericano y con base a los análisis de aspectos relevantes y mejores prácticas de dichas metodologías, se diseña una metodología basada en los aspectos mencionados y en la Norma ISO/IEC 27037:2012.

[4] Los resultados de la entrevista se puede leer en el apartado 3.3 con el análisis del caso

2.3 POBLACIÓN Y MUESTRA

La población para la presente investigación son los peritos informáticos calificados en la Función Judicial los mismos que a la fecha de la investigación contaban con un número de 97 que constan en el portal del Consejo de la Judicatura ecuatoriano, la información del cálculo del número de la muestra se encuentra detallado en el presente documento. Además se eligió a un perito informático calificado en el Consejo de la Judicatura, el mismo que fue entrevistado para que dé su opinión de experto con respecto a la metodología propuesta en esta tesis.

2.4 SELECCIÓN DE INSTRUMENTOS DE LA INVESTIGACIÓN

En la investigación se eligió como instrumento principal la Norma Internacional ISO/IEC 27037:2012, que es la base del estudio, además se utilizó la información de metodologías y buenas prácticas de manejo de evidencia digital utilizadas a nivel iberoamericano, en países como España, Argentina y Colombia, las cuales contribuyeron para el desarrollo de la metodología planteada.

Otro instrumento que aportó en la investigación, fue una encuesta a peritos informáticos con el fin de diagnosticar los métodos utilizados en el país respecto a la extracción de evidencia digital en Ecuador.

2.4.1 CÁLCULO DE LA MUESTRA PARA LA ENCUESTA

Con el fin de orientar, diagnosticar, reforzar, guiar la investigación, se utiliza como un instrumento una encuesta previa al diseño de la metodología planteada en el presente documento, la encuesta va dirigida a un público objetivo que son los peritos informáticos en Ecuador.

Para calcular el número de la muestra se parte del hecho del número de peritos informáticos a la fecha del planteamiento de la encuesta, la misma que se realizó el 15 de agosto de 2018, en esa fecha, estuvieron registrados un total de 97 peritos informáticos

calificados en el Consejo de la Judicatura según la página web de la función judicial ecuatoriana. Los mismos que se encuentran distribuidos como se muestra a continuación:

Tabla 11. Distribución de peritos informáticos a nivel nacional

Provincia	Número de Peritos
AZUAY	16
BOLIVAR	0
CAÑAR	0
CARCHI	0
COTOPAXI	3
CHIMBORAZO	5
EL ORO	3
ESMERALDAS	1
GUAYAS	11
IMBABURA	3
LOJA	4
LOS RÍOS	2
MANABÍ	3
MORONA SANTIAGO	0
NAPO	1
PASTAZA	1
PICHINCHA	33
TUNGURAHUA	8
ZAMORA CHINCHIPE	0
GALÁPAGOS	0
SUCUMBÍOS	0
ORELLANA	0
SANTA ELENA	0
SANTO DOMINGO DE LOS TACHILLAS	3
TOTAL	97

Fuente: El autor

El cálculo de la muestra sabiendo el tamaño de la población se calcula con la siguiente fórmula:

$$n = \frac{N\,\delta^2 Z^2}{(N-1)\,e^2 + \delta^2 Z^2}$$

Donde *n* es el tamaño de la muestra, *N* equivale al tamaño de la población en este caso 97, δ es la desviación estándar de la población que, generalmente cuando no se tiene su valor, suele utilizarse un valor constante de 0,5; *Z* es el valor obtenido mediante niveles de confianza. Es un valor constante que, si no se tiene su valor, se lo toma en relación al 95% de confianza equivale a 1,96 (como más usual) o en relación al 99% de confianza

equivale 2,58; valor que queda a criterio del investigador; finalmente el valor *e* es el límite aceptable de error muestra que, generalmente cuando no se tiene su valor, suele utilizarse un valor que varía entre el *1%* (0,01) y *9%* (0,09), valor que queda a criterio del encuestador en este caso se tomó el valor 0,5.

Reemplazando en la fórmula, el número de la muestra que se debe tomar es de *27* que serán el número de peritos encuestados.

A continuación, se indica las preguntas de la encuesta realizada en la fecha *15* de agosto de 2018 a través de las funciones del correo electrónico *mail* en la opción Drive / Formularios de Google.

2.4.2 PREGUNTAS DE LA ENCUESTA PARA DIAGNOSTICAR LA FORMA DE EXTRACCIÓN DE EVIDENCIA DIGITAL EN ECUADOR

Fecha: 15-08-2018
Nombre y Apellido: _____
Correo electrónico: _____

1. ¿Cuál es su nivel de educación actualmente?

- □ Tecnólogo
- □ Superior Terminada (Título de Tercer Nivel)
- □ Maestría Iniciada
- □ Maestría Terminada (Título de Cuarto Nivel)
- □ Otro Especifique _____

2. ¿Cuál es el área de especialidad que tiene actualmente?

- □ Ingeniero Informático
- □ Especialista en Ciberseguridad
- □ Especialista en Informática Forense
- □ Especialista en Criminalística

□ Otro Especifique _____

3. ¿Cuántos años de experiencia tiene actualmente como perito informático?

□ 0 a 1 año
□ 2 años
□ 3 años
□ 4 años
□ Más de 4 años

4. ¿Utiliza alguna metodología para extraer evidencia digital de un disco duro?

□ Si
□ No

En caso que su respuesta sea afirmativa indique qué método utiliza:

_____

5. De las metodologías que se utilizan para extracción de evidencia digital valore del 1 al 5 su grado de utilización:

Tabla 12. Utilización de estándares de metodologías para extracción de evidencia digital

Metodología	**1**	**2**	**3**	**4**	**5**
RFC 3227					
ISO/IEC 27037:2012					
UNE 71505					
UNE 71506					
ISO/IEC 27041:2015					
ISO/IEC 27042:2015					
ISO/IEC 27043:2015					
UNE 197010:2015					
ISO/IEC WD 27044					
Otro Especifique: -------					

Fuente: El autor

6. ¿Conoce usted que personas son las responsables de la identificación, recolección, adquisición y preservación de potencial evidencia digital conforme a lo indicado en la norma ISO 27037?

□ Si

□ No

En caso que su respuesta sea afirmativa indique cuales son: _____

7. ¿Qué tipo de atributos en la extracción de evidencia digital de un disco duro según su criterio es válido en un proceso judicial?

□ Relevancia

□ Confiabilidad

□ Suficiencia

□ Todas las anteriores

8. Porcentaje de uso de Herramientas: (Califique según el caso Mucho, Poco, Rara Vez, Nunca)

Tabla 13. Utilización de herramientas para extracción de evidencia digital

Herramienta	1. Nada	2. Rara Vez	3. Poco	4. Mucho	5. Siempre
FTK Imager					
Dd					
Fdisk					
RegRipper					
Exiftool					
The Sleuth Kit					
TestDisk					
PhotoRec					
Hélix					
Autopsy					
Fire Linux					
WinCE					
Encase					
Keylogger					
Dcfldd					
Caine					
Caine & Abel					
Otro Especifique: -------					

Fuente: El autor

9. ¿Cuál de los siguientes conceptos indica que existe ruptura de la cadena de custodia en extracción de evidencia digital de un disco duro?

- □ Si la evidencia es manipulada destruyendo o alterando su integridad.
- □ Es la interrupción de la secuencia lógica de los procesos que la conforman, la cual puede o no constituir una alteración de la evidencia.
- □ La cadena de custodia se rompe cuando no se registra todo lo que acontece a los indicios o evidencias.
- □ Todos los anteriores

10. Indique 3 principios básicos que se deben considerar durante la recolección de evidencia digital de discos duros:

1._____
2._____
3._____

11. Indique 5 actividades o pasos que usted realiza para la presentación de evidencia digital de unidades de disco duro en un proceso judicial

1._____
2. _____
3._____
4. _____
5. _____

12. Cuál de las metodologías citadas de extracción de evidencia digital de discos duros listadas en la pregunta 5 cree usted que cumple con los siguientes principios básicos.

- □ La aplicación de métodos, se deben utilizar métodos adecuados de manera que las evidencias puedan preservar la originalidad de la prueba y si es posible obteniendo una copia de respaldo.

- □ Proceso auditable, los procedimientos y la documentación que se creen deben ser realizados siguiendo las buenas prácticas profesionales, pudiendo seguir las trazas y ver las evidencias del trabajo realizado y sus resultados.
- □ Proceso reproducible, de manera que los métodos y procedimientos sean reproducibles, verificables y argumentales para que otros entendidos puedan dar validez a las actuaciones realizadas.
- □ Proceso defendible, se deben nombrar las herramientas utilizadas, siendo estas validadas y contrastadas para su fin dentro del análisis.
- □ Digite su respuesta:

_____

2.4.3 RESULTADOS DE LA ENCUESTA DE EXTRACCIÓN DE EVIDENCIA DIGITAL

1. Respecto a la pregunta: De las metodologías que se utilizan para extracción de evidencia digital valore del 1 al 5 su grado de utilización; se verificó con respecto a la Norma ISO/IEC 27037:2012.

Únicamente el 33% de los peritos de un total de 27 considera que la norma ISO/IEC 27037:2012 es la más importante tomar en cuenta en la extracción de Evidencia digital de discos duros, es decir actualmente no es muy utilizada en la actuación pericial en el país.

Tabla 14. Uso de metodologías de extracción de evidencia digital

Metodología / Grado Utilización	1	2	3	4	5
RFC 3227	12	1	4	2	8
ISO/IEC 27037:2012	6	2	6	4	9
UNE 71505	10	3	2	8	4
UNE 71506	10	4	1	10	2
ISO/IEC 27041:2015	8	1	8	8	2
ISO/IEC 27042:2015	8	3	8	4	4
ISO/IEC 27043:2015	10	1	8	6	2
UNE 197010:2015	10	3	6	6	2
ISO/IEC WD 27044	8	1	8	8	2
Otro Especifique: -------	16	1	4	2	4

Fuente: Encuesta a peritos informáticos elaborado por el autor

2. Respecto a la pregunta: ¿Conoce usted que personas son las responsables de la identificación, recolección, adquisición y preservación de potencial evidencia digital conforme a lo indicado en la norma ISO 27037?

Esto indica que el 33,3% de un total de 27 peritos encuestados conoce los responsables del manejo de evidencia digital indicados en la Norma ISO/IEC 27037:2012, es decir, el restante 66,7% no tiene conocimiento de los perfiles que se manejan en la actuación pericial según la norma mencionada. .

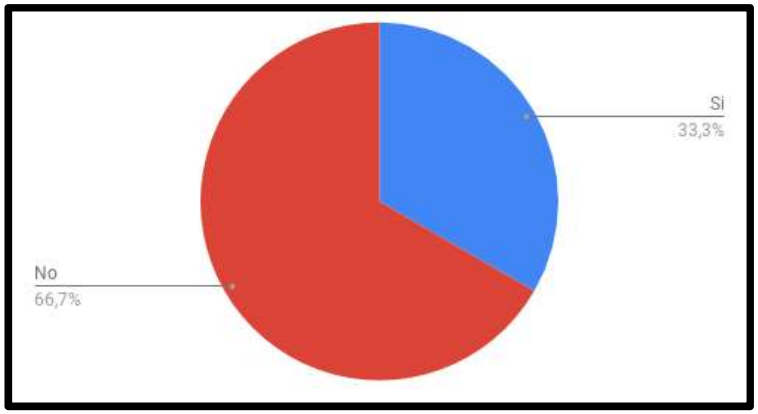


Figura 3. Perfiles de investigadores en la ISO/IEC 27037:2012

Fuente: Autor

3. Respecto a la pregunta 7 que se refiere a ¿Qué tipo de atributos en la extracción de evidencia digital de un disco duro según su criterio es válido en un proceso judicial? las opciones consideradas son: Relevancia, Confiabilidad, Suficiencia y Todas las anteriores, se obtuvo:

Un 58,3% de los encuestados indica que el tipo de atributos válidos son la relevancia, confiabilidad y suficiencia para la extracción de evidencia digital y un 41,7% únicamente elije el atributo de la confiabilidad en la extracción de evidencia digital como se muestra a continuación.

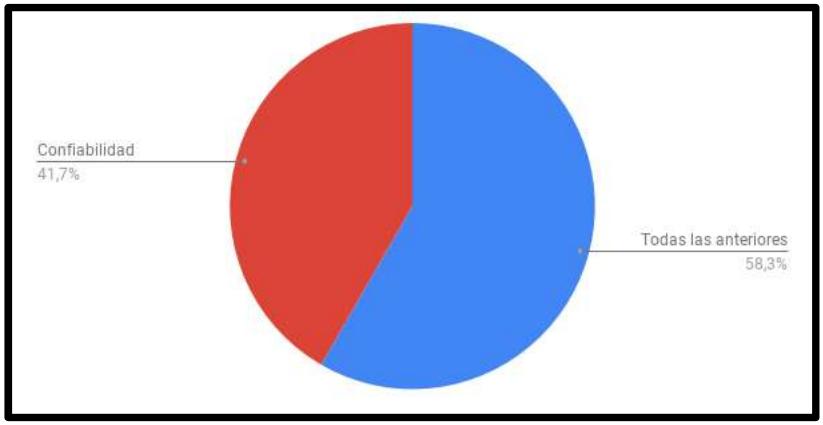


Figura 4. Criterio de validez de tipo de atributos para extracción de evidencia digital

Fuente: Autor

CAPÍTULO III

RESULTADOS

3.1 DISEÑO DE LA METODOLOGÍA

La Norma Internacional ISO/IEC 27037:2012 proporciona pautas para actividades específicas en el manejo de la evidencia digital; se requieren procesos como son: identificación, recopilación, adquisición y preservación de la evidencia digital potencial con el fin de mantener su integridad.

Se pretende en el presente documento diseñar una metodología aceptable para la obtención de evidencia digital que contribuya a su admisibilidad en procesos judiciales y/o en las instancias requeridas; esta norma pretende orientar a Especialistas en evidencia digital de Primera Intervención (DEFR), Especialistas En Evidencia Digital (DES), Especialistas en respuesta a incidentes y gerentes de laboratorios forenses.

La aplicación de la Norma Internacional ISO 27037 requiere el cumplimiento de las leyes, normas y regulaciones nacionales, es decir no pretende reemplazar requisitos legales específicos de ninguna jurisdicción. Esta Norma Internacional puede ayudar a facilitar el intercambio de evidencia digital entre jurisdicciones.

La Norma ISO 27037 proporciona orientación para los siguientes dispositivos y/o funciones que son utilizados en diversas situaciones, eso coadyuva a la identificación de incidentes:

- Medios de almacenamiento digital utilizados en ordenadores estándar como discos duros, disquetes, discos ópticos y magneto - ópticos, dispositivos de datos con funciones afines.
- Telefonías móviles, asistentes digitales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria.

- Sistemas de navegación móvil.
- Cámaras fotográficas y videocámaras digitales (incluido CCTV).
- Ordenador estándar con conexiones de red,
- Redes basadas en TCP/IP y otros protocolos digitales, y
- Dispositivos con funciones similares a las anteriores.

Se debe tomar en cuenta que la norma en mención no incluye la preparación forense, sin embargo, es la preparación forense la que puede respaldar en gran medida el proceso de identificación, recopilación, adquisición y preservación de la evidencia digital (ISO/IEC, 2012).

3.1.1 Fases de la Metodología

La presente metodología ha sido diseñada en base a la Norma Internacional ISO/IEC 27037:2012, la misma que contiene pautas para la identificación, recolección, adquisición y preservación de evidencia digital, además se incluyen aspectos de mejores prácticas de informática forense utilizadas en España, Argentina y Colombia.

Las fases o procesos de la metodología planteada basada en la norma ISO/IEC 27037:2012 son:

1. Ubicación de la Escena
2. Asegurar y Evaluar la Escena
3. Identificación de las evidencias
4. Recolección y Adquisición
5. Conservación y Preservación
6. Análisis de la Evidencia

La metodología propuesta está compuesta por las fases indicadas, cabe indicar que el Análisis queda fuera del alcance de la Norma ISO/IEC 27037:2012, no obstante, la fase de análisis fue diseñada en base a las mejores prácticas de informática forense de los países que se incluyen en el estudio, por lo tanto es parte del proceso diseñado para la metodología planteada.

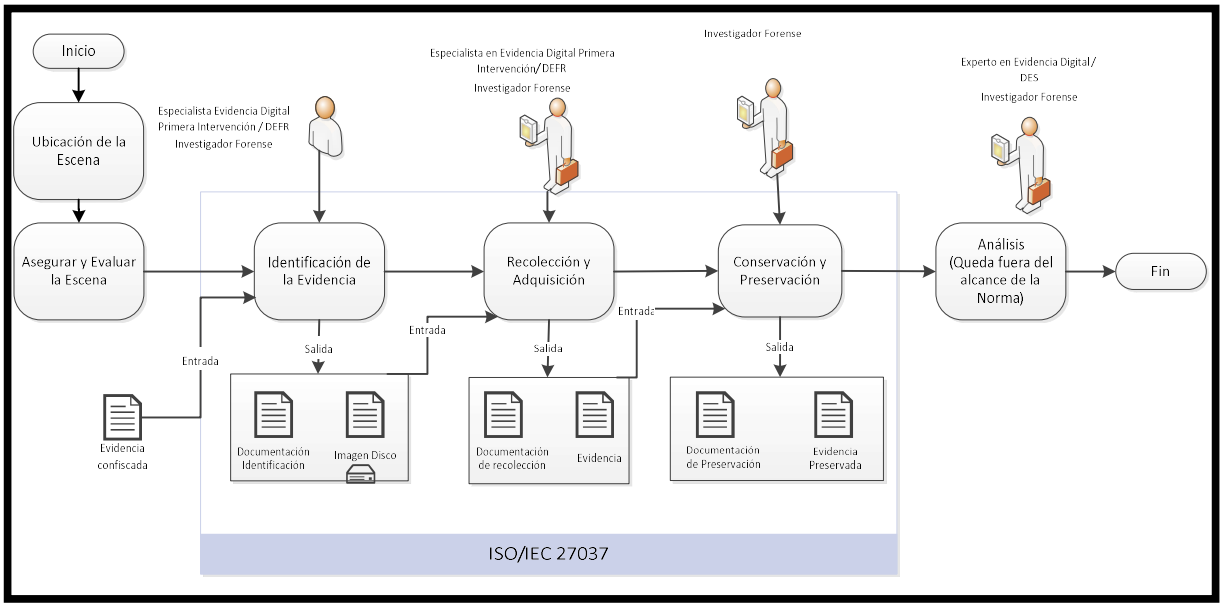


Figura 5. Diagrama general de metodología propuesta

Fuente: Autor

Fase 1: Ubicación de la escena de los hechos

Es importante la ubicación del lugar de los hechos que es el espacio físico que debe ser comprendido en un concepto amplio, su superficie depende de la naturaleza y las situaciones del hecho que se investiga; es decir se refiere a toda extensión, área física o lugar donde se ha producido un hecho presumiblemente delictivo (Gitec, 2012,p.16).

En este caso el lugar de los hechos es donde se ha cometido un delito informático, sin embargo, existen hechos punibles que se comenten como consecuencia del incidente cibercriminal.

Se tomó de la Metodología Colombiana del Manual de Procedimientos Para Cadena de Custodia y se acopló a la metodología diseñada en el presente trabajo de investigación, aspectos que son idóneos para ubicar la escena de los hechos, asimismo se elaboró una lista de verificación (CheckList) de la información relevante que se considera para la localización de la escena, además una hoja de trabajo para registrar dicha información.

Tabla 15 Lista de Comprobación - Checklist Fase 1 Ubicación del lugar de los hechos

Actividades de la Fase 1 Ubicación del lugar de los hechos	**Chequeo: SI**	**NO**
I. Localización de la Escena		
Información Dirección		
Provincia, Cantón Parroquia		
Barrio		
Localidad		
Características		
Zona Urbana		
Zona Rural		
I. Institución donde se desarrollan los hechos		
Empresa Pública		
Empresa Privada		
Persona Natural (Particular)		
Fijación Fotográfica		
Ilustración de imágenes de la ubicación del lugar de los hechos		

Fuente: Autor

Tabla 16. Actuación del perito. Fase 1. Ubicación del lugar de los hechos

Provincia	**Ciudad**	**Parroquia**	**Fecha y Hora**
_____	_____	_____	_____
I. Lugar de los Hechos			
Barrio: _____			
Zona: _____			
Calle Principal: _____			
Intersección: _____			
Número: _____			
Hora probable de ocurrencia de los hechos: _____			
II. Protección del lugar de los hechos			
Acordonamiento: Si _____	No _____		
III. Observaciones del lugar de los hechos			
¿Hubo alteración del lugar de los hechos? Si _____	No		
Peritos Intervinientes _____			
Observaciones: _____			
IV Especialista de Primera Intervención (DEFR)			
Nombres y Apellidos del Perito _____			
Profesión: _____			
No. Identificación Pericial: _____			
Dirección de Contacto: _____			
Teléfono (s): _____			
Correo Electrónico: _____			

Fuente: Autor

Fase 2: Asegurar y Evaluar la Escena

La etapa de aseguramiento y evaluación de la escena fue tomada de la Metodología Argentina, debido a su importancia para iniciar la investigación en escenas donde se han cometido delitos informáticos en este caso.

La consideración primordial del especialista de primera intervención DEFR debe ser la seguridad de todos en la escena del crimen. Toda acción debe cumplir con las leyes estatales según su jurisdicción.

El DEFR debe asegurar la escena y debe asegurarse que se preserva la integridad de la evidencia potencial, se debe tomar en cuenta que la misma puede alterarse, eliminarse o destruir fácilmente; por lo que los investigadores deben documentar, fotografiar y asegurar la evidencia en la escena, debe seguir los siguientes pasos:

- Seguir la política del departamento para asegurar las escenas del crimen.
- Asegurar de inmediato todos los dispositivos electrónicos.
- Asegurarse que ninguna persona no autorizada tenga acceso a ningún dispositivo electrónico en la escena.
- Rechazar la ayuda o asistencia técnica de personas no autorizadas.
- Retirar a todos los individuos de la escena del crimen o del área donde se recolectarán las pruebas de evidencia digital.
- Asegúrese de que la condición de cualquier dispositivo electrónico no se altere.
- Deje el ordenador o dispositivo apagado en caso que esté en dicho estado.

Los componentes como son teclado, ratón, los medios de almacenamiento extraíbles, y otros elementos pueden contener pruebas latentes como huellas dactilares, ADN u otras pruebas físicas que deben conservarse. Los primeros en responder deben tomar medidas adecuadas para garantizar que la evidencia física no se vea comprometida durante la documentación; se generó una lista de comprobación (CheckList) y una hoja de trabajo para asegurar y evaluar la escena que se presentan a continuación (Mukasey, Sedgwick, & Hagy, 2001).

Tabla 17. Lista de comprobación - Checklist fase 2 Asegurar y evaluar la escena

Actividades de la Fase 2 Asegurar y Evaluar la Escena	**Chequeo: SI**	**NO**
I. Seguir procedimientos para asegurar las escenas del crimen		
Registro de información de dispositivos encontrados en la escena:		
Computadoras de Escritorio		
Computadoras portátiles		
Discos duros		
Discos externos		
Discos ópticos		
Impresoras		
Escáneres		
Memorias USB		
Tarjetas de Memoria		
Dispositivos Móviles		
Dispositivos periféricos:		
Teclado		
Mouse		
Micrófono USB		
Cámaras web		
Lectores de tarjetas de memoria		
Dispositivos de VoIP		
Otras fuentes potenciales de evidencia digital		
Unidades de cinta de almacenamiento de datos		
Equipo de vigilancia		
Cámaras digitales		
Cámaras de video		
Grabadoras de audio digital		
Grabadoras de video digital		
Reproductores mp3		
Audio satelital, receptor de video y tarjetas de acceso		
Consolas de video juegos		
Auriculares de chat de ordenadores		
Switch para compartir teclado, mouse y video (KM)		
Lector de tarjetas SIM		
Receptor del sistema de posicionamiento global GPS		
Lector de huella digital		
Dispositivos de red:		
Hub de red		
Tarjeta de red para laptop y cable Ethernet		
Módems de Internet		
Switch de red y fuente de alimentación		
Puntos de acceso inalámbrico		
Servidor de red inalámbrica		
Tarjetas y dispositivos inalámbricos		
Tarjeta inalámbrica para PC		
Dispositivo USB inalámbrico		
Antena direccional para tarjeta inalámbrica		
Otro dispositivo		
II. Asegurar de inmediato todos los dispositivos electrónicos		
Materiales:		
Cámaras (foto y video)		
Cajas de cartón		
Guantes		
Cinta de evidencia		
Bolsas de papel para evidencia		

Stickers para etiquetar evidencia
Cinta de la escena del crimen
Bolsas antiestáticas
Marcadores permanentes
Herramientas no magnéticas
III. Directivas para asegurar la evidencia en la escena
Actividades del Investigador:
Asegurar que las personas no autorizadas no tengan acceso a ningún dispositivo en la escena
Únicamente solicitar asistencia a personas autorizadas y asignadas por la empresa que solicita los servicios del perito informático.
Retirar a todas las personas del área donde se recolectarán las pruebas de evidencia digital.
Asegurarse de que la condición de cualquier dispositivo electrónico no se altere.
Deje el ordenador o dispositivo apagado en el caso que esté en dicho estado.

Fuente: Autor

Asimismo, una vez que se ha revisado las actividades de la fase de asegurar y evaluar la escena, se requiere cumplir con el registro de la información que implica el aseguramiento y evaluación de la escena.

Tabla 18. Actuación del perito fase 2 asegurar y evaluar la escena

Nombre del caso	**No. Caso**	**Fecha**	**Hora**
_____	_____	_____	_____
I. Información de Ordenadores			
Ordenador 1:			
Marca: _____	Modelo: _____		
Número de Serie: _____			
Tipo de computador:			
Desktop: _____			
Laptop: _____			
Tabla 11. (cont.)			
Otra: _____			
Condición:	Buena _____	Mala	_____
Ordenador 2:			
Marca: _____	Modelo: _____		
Número de Serie: _____			
Tipo de computador:			
Desktop: _____			
Laptop: _____			
Otra: _____			
Condición:	Buena _____	Mala	_____
Número de Discos Duros: _____			
Lector Multitarjeta: _____	Tarjeta de Video:	_____	
Módem: _____	Memoria Ram:	_____	

Tarjeta de Red: _____	DVDRW:	_____
Puertos USB: _____	Puertos HDMI:	_____
II. Otros Dispositivos (Discos Externos, USB, Periféricos)		
Serie / Modelo	Donde fue encontrado:	
_____	_____	
III. Información de Material para asegurar la evidencia		
Materiales	**Descripción de su utilización**	
Cámara de fotos / video		
Bolsas antiestáticas		
Guantes		
Cinta de Evidencia		
Stickers para etiquetar la evidencia		
Marcadores permanentes		
Otros Elementos		
IV Información del Investigador		
Nombres y Apellidos del Perito:	_____	
Profesión:	_____	
No. Identificación Pericial:	_____	
Dirección de Contacto:	_____	
Teléfono (s):	_____	
Correo electrónico:	_____	

Fuente: Autor

Fase 3: Identificación de Evidencia

En esta fase se realizan las siguientes acciones una vez que se recibe la solicitud de análisis forense, en Ecuador se designa a un perito según lo indica el Art. 12 del Reglamento 040-2014 del Sistema Pericial del Consejo de la Judicatura ecuatoriano que indica:

Art. 12.- Designación. - Para la designación de peritos en los distintos procesos judiciales o pre procesales de la Función Judicial, se respetarán los principios de profesionalidad, especialidad, transparencia, alternabilidad, e igualdad (Consejo de la Judicatura, 2016).

En la identificación de evidencia se ejecutan las siguientes acciones mediante la aplicación de métodos que permitan que dicho procedimiento sea auditable, reproducible y defendible.

El proceso incluye la indagación, detección y documentación de evidencia digital, deben identificarse todos los dispositivos que puedan contener dicha evidencia. El DEFR (Especialista en evidencia digital de Primera Intervención) debe efectuar la exploración metódica de la escena del crimen para evitar pasar por alto dispositivos o material camuflado que parece irrelevante a primera vista.

Se describen las actividades a considerar durante esta fase, se debe garantizar la integridad de la cadena de custodia de la evidencia, como se indica a continuación.

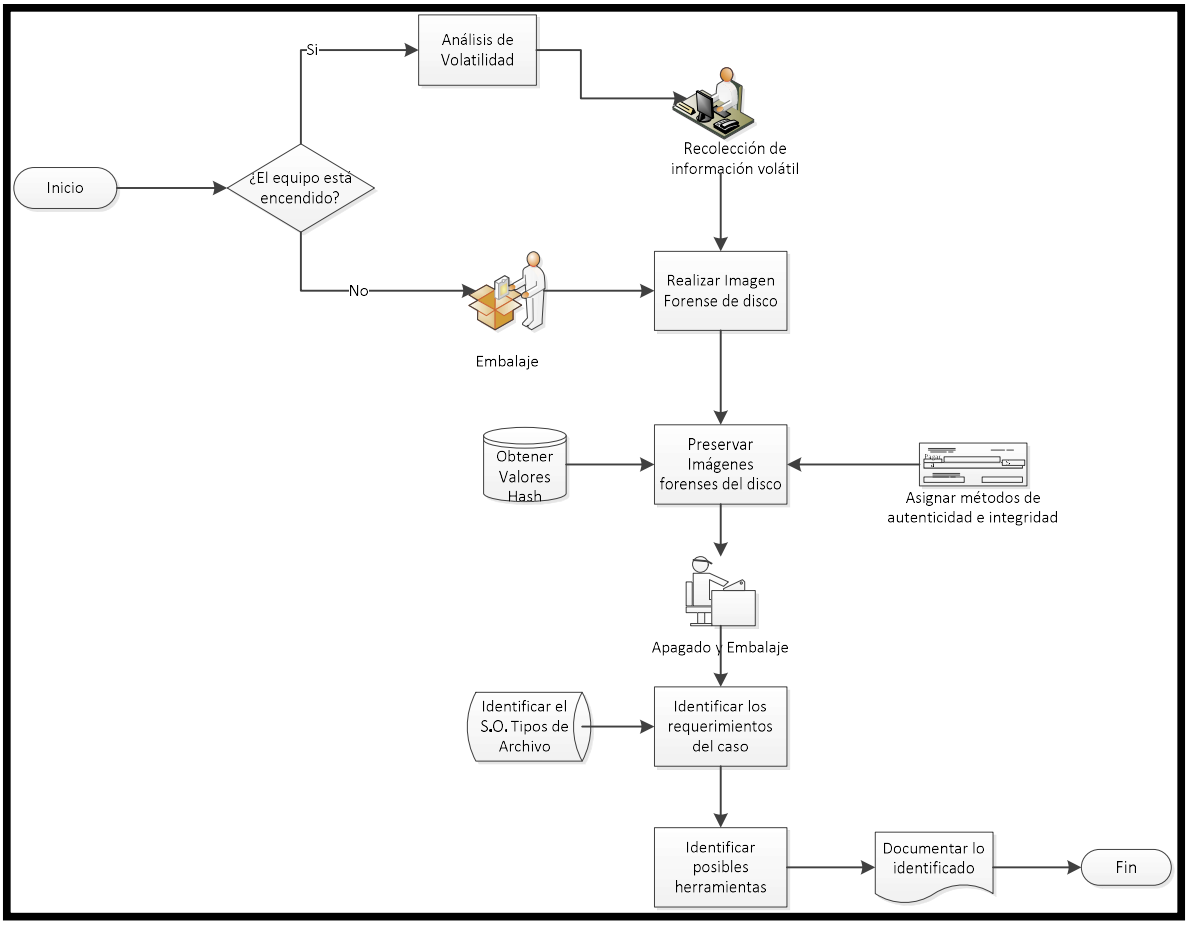


Figura 6. Flujo de actividades de la fase 3 Identificación de la evidencia

Fuente: Autor

Verificar el estado del ordenador

Se revisa si el equipo está encendido, en caso que esté encendido se considera la volatilidad de la evidencia con el fin de evitar perdida de información valiosa cuando éste se apague y capturar la misma. Se recomienda esta tarea a un técnico forense.

Si la pantalla está encendida, se captura los procesos que se estén ejecutando de acuerdo a la ISO 27037. Además de inmediato se debe proceder con el siguiente paso para evitar disipar la mayor cantidad de información.

En el caso que el equipo esté apagado, no se necesita un análisis de volatilidad, sino que se recomienda retirar el dispositivo de almacenamiento del ordenador y se realiza el respectivo embalaje de acuerdo con la norma ISO/IEC 27037 (2012), luego de esto se puede continuar con la realización de la imagen del disco.

Realizar el análisis de volatilidad

El investigador forense digital debe establecer prioridades en la evidencia; ya que puede ser de valiosa importancia en una investigación, dicha acción disminuye la posibilidad de perder evidencia. Según la RFC 3227, el orden de volatilidad que se debe tomar en cuenta es:

- Registros de la memoria caché del dispositivo.
- Tabla de enrutamiento de red, caché ARP, tabla de procesos, estadísticas del kernel y memoria.
- Información temporal del sistema.
- Datos almacenados en disco.
- Log del sistema.
- Configuración física y topología de la red.
- Documentación. (Rivas, 2014, pp. 25)

Inmediatamente, después de realizar la captura de datos sensibles según dicha escala de volatilidad, la norma ISO/IEC 27037 (2012), recomienda verificar si la

información que se mantiene en el computador se conservan de forma estable; si ese es el caso se procede a apagar el computador de manera normal; pero de no ser el caso y los datos almacenados estén en riesgo, por ejemplo se esté ejecutando un borrado de archivos, se debe retirar la fuente de energía del mismo.

Realizar Imágenes Forenses

Se recomienda efectuar copias bit a bit de la evidencia digital que contienen los dispositivos, en nuestro caso los discos duros, con el fin de asegurar la integridad de la evidencia digital original. Dichas imágenes forenses sirven a los peritos para incautar evidencia o para realizar análisis sin alterar la evidencia original.

Se debe extraer los valores hash de las imágenes forenses como una actividad que permite comparar su integridad en todo momento, para lo cual es recomendable utilizar una herramienta validada para este proceso en referencia con la ISO/IEC 27037.

Preservar Imágenes Forenses

Se recomienda al momento de almacenar las imágenes forenses garantizar que únicamente los individuos que tengan esa competencia deben tener acceso a la misma, por consiguiente, se recomienda usar técnicas de autenticación, integridad como son firma digital, valores del archivo criptográfico hash, claves primarias.

Identificación de los requerimientos del caso

Implica conocer el tipo de caso que se va a indagar; se trata de considerar que evidencia disponible en este caso dispositivos de almacenamiento entre los cuales están los discos duros, el sistema operativo que se utilizó para cometer el ilícito, tipo de archivos (FAT, NTFS, ext2, ext3, ext, HFS, etc.), de ser posible el tipo de trabajo que realiza el personal, y posibles motivaciones del sospechoso.

La información indicada ayuda a facilitar el trabajo para posteriormente elegir las herramientas apropiadas para la investigación.

Identificación de las posibles herramientas

De acuerdo a la información investigada, es viable identificar las herramientas que pueden ser utilizadas para el proceso de recolección, adquisición y preservación de la evidencia digital. Las mismas deben ser compatibles al medio de almacenamiento y demás requerimientos, en este caso al sistema de archivos, sistema operativo de la evidencia almacenada en el disco duro.

Identificación de software de borrado de archivos

Conforme lo recomienda la ISO 27037 (2012), se debe verificar si en el ordenador existe algún programa de borrado de archivos como Ccleaner; esto con el fin de tener presente las posibles acciones que pudo hacer el usuario.

La fase de Identificación implica finalmente obtener:

- Expediente de toda la información identificada en esta etapa.
- Imágenes forenses.
- Reporte de cadena de custodia.

Se indica a continuación además un CheckList que indica las acciones que realiza la etapa de Identificación:

Tabla 19. Lista de comprobación - Checklist fase 3 Identificación evidencia

Actividades de la Fase 3 Identificación Evidencia	**Chequeo:**	**SI**	**NO**
I. Verificar el estado del ordenador			
Actividades del Investigador:			
Verificar que el ordenador está encendido			
II. Realizar el análisis de volatilidad			
Actividades del Investigador:			
Define el orden de volatilidad en caso de estar encendido			
Captura de información volátil en caso de estar encendido			

En caso que el ordenador no esté encendido:
Procede a empaquetar e incautar el equipo de manera de no alterar la evidencia
III. Realizar imágenes forenses
Actividades del Investigador:
Realizar copias genuinas del estado en el que el disco fue encontrado
IV. Preservar Imágenes forenses
Actividades del Investigador:
Utiliza técnicas de autenticación
Define técnicas de integridad
Aplica dichos métodos a las imágenes obtenidas
V. Identificación de los requerimientos del caso
Los dispositivos donde se guarda la evidencia potencial
Identifica el sistema operativo, tipo de archivos, competencias del personal
VI. Identificación de las posibles herramientas
Posibles herramientas que aporten a la investigación
Elegir la herramienta de software más apropiada de acuerdo a la información investigada
VII. Verificación de existencia de software de borrado
Si el sistema tiene instalado un programa que elimine archivos del sistema
En el caso que tenga, se toma precauciones de ese hecho para la investigación

Fuente: El autor

Asimismo, una vez que se ha revisado las actividades de la fase de asegurar y evaluar la escena, se requiere cumplir con el registro de la información que implica el aseguramiento y evaluación de la escena.

Tabla 20. Actuación del perito fase 3 Identificación de Evidencia

Nombre del caso	**No. Caso**	**Fecha**	**Hora**
_____	_____	_____	_____
I. Métodos de preservación de evidencia			
Identificación unívoca de potencial evidencia	Tipo de Dispositivo	Método de preservación (claves de acceso, checksum, valores hash, firma digital)	
_____	_____	_____	
II. Respaldo de la evidencia			
Nombre de la evidencia	Núm. De copias	Embalaje y sellado de evidencia bajo condiciones adecuadas (SI/NO)	
_____	_____	_____	
Nombre evidencia (00001): _____			
Nombre y Firma del Responsable del manejo de evidencia digital	**Fecha de acceso a la evidencia**	**Lugar donde accedió**	**Realizó algún cambio (Si/No)**
_____	_____	_____	_____

Nombre evidencia (0000n):

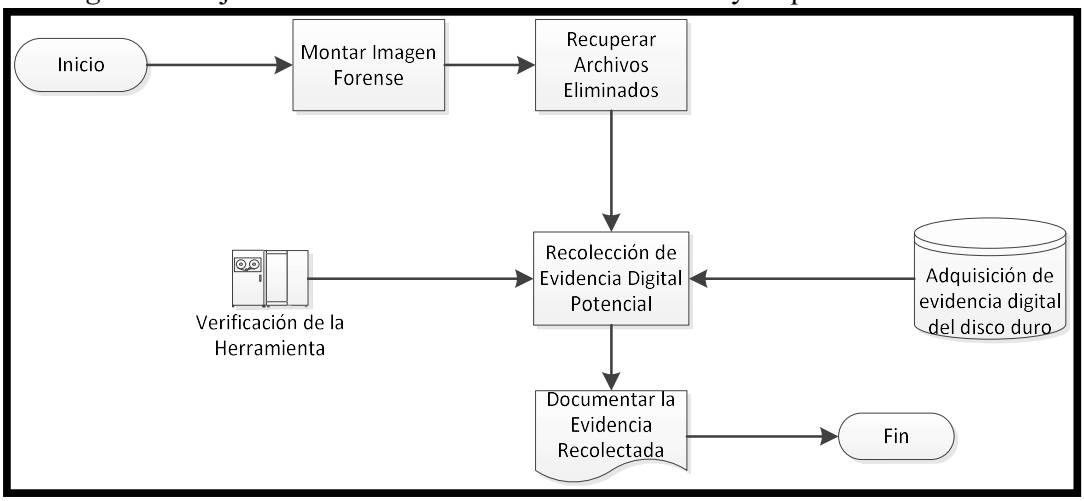
Nombre y Firma del Responsable del manejo de evidencia digital	Fecha de acceso a la evidencia	Lugar donde accedió	Realizó algún cambio (Si/No)
_____	_____	_____	_____

Fuente: Autor

Fase 4: Recolección y Adquisición de Evidencia

La entrada de esta fase son las imágenes forenses establecidas en la identificación de indicios iníciales indicadas en la etapa anterior. Las actividades se describen a continuación considerando la integridad de las pruebas.

Figura 7. Flujo de actividades de la fase 4 Recolección y adquisición de evidencia



Fuente: Autor

Montar la Imagen Forense

Esta actividad se realiza con el objeto de verificar el estado en que el equipo o dispositivo fue encontrado, se sugiere previamente antes de montar la imagen forense revisar si las sumas de verificación son correctas, es decir las mismas deben coincidir para tener la certeza que la evidencia es íntegra; adicionalmente según lo recomendado si es necesario se debe obtener un espacio asignado y no asignado (archivos eliminados).

Dependiendo del resultado del proceso, si se produce cambios inevitables en la copia creada comparada con la original, es necesario se documente qué datos se modificaron. En los casos en que el proceso de verificación no se puede llevar a cabo el DEFR debe utilizar el mejor modo posible y luego poder habilitar, justificar y reivindicar su elección de métodos. En el caso de que la copia digital creada no se puede verificar, esto debe documentarse y justificarse. Si la fuente de evidencia digital es demasiado grande para ser manejada, el DEFR puede adquirir solo la parte relevante como archivos seleccionados, carpetas o rutas (Veber & Smutny, 2015, p.295).

Recuperar archivos eliminados

Previamente a la recolección de la información que se encuentra en el disco duro, se pretende una recuperación de archivos eliminados del dispositivo y además se identifica posible evidencia potencial dentro de los mismos.

Recolección de evidencia digital potencial

Según la norma ISO/IEC 27037, se recomienda entre otros aspectos identificar las carpetas, archivos o cualquier información relevante con el fin de adquirir los datos deseados, incluso se recomienda emplear técnicas de minería de datos.

La fase de recolección implica finalmente obtener:

- Expediente de la evidencia recolectada, su procedencia y tipo.
- Evidencia digital.

Tabla 21. Lista de comprobación - Checklist fase 4 Recolección de evidencia

Actividades de la Fase 4 Recolección de Evidencia Digital	**Chequeo: SI**	**NO**
I. Autorizaciones para realizar la pericia sobre un equipo		
Actividades del Investigador:		
Autorización y otros para realizar prácticas en el ordenador y/o dispositivo		
Obtiene la Imagen Forense para ser montada		
II. Montar Imagen Forense		
Actividades del Investigador:		

Verifica las sumas de verificación Hash [Computed Hashes]
Seleccionar el método más apropiado para adquirir los datos
III. Recuperar archivos eliminados
Actividades del Investigador:
Elegir el método adecuado de recuperación de archivos del disco
Se guarda la información recuperada para buscar evidencia
IV. Recolección de potencial evidencia digital
Expediente de la evidencia recolectada, su procedencia y tipo
Adquisición de potencial Evidencia digital

Fuente: El autor

Se muestra también una hoja de trabajo, de la información de la fase de recolección de evidencia digital.

Tabla 22. Actuación del perito fase Recolección de evidencia digital

Nombre del caso	**No. Caso**	**Fecha**	**Hora**
_____	_____	_____	_____
I. Documentación y autorización de pericia sobre un equipo			
Documento		**Descripción**	
1. Solicitud de la parte interesada	_____	Solicita a un Juez o un fiscal de la función judicial la designación de un perito	_____
2. Designación de Perito	_____	Según la Resolución 040-2014 a través del SATJE	_____
3. Aceptación de la Pericia	_____	El perito es notificado por medio del correo electrónico	_____
4. Providencia del Proceso Judicial	_____	Especificaciones del caso judicial, fecha y hora en la que el perito deberá posesionar el caso	_____
5. El perito debe solicitar autorización para acceder al equipo a investigar	_____	El perito solicita autorización para poner en práctica su experticia, romper claves, sacar imágenes forenses, investigar archivos.	
II. Verificación de la imagen forense obtenida en la identificación			
Software utilizado			
Método Utilizado		_____	
Hash MD5		_____	
SHA1		_____	
Sistema Operativo usado / versión		_____	
Mantiene Integridad SI / NO		_____	
III. Información de Imagen forense recuperación de archivos eliminados			
Nombre de archivo recuperado	**Tipo archivo**	**Fecha de última modificación**	
_____	_____	_____	

IV. Información de Recolección de potencial evidencia digital			
Nombre de archivo	**Fecha de Creación**	**Fecha de Modificación**	**Integridad evidencia SI/NO**

V. Información del Investigador	
Nombres y apellidos del perito	
Profesión	
No. Identificación Pericial	
Dirección de contacto	
Teléfono(s)	
Correo Electrónico	
Firma	
Nombre del Investigador que realiza el relevo	
Profesión investigador relevo	
No. Identificación Pericial relevo	
Dirección de Contacto relevo	
Teléfono(s) relevo	
Correo electrónico relevo	
Firma relevo	

Fuente: El autor

Fase 5: Preservación y Conservación de la Evidencia

La fase de preservación y conservación inicia con la evidencia recolectada, la misma que debe ser adecuadamente preservada, en caso de no contar con ninguna limitación, los métodos de preservación son especificados y utilizados por el investigador forense. Se indican a continuación las actividades de la presente fase.

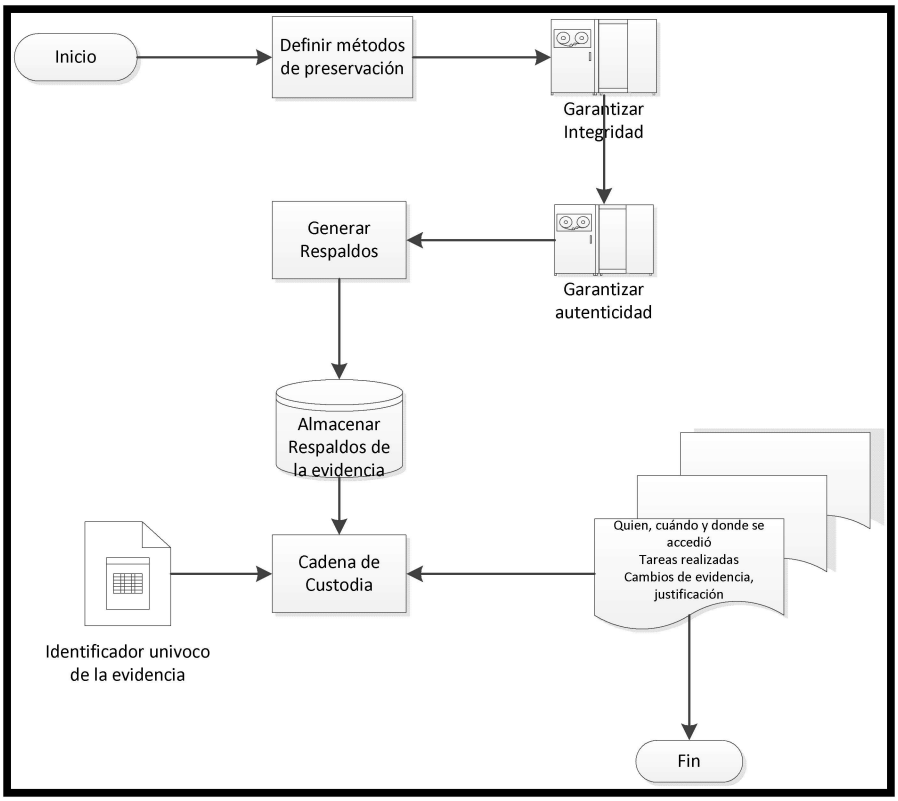


Figura 8. Flujo de actividades de la fase 5 Preservación y conservación de evidencia

Fuente: Autor

Definir métodos de preservación

Es necesario que se definan métodos para garantizar la integridad y autenticidad sobre la evidencia recolectada. Se debe establecer que solo el personal acreditado posea acceso a la evidencia digital, asimismo, que la misma se conserve íntegra en toda la investigación, para esto se puede contar con claves de acceso, checksum, valores hash, firmas digitales, entre otros.

La función de verificación se utiliza para que las copias de la evidencia sean proporcionales a la original. Se debe tomar en cuenta también enlazar la evidencia con el investigador forense usando métodos biométricos, formas digitales, fotografía en concordancia con la ISO/IEC 27037 (2012).

Generar respaldos

Una vez recolectada la potencial evidencia, se procede a respaldar y preservar con métodos del modo menos intrusivo posible, con el fin de conservar la originalidad de la prueba y obtener copias de respaldo. Dicho respaldo debe conservar una identificación del dispositivo de almacenamiento.

Seguimiento de la cadena de custodia

Para las actividades asociadas a la identificación, recopilación, obtención y conservación de la evidencia digital se debe tener en cuenta la Cadena de Custodia que establece:

- Un identificador univoco de la evidencia.
- Quién, cuándo y dónde se accede a la evidencia.
- El pasaje de la evidencia de un sitio a otro y tareas realizadas.
- Todo cambio potencial en la evidencia digital debe registrarse con el nombre del responsable y la justificación de las acciones realizadas (Roatta et al., 2017, p.4).

Una vez realizadas las actividades detalladas de esta etapa, se deriva lo siguiente: La evidencia digital apropiadamente preservada y la documentación de esta etapa con los métodos empleados para dicha preservación y las herramientas utilizadas.

Tabla 23. Lista de comprobación - Checklist fase 5 Preservación de la evidencia

Actividades de la Fase 5. Preservación de Evidencia	**Chequeo:**	**SI**	**NO**
I. Definir métodos de preservación de evidencia			
Actividades del Investigador:			
Define métodos de preservación			
II. Generar respaldos de la evidencia			
Actividades del Investigador:			
Realización de copias de respaldo			
Almacenamiento de respaldos, embalaje y sellamiento de evidencia en función del tipo de evidencia, utilización de bolsas antiestéticas, contenedores, etc.			
III. Seguimiento de la cadena de custodia			

Actividades del Investigador:
Se documenta la evidencia con identificadores unívocos
Se documenta quién, cuándo y dónde se accede a la evidencia
Se documenta si se trasladó la evidencia
Se documenta todo cambio de la evidencia con el nombre del Responsable

Fuente: Autor

Se muestra la hoja de trabajo de la cadena de custodia de la etapa de preservación de la evidencia y de la conservación de la misma.

Tabla 24.Actuación del perito fase 5 Preservación de evidencia

Nombre del caso	**No. Caso**	**Fecha**	**Hora**
I. Métodos de preservación de evidencia			
Identificación unívoca de potencial evidencia	**Tipo de Dispositivo**		Método de preservación(claves de acceso, checksum, valores hash, firma digital)
II. Respaldos de la evidencia			
Nombre de la evidencia	Núm. Copias	Embalaje y sellado de evidencia bajo condiciones adecuadas (Si / No)	
III. Seguimiento de la cadena de custodia			
Nombre evidencia (001)			
Nombre y firma del responsable del manejo de evidencia digital	**Fecha de acceso a la evidencia**	**Lugar donde accedió**	**Realizó algún cambio (Si / No)**
Nombre evidencia (n)			
Nombre y firma del responsable del manejo de evidencia digital	**Fecha de acceso a la evidencia**	**Lugar donde accedió**	**Realizó algún cambio (Si / No)**

Fuente: El autor

Fase 6: Análisis de la Evidencia

La fase de análisis se toma en base a aspectos relevantes de la Metodología Española, la misma que está basada en normas como la ISO 27037, el RFC 3227 y las normas españolas UNE 71505 y UNE 71506.

La fase en mención es muy importante en la metodología, debido a que se determina qué o quién causó el incidente, así como también como lo hizo o que afectación ha tenido en el sistema, en esta fase apegada a la Norma UNE que manifiesta entre otros principios, que una persona es responsable de todas las operaciones llevadas a cabo con relación a la evidencia electrónica mientras se encuentra en su posesión. Además, se debe indicar que en la ISO 27037 sería equivalente al rol del investigador DES (Experto en Evidencia Digital).

Cabe señalar, que la fase de Análisis e Interpretación de la Evidencia digital queda fuera del alcance la Norma ISO/IEC 27037; la fase en mención es tratada específicamente en la Norma ISO/IEC 27042, por consiguiente, la fase indicada se trata como un aspecto adicional relevante del trabajo de investigación, en el que se utiliza métodos para obtener resultados confiables para resolver los incidentes que se presentan en los casos de delitos informáticos.

Tabla 25. Lista de comprobación - Checklist fase 6 Análisis de la evidencia

Actividades de la Fase 6. Análisis de la Evidencia	**Chequeo:**	**SI**	**NO**
I. Disponer un escenario de trabajo apropiado a las necesidades del acontecimiento			
Actividades del Investigador:			
Trabaja con las copias de las imágenes forenses obtenidas en las anteriores fases			
II. Identificar el autor o autores de los hechos investigados			
Actividades del Investigador:			
Analiza exhaustivamente la información de la potencial evidencia recolectada y preservada en las anteriores fases.			
Analiza exhaustivamente las distintas motivaciones del presunto ciberdelincuente para el cometimiento del delito.			
III. Documentar la información relevante encontrada en relación al caso investigado			
Actividades del Investigador:			
Registra la información relevante encontrada que servirá posteriormente para demostrar el cometimiento de un delito informático tipificado en la ley.			
Preserva la cadena de custodia durante todo el proceso de la investigación.			

Fuente: Autor

Las actividades del investigador indicadas permiten que la potencial evidencia digital sea admisible cuando es presentada ante un tribunal, en consideración que dicha

evidencia cumple con los principios fundamentales de relevancia, confiabilidad y suficiencia.

3.2 APLICACIÓN DE LA METODOLOGÍA

El objeto de este capítulo es detallar la aplicación de la metodología propuesta, de acuerdo con la información de la Norma ISO/IEC 27037 indicada en la presente investigación. Esto con el fin de validar la metodología planteada, en una escena real, la cual se podría aplicar en un laboratorio de informática forense proporcionando orientación a las personas responsables de identificación, recopilación, adquisición y preservación de evidencia digital.

ESCENARIO PROPUESTO Y ACTIVIDADES REALIZADAS

El escenario puede tener diversas formas de planteamiento puesto que va a depender del caso en que se desarrolla el incidente o circunstancia donde se ha cometido un delito informático, en este caso supuesto se requiere recuperar información de varios discos duros que se encontraron en la escena del delito en una oficina en la que se recolectaban documentos para después ser falsificados.

El caso en mención implica los procesos que son de competencia de la Norma ISO/IEC 27037:2012, en los cuales la recolección de la evidencia digital es un procedimiento fundamental para la investigación forense. A continuación, se indican los discos recolectados en la escena los cuales han sido incautados.

Figura 9. Escenario propuesto discos incautados

Fuente: autor

En el presente caso se indican además el escenario que contempla los discos incautados, materiales para extracción de evidencia digital de dispositivos en este caso discos duros de diferentes tipos, una computadora en donde se extraerá las imágenes forenses de los dispositivos y se realizará el análisis correspondiente de la información extraída.

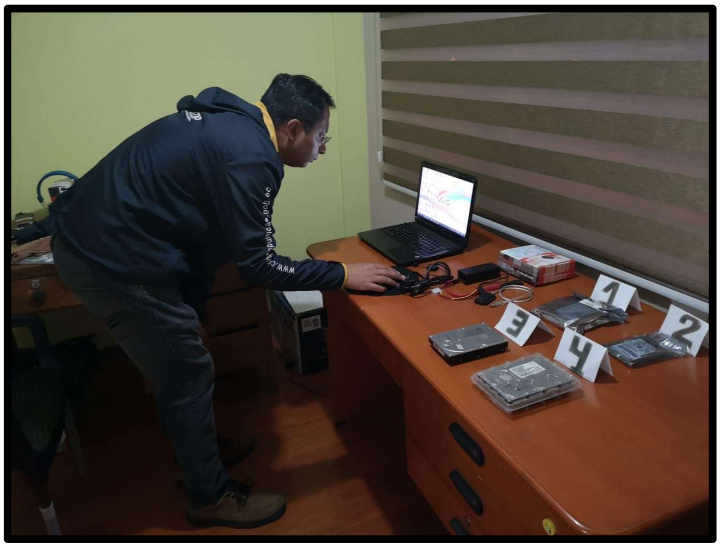


Figura 10. Escena propuesta materiales discos kit de extracción de evidencia

Fuente: Autor

Ubicación de la escena

En esta etapa, se describe el lugar de los hechos, en el que se ha considerado detallar la información de la localización de la escena, aspectos como dirección física, tiempos en los que se accede a la escena, entre otros parámetros.

Se ha realizado un CheckList de acciones que se deben realizar para que la ubicación del lugar de los hechos sea clara y las acciones de fijación necesarias, además se ilustra una hoja de trabajo con base a la Cadena de Custodia de Colombia acoplada al diseño de la metodología indicada en la presente investigación.

Localización de la escena

Esta etapa tiene como objetivo registrar de modo general dónde se encuentra el lugar de los hechos y conocer la situación del mismo.

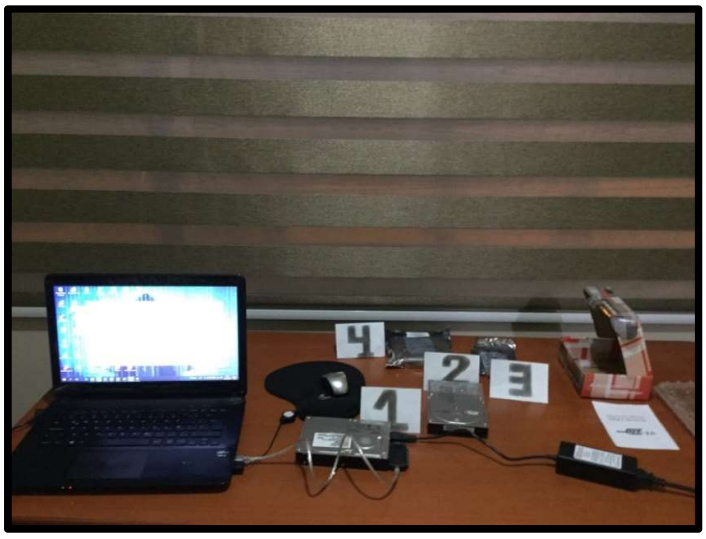


Figura 11. Localización del lugar de los hechos

Fuente: Autor

Institución donde se desarrollan los hechos

Es importante tener en cuenta si la pericia va a ser desarrollada en una empresa o a nivel particular, puesto que se investigan de manera diferente según el caso, sin embargo, por lo general lo requieren empresas.

Fijación fotográfica

Se refiere a métodos que sirven para dilucidar y comunicar de manera ilustrativa a través de imágenes el escenario y lugar de los hechos, esto se realiza de forma metodológica, de lo general a lo particular.

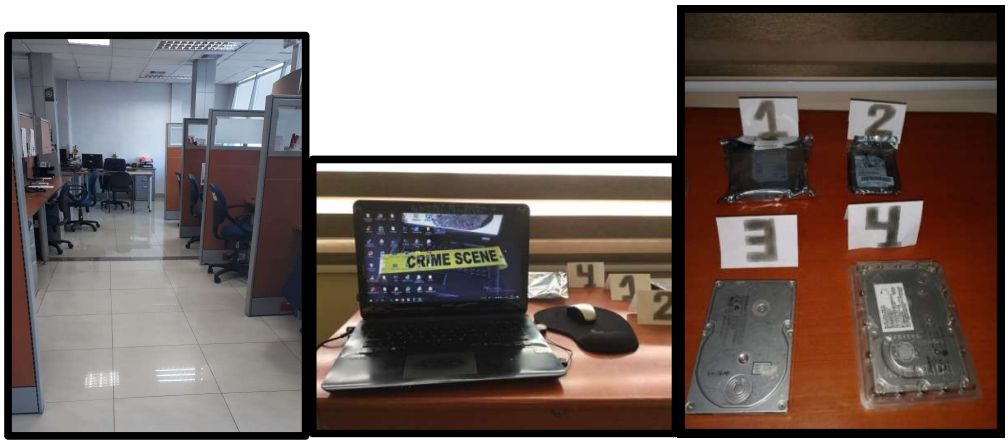


Figura 12. Fijación fotográfica del lugar de los hechos

Fuente: Autor

Fijación vídeo gráfica

La fijación Video gráfica se utiliza cuando los hechos sean graves, para complementar la fijación fotográfica, incluyendo video y audio de la escena en la que se ha cometido un delito informático de gran magnitud, donde se requieren detalles específicos que pueden influir en la investigación.

En esta etapa se registran la información del lugar de los hechos, se especifica de manera precisa además las fechas y demás información considerada en el Checklist y en la actuación pericial indicados en el apartado anterior en el diseño de la metodología fase 1.

Asegurar y evaluar la escena

El experto asegurará y obtendrá toda la información necesaria para ser posteriormente evaluada, se recaba dicha información para diseñar la estrategia de actuación para la obtención de la potencial evidencia digital, se planifica además la intervención, detallando las posibles fuentes de las que deriven esos hechos (Puig, 2014).

Para asegurar la escena, los investigadores de primera intervención a más de registrar la localización de la escena y fotografiar la misma, previamente deben separar e identificar los dispositivos y los posibles involucrados en el lugar de los hechos, además se debe obtener la mayor información posible de las personas indicadas, lo mismo que incluye:

Identificación de la evidencia digital

Entrada: En este caso la entrada son los equipos de los cuales se incautan los discos duros que son objeto de la investigación.

Se empieza identificando la evidencia potencial con un código único, en nuestro caso los discos duros provenientes de uno o varios ordenadores que se hayan incautado.

Identificador del ordenador: *PC001*.

Además, se registra la hora y fecha en que se incautan los equipos, en caso que estén encendidos los equipos se captura la hora y fecha del sistema para comparar con la actual.

Número de serie de evidencias:

S/N: *ZC60QAW1*

S/N: *121204J510007DHYJJEP*

S/N: *MX4K060H3*

Figura 13. Series de discos duros incautados

Fuente: autor

Confiscada la evidencia potencial, se procede con las acciones indicadas en la fase de Identificación de la metodología propuesta la misma que consta de las siguientes actividades:

Verificar el estado del ordenador

Se puede verificar a continuación que el ordenador con identificación PC001, se encuentra encendido, por tanto, se procede con el análisis de volatilidad.

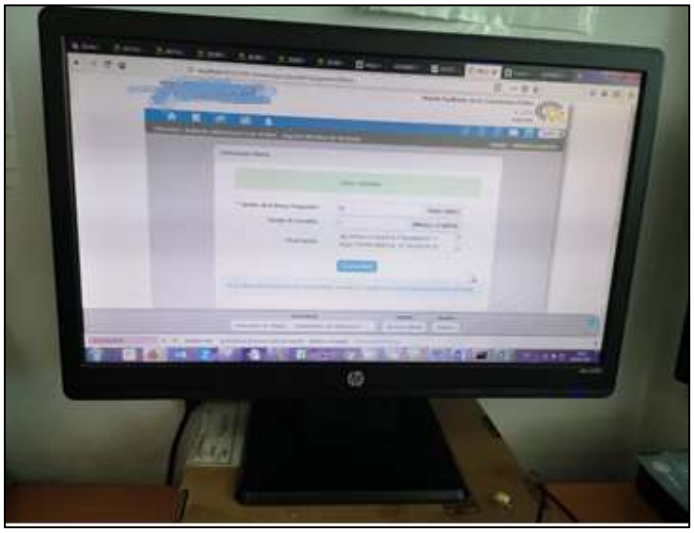


Figura 14. Estado del ordenador codificada PC001

Fuente: Autor

Análisis de volatilidad de la evidencia

Se procede conforme a las pautas indicadas en el apartado anterior, es decir se recolecta la información de acuerdo al siguiente orden establecido: Memoria Física, Archivos Temporales y disco.

Se elige la herramienta OSForensics con el fin de recolectar la información de memoria ram, se procede además a generar el hash correspondiente para garantizar su integridad. La captura de memoria se almacena con un identificador en este caso: "memoriatest.mem".

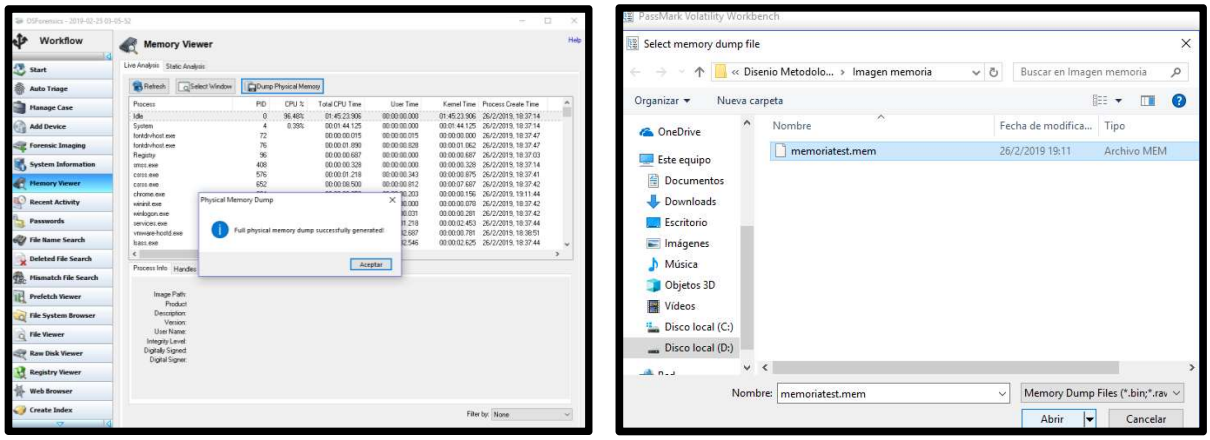


Figura 15. Generación de captura de memoria en OSForensics (memoriatest.mem)

Fuente: Autor

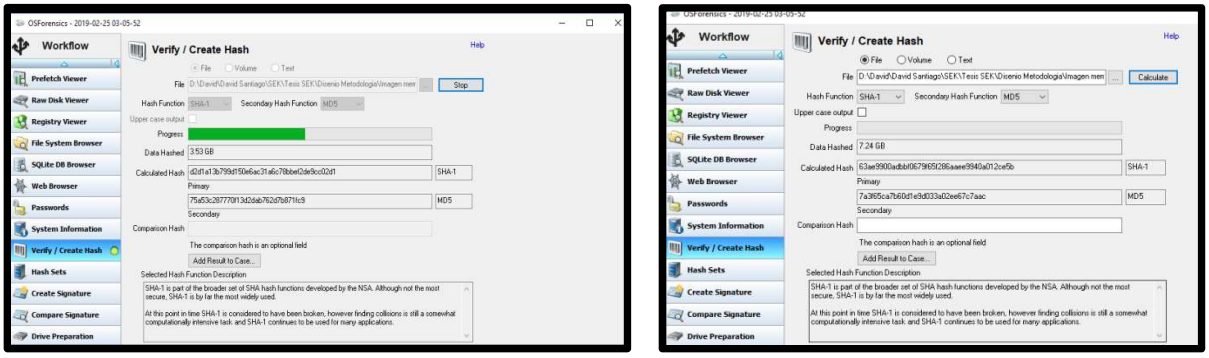


Figura 16. Generación de hash de memoria capturada

Fuente: Autor

Realizar Imágenes Forenses

Para realizar las imágenes forenses se utilizó el software FTK Imager, la imagen realizada del disco del ordenador PC001 se obtuvo el hash correspondiente para mantener la integridad de la prueba.

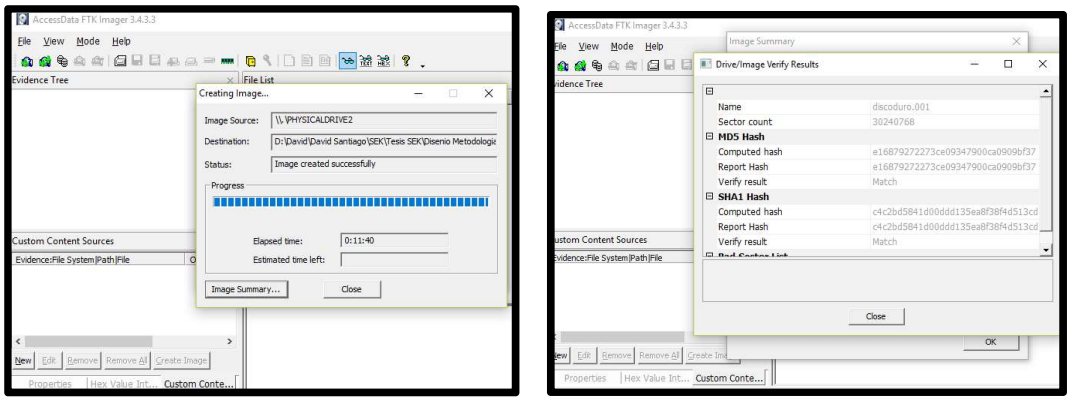


Figura 17. Valores hash de la imagen forense del ordenador PC001 (discoduro.001)

Fuente: Autor

Preservar Imágenes forenses

En los dos casos, tanto en la generación de la captura de memoria RAM como en la generación de la imagen forense del disco, se procede con la generación de los valores Hash correspondientes indicados en las ilustraciones 12 y 13 respectivamente con el fin de preservar la evidencia; además se realizan respaldos de la evidencia.

Identificar los requerimientos del caso

En los discos duros, una vez que se ha obtenido la imagen forense, se puede encontrar evidencia digital potencial, la cual se clasifica en:

- Información generada por aplicaciones de software.
- Archivos electrónicos generados por personas, almacenados en los discos duros.
- Archivos electrónicos remitidos como adjuntos en correos electrónicos.

- Elementos que hayan sido almacenados y eliminados posteriormente, los cuales pueden contener información del caso investigado(Guerron, 2018).

Identificar posibles herramientas

En la metodología propuesta, las herramientas utilizadas son FTK Imager, Autopsy, OSForensics, DiskDigger; dichas aplicaciones fueron elegidas por que son idóneas para el tipo de actividades que se realizan al identificar, recolectar y preservar la evidencia digital encontrada.

Verificar existencia de software de borrado

En el ordenador incautado, se analizó y no fue encontrado ningún programa computacional instalado para borrado de archivos.

Salidas: Imágenes forenses realizadas.

Recolección y Adquisición de la Evidencia

Entradas: Imágenes generadas del disco (discoduro.001), imagen de la memoria (memoriatest.mem).

Para la recolección de evidencia digital de discos duros se recomiendan las actividades que se detallan en la siguiente lista de comprobación Checklist:

Montar Imagen Forense

Se procede con la suma de verificación de la imagen forense, la misma que debe ser integra, el proceso que se realiza es comparar los valores hash del disco fuente es decir del disco original con el hash de la imagen forense generada es decir del disco clonado en OSForensics.

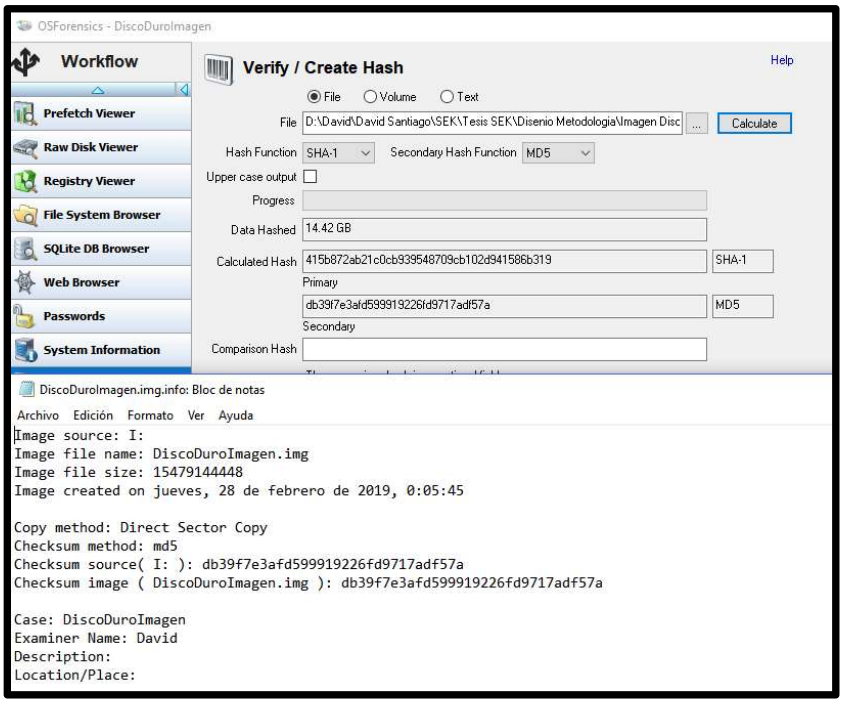


Figura 18. Comparación de valores hash de la imagen forense

Fuente: autor

Recuperar archivos eliminados

Mediante las herramientas *Recuba*, *DiskDigger*, *Autopsy* y *OsForensics* se procede a recuperar archivos eliminados en el disco de evidencia, en donde se puede verificar archivos eliminados, entre ellos fotografías de documentos como cédulas de ciudadanía, matrículas de vehículos y demás información que puede constituir evidencia potencial del caso investigado. Se muestra en las siguientes imágenes la forma en que se recupera los archivos eliminados de un disco.

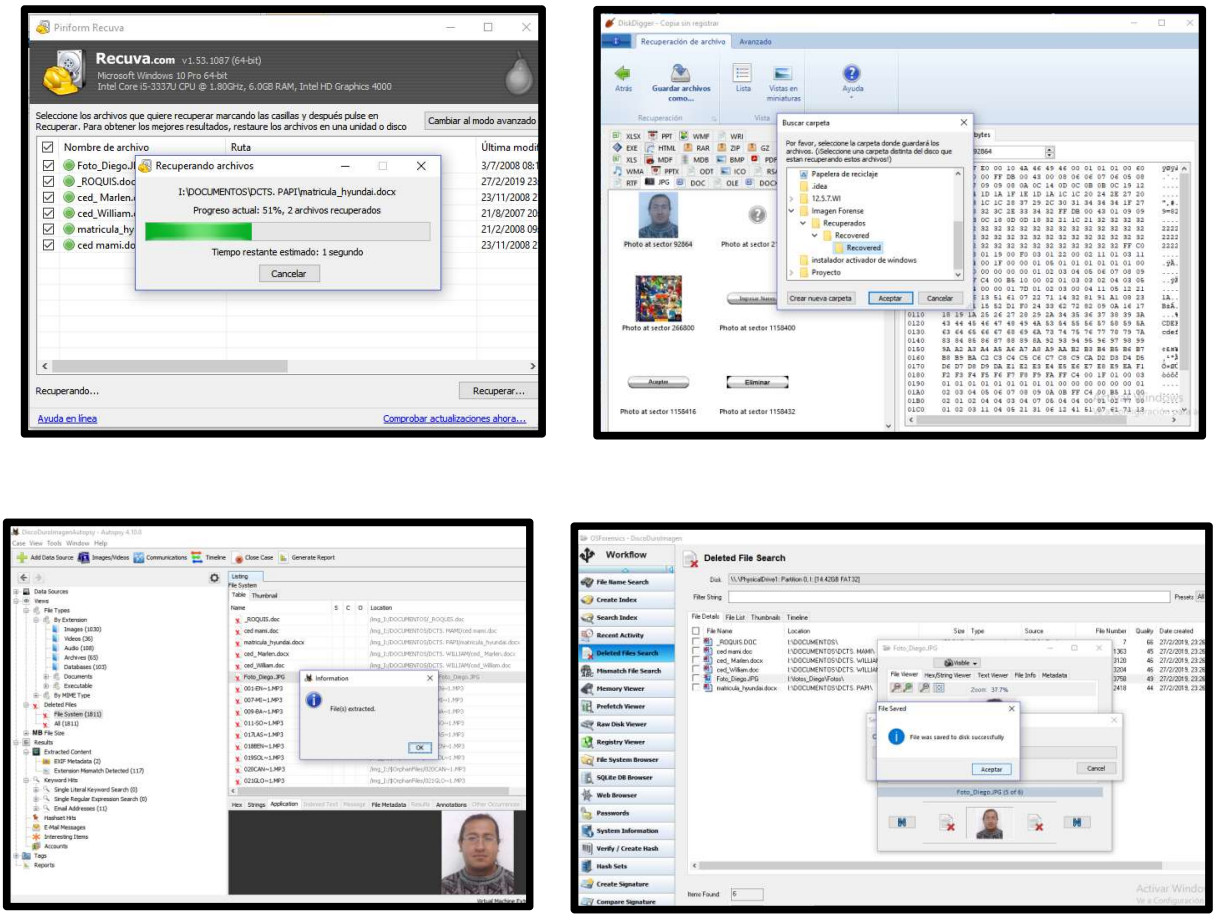


Figura 19. Recuperación de archivos eliminados del disco

Fuente: Autor

Recolección de potencial evidencia digital

La recolección de la potencial evidencia, se lo realiza en este caso con la herramienta OSForensics, la cual permite obtener del disco montado la información que se encuentre almacenada; se procede además a recolectar evidencia con la herramienta Autopsy, en las figuras siguientes se indican la información que se puede obtener como actividades recientes, archivos eliminados, rutas donde estuvieron guardadas las potenciales evidencias.

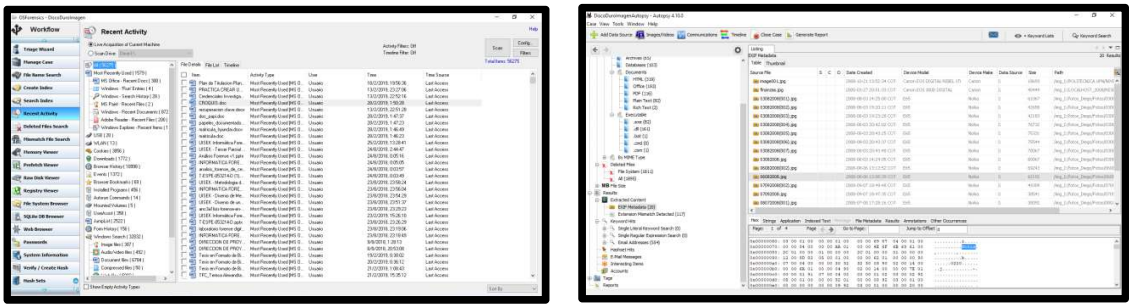


Figura 20. Recuperación de archivos eliminados del disco

Fuente: Autor

Se identifica la evidencia recolectada con el identificador: "*PotencialEvidencia001*". *Salida*: Evidencia recolectada: "*PotencialEvidencia001*".

Preservación y Conservación de la Evidencia

Entradas: Datos relevantes de recolección de potencial evidencia "*PotencialEvidencia001*" e imagen del disco duro con identificación: "*discoduro.001*".

En la fase de preservación y conservación se recomiendan las actividades indicadas en el apartado anterior relacionadas a esta fase de la informática forense de la metodología planteada.

Definir métodos de preservación de la evidencia

Una vez que se obtiene la potencial evidencia digital, los métodos de preservación de la evidencia utilizados son:

- Extraer valores hash de la potencial evidencia recolectada siguiendo el mismo procedimiento empleado para la imagen del disco.
- Asignación de firma digital; esta actividad se realiza en este caso con la herramienta OSForensics, como se indica en la siguiente ilustración.

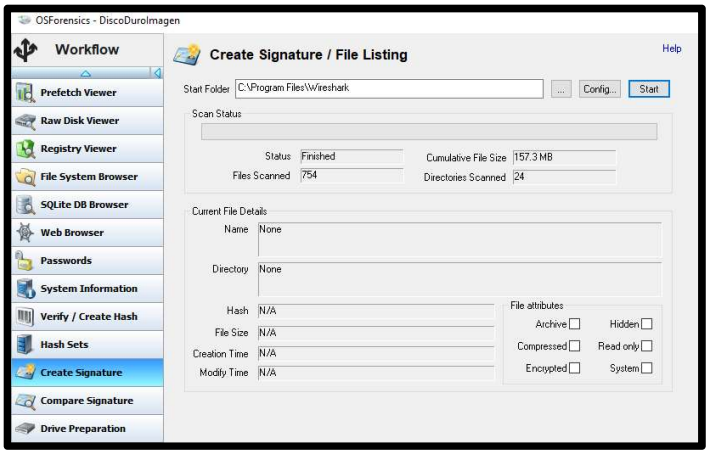


Figura 21. Creación de firma digital mediante OSForensics

Fuente: Autor

Generar respaldos de la evidencia

Se realizan los respaldos que sean necesarios, en lugares como discos duros externos, memorias USB, entre otros dispositivos; se identifica con un nombre unívoco a los respaldos en este caso con el nombre: "*RespaldoDExt001*" se registra además su respectivo hash y firma digital; dicho respaldo se almacena en un lugar determinado con las seguridades del caso.

Figura 22. Respaldo físico de potencial evidencia digital (RespaldoDExt001)

Fuente: Autor

Salidas: Evidencia identificada por "*PotencialEvidencia001*" y "*discoduro.001*"; juntamente con la información de métodos de preservación.

Se realiza un seguimiento de la cadena de custodia

El seguimiento de la cadena de custodia consiste en verificar que se hayan cumplido con los procedimientos respectivos para preservación de la potencial evidencia digital, en la metodología propuesta se debe verificar que la documentación de la evidencia tenga identificadores unívocos es decir con el mismo valor y equivalencia que no haya ambigüedad; se debe documentar también quién, cuándo y dónde se accede a la evidencia, eso indica que debe haber un registro que indique el nombre del investigador, la fecha y el lugar en el que se accede a la misma; documentar si se trasladó la evidencia y documentar finalmente cuando haya algún cambio en la evidencia con su respectivo nombre de responsable.

Análisis de la evidencia

La fase de Análisis de la Evidencia digital queda fuera del alcance la Norma ISO/IEC 27037:2012; no obstante, se toma de la Metodología Española, la misma que está basada a más de la ISO 27037, también en el RFC 3227 y las normas españolas UNE 71505 y UNE 71506.

La fase en mención es muy importante en la metodología debido a que se determina qué o quién causó el incidente, así como también como lo hizo o que afectación ha tenido en el sistema.

Una vez que se ha realizado todas las fases indicadas, la evidencia estará lista para ser analizada y posteriormente presentada en los tribunales. Como se indicó en el apartado anterior el análisis de la evidencia queda fuera del alcance de la norma ISO/IEC 27037, sin embargo, es importante indicar que, una vez manejada la evidencia de manera correcta, de eso dependerá que el análisis y su presentación sean exitosos.

3.3 CASO DE ESTUDIO DE INFORMÁTICA FORENSE JUICIO DE EXPERTO

Una vez que se diseñó la metodología, se propuso un caso de estudio real, que está desclasificado en la página del Consejo de la Judicatura, sin embargo por principios de

ética, se redacta de forma anónima los nombres de actores e involucrados, así como también el número de proceso.

DATOS GENERALES DEL JUICIO

Tabla 26. Proceso de indagación previa de un caso real de informática forense

Nombre Judicatura o Fiscalía	**SALA PENAL DE LA CORTE PROVINCIAL DE PICHINCHA**
Actor	VM
Demandados	Procuraduría, SC, Empresa T. Ec. DG., Gerente General
No. De Proceso	XX-2018-XXX99
Nombre y Apellido de la o el perito	RL.
Profesión y Especialidad Acreditada	Perito en Sistemas
No. De Calificación	18XXX92
Fecha de caducidad de la acreditación	XXX de Mayo del 2019
Dirección de Contacto	XXX y Av. 6 de Diciembre
Teléfono fijo de contacto	02 XXX 3XX8
Teléfono celular de contacto	09XXX2XX9
Correo electrónico de contacto	XXXX@gmail.com

Fuente: Autor

Quito, xxx de enero de 2019

ANTECEDENTES

La pericia informática se debe desarrollar in situ, en la Empresa de Telecomunicaciones, las cuentas de correo electrónico corporativo de los servidores públicos MR (Gerente de Canal Indirecto); GB (Jefe de Seguridad Industrial y Seguridad Ocupacional); PV (Trabajadora Social) y VV (Jefe de Nómina), a fin de que se verifique si existe algún mensaje de datos o correo electrónico enviado por el señor CR, identificado con cédula de ciudadanía No. *100XXXX000* (ex funcionario de la mentada Institución), a los mencionados funcionarios de la Empresa T en relación al estado de gravidez de la ex servidora MV, en el período comprendido desde el XX de noviembre del 2017 a XX de enero del 2018.

CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE.

La parte actora solicita realizar una pericia informática a las cuentas electrónicas intentando determinar la existencia y validez de un correo electrónico enviado a las cuentas electrónicas:

- mr.xxxx@xxx.gob.ec
- gb.xxxx@xxx.gob.ec
- pv@xxx.gob.ec
- vv@xxx.gob.ec

Y la desmaterialización del correo electrónico mencionado en el periodo de xx de noviembre del 2017 a xx de enero del 2018. Las cuentas que se deben revisar corresponden a:

1. MR. *(*Gerente de Canal Indirecto*) (*mr.xxxx@xxx.gob.ec*)*
2. GB. *(*Jefe de Seguridad Industrial y Seguridad Ocupacional*) (*gb.xxxx@xxx.gob.ec*)*
3. PV. *(*Trabajadora Social*) (*pv.xxxx@xxx.gob.ec*)*
4. VV. *(*Jefe de Nómina*) (*vv.xxxx@xxx.gob.ec*)*

La existencia del dominio usado para los emails:

1. *xxx.gob.ec*

Y la desmaterialización del correo electrónico:

Mail remitido por César R., identificado con cédula de ciudadanía No. *100XXXX000* (ex funcionario de la mentada Institución), a los mencionados funcionarios de la Empresa de Telecomunicaciones en relación al estado de gravidez de la ex servidora María V. Asisto en calidad de perito informático con todos los documentos habilitantes:

- Copia de la cedula de identidad.
- Certificado de calificación en el registro de peritos de la Función Judicial.

- Posesión de perito al Juicio No. *17XXXXX18XXX99*.

CONCLUSIONES DEL INFORME PERICIAL

Respecto al cumplimiento de lo solicitado por la autoridad se concluye lo siguiente:

a) La pericia fue realizada los días *XX* y *XX* de enero del 2019, en las oficinas de la empresa de Telecomunicaciones.

b) Se realizó la verificación de la cuenta de MR. (mr.xxxx@xxx.gob.ec), el cual se observó que está activa.

c) Se realizó la verificación de la cuenta de GB. (gb.xxxx@xxx.gob.ec), el cual se observó que está activa.

d) Se realizó la verificación de la cuenta de PV. (pv.xxxx@xxx.gob.ec), el cual se observó que está activa.

e) Se realizó la verificación de la cuenta de VV. (vv.xxxx@xxx.gob.ec), el cual se observó que está activa.

f) Se realizó la verificación del dominio xxx.gob.ec dominio el dominio se observó que está activa y funcional.

g) En la revisión del buzón de correo de PV. (Trabajadora Social) (pv.xxxx@xxx.gob.ec), Al momento de realizar la exploración del buzón de correo a través de los filtro de búsqueda por asunto; utilizando la palabra “embarazo”, se obtuvo como resultado la existencia de un mail con las siguientes características:

   De: “COM RA”
   Para: “FIN JA, COM RM, DEO BG, DEO VV, DEO PF, DEO VP”.

Asunto: "*NOTIFICACIÓN DE EMBARAZO COLABORADORA DE LA JEF COM RETAIL*".

Cuyo contenido indica que la colaboradora "*MV.*", según certificado que adjunta en el correo, cursa embarazo. (*Anexo X* y *Anexo Y*, copia del mail y del certificado de embarazo respectivamente)

h) En el momento de la pericia se encontró el mail enviado el día *XX* de noviembre de 2017 a las *1X:X5* por el ex empleado "*RA*" para "*FIN JA*, *COM RM*, *DEO BG*, *DEO VV*, *DEO PF*, *DEO VP*", cuyo asunto indica "*NOTIFICACIÓN DE EMBARAZO COLABORADORA DE LA JEF COM RETAIL*".

i) En el momento de la pericia, se observó que el mail enviado por "RA" para "FIN JA, COM RM, DEO BG, DEO VV, DEO PF, DEO VP", fue reenviado desde el correo de "DEO VP" a "DEO DA" el mismo día, es decir el XX de noviembre de 2017 a las 1X:5X, para los fines pertinentes.

j) Se realizó la verificación en el buzón de la cuenta de COM RM (mr.xxxx@xxx.gob.ec), pero no se encuentra la copia de dicho mail del inciso g.

k) Se realizó la verificación en el buzón de la cuenta de DEO BG (gb.xxxx@xxx.gob.ec), pero no se encuentra la copia de dicho mail del inciso g.

l) Se realizó la verificación en el buzón de la cuenta de DEO VV (vv.xxxx@xxx.gob.ec), pero no se encuentra la copia de dicho mail del inciso g.

DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO

Lugar donde se realiza Peritaje Informático

Equipos a Inspeccionar

OTROS REQUISITOS

A la fecha de la entrega del informe no se ha planteado por ninguna de las partes requisito adicional a los mencionados en la petición.

DECLARACIÓN JURAMENTADA

Declaro bajo juramento que el presente informe es independiente y corresponde a mi real convicción profesional, así como también, toda la información que he proporcionado es verdadera salvo error u omisión.

CRITERIO DEL PERITO COMPARACIÓN CON LA METODOLOGÍA PLANTEADA

Análisis Cualitativo

Se realizó una entrevista a un perito informático calificado en el Consejo de la Judicatura, una vez que revisó la metodología propuesta y se le preguntó su opinión de la propuesta en esta tesis, indicó: A mi criterio los *CheckList* para validar la metodología y el seguimiento de la cadena de custodia a través de la actuación pericial, están bastante bien y contemplan todo lo que se debe realizar en un procedimiento de pericia informática, el estándar utilizado es decir la norma ISO 27037 es el más adecuado y correctamente elegido para el manejo de la potencial evidencia digital; como ventajas se puede indicar que ahorra tiempo en la actuación pericial por considerar elementos relevantes, se preserva la evidencia siguiendo estándares internacionales, se utilizan las mejores partes de las metodologías estudiadas de la investigación para obtener resultados admisibles.

Con respecto a la solución del caso presentado el perito indicó que, la verificación de las cuentas de correo se realizó en sitio y visualizando las configuraciones de los programas como el Outlook o el programa que ellos utilizaban para el manejo del correo.

El tiempo que tomó la revisión por mail fue de unos 45 a 60 min, para el caso de verificar archivos adjuntos en los correos, se analizó los discos duros a través de herramientas para dicho fin.

Para la verificación del dominio lo haces con el comando Whois o a través de la página web nic.ec si se necesita validar un dominio *.ec*

Siguiendo la metodología planteada en el documento; para realizar la misma pericia, tomando en cuenta los pasos que conciernan al caso realizado, facilitaría el proceso y aportaría confiabilidad y valor probatorio para ser presentada.

FIRMA Y RUBRICA

Ing. RL.

CC 06XXXXXX35

Código: 18XXX92

El perito que emitió su criterio además otorgó su credencial con sus datos y firma respectiva como se indica a continuación:

Tabla 27. Firma otorgada a la investigación por el experto

Nombres y Apellidos del Perito	RL.
Profesión	Ingeniero en Sistemas Informáticos
No. Identificación Pericial	18XXX92
Dirección de Contacto	Miguel G. X8-X9 y Av. XXXX
Teléfono(s)	09X-XXX2-XX4
Correo Electrónico	XXXX@gmail.com
Firma	*Ing. RL.* *CC 06XXXXXX35* *Código: 18XXX92*

Fuente: Autor

A continuación, se muestra la credencial del perito en mención:

"CONSEJO DE LA JUDICATURA"

CERTIFICADO DE CALIFICACIÓN EN EL REGISTRO DE PERITOS DE LA FUNCIÓN JUDICIAL

DATOS GENERALES

LUGAR Y FECHA DE CALIFICACIÓN	QUITO, May 2017		
FECHA DE VENCIMIENTO	May 2019		
AREA	INGENIERIA		
ESPECIALIDAD	Ingeniera Informatica o de Sistemas		
No. DE CALIFICACIÓN	1(2		
APELLIDOS Y NOMBRES	LL [redacted] RENATO [redacted]		
DOCUMENTO DE IDENTIDAD	0E [redacted]5		
PROVINCIA	PICHINCHA		
CANTÓN	QUITO		
SERVIDOR/A	NO	INSTITUCIÓN	

El portador del presente certificado es PERITO CALIFICADO EN EL REGISTRO DE LA FUNCION JUDICIAL, está autorizado para participar como tal en los distintos procesos judiciales o pre procesales de la Función Judicial, durante la vigencia de su calificación

Director(a) Provincial de [redacted]
del Consejo de la Judicatura"

Figura 23. Credencial del perito calificado por el Consejo de la Judicatura

Fuente: Autor

3.4 DIFUSIÓN DEL DISEÑO DE LA METODOLOGÍA DE INFORMÁTICA FORENSE PROPUESTA

La información registrada en esta encuesta es de carácter CONFIDENCIAL y para fines académicos, la misma que fue diseñada como proyecto de tesis en la Universidad Internacional SEK. Nos gustaría conocer tu opinión sobre la metodología propuesta que contiene las Mejores Prácticas a nivel internacional sobre informática forense. Rellena esta breve encuesta y dinos qué piensas (las respuestas son anónimas).

Preguntas y Resultados de la Encuesta

Fecha Emisión Encuesta: 10/06/2019

1. En la etapa de Ubicación de la escena de los hechos detallada en la metodología planteada, ¿los aspectos referenciados en la misma se consideran suficientes para detallar

la localización, así como también determinar detalles de manera clara para la situación del lugar de los acontecimientos?

Si

No

La respuesta de la pregunta número uno destaca que un 92,3% de peritos encuestados opina que considera suficiente para detallar la localización de la escena, los aspectos referenciados en la metodología planteada.

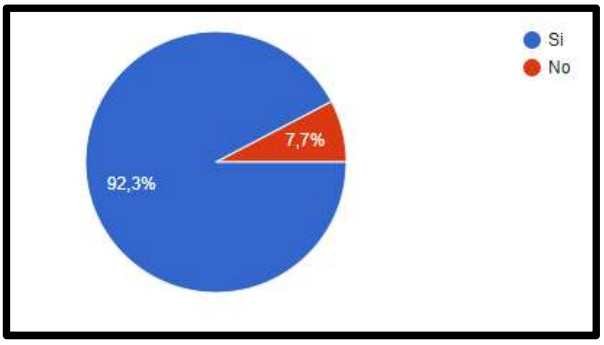


Figura 24. Respuestas de la fase Ubicación de la Escena

Fuente: autor

2. Entre las actividades de asegurar la escena de los hechos, se destacan actividades como registrar los dispositivos encontrados, asegurarlos, etiquetarlos, fotografiarlos; el DEFR además controla que personas no autorizadas, no tengan acceso a dispositivos de la escena; según su criterio y lo revisado en esta etapa, ¿la fase de aseguramiento del lugar de los hechos planteada en la metodología propuesta es confiable?

Si

No

La respuesta a la pregunta dos, evidencia un 88,5% de peritos que indica que la fase de aseguramiento de la escena de los hechos de la metodología planteada es confiable.

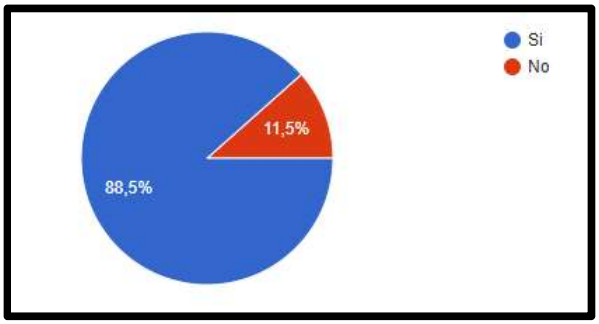


Figura 25. Respuestas de la fase Aseguramiento de la escena

Fuente: autor

3. En la fase de Identificación de la evidencia, se designan peritos por sorteo desde la Función Judicial a través del Sistema Informático Pericial; en esta fase según la metodología propuesta se garantiza la integridad de la cadena de custodia de la evidencia, según lo indicado en esta etapa, ¿es la fase de identificación admisible?

Si

No

En la respuesta de la pregunta tres, relacionada con la fase de identificación, el 76,9% de encuestados indica que la fase es admisible.

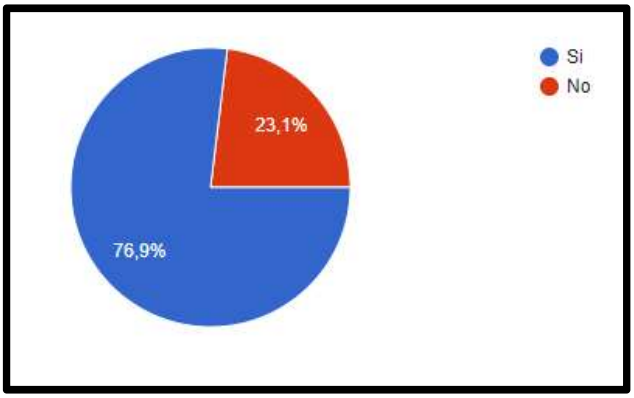


Figura 26. Respuestas de la fase Identificación de la Evidencia

Fuente: autor

4. En la fase de identificación, como parte de la actuación pericial, se deben efectuar copias bit a bit de la evidencia contenida en discos duros, se obtiene la firma hash de los

bits leídos durante el proceso; se identifica de manera clara y precisa la evidencia, todo cambio potencial en la evidencia se registra, dichas acciones según su criterio, le ¿aporta validez e integridad a la evidencia?

Sí

No

En la respuesta a la pregunta cuatro, un 92,3% de los peritos informáticos encuestados, considera que la fase de identificación de la evidencia, aporta validez e integridad a la evidencia.

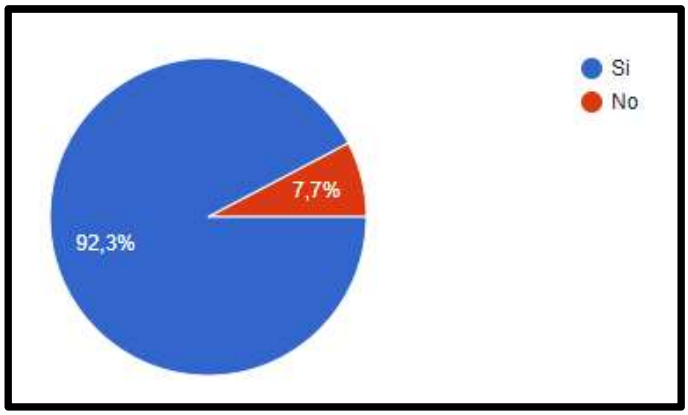


Figura 27. Respuestas de la validez de la identificación de la evidencia

Fuente: autor

5. En la fase de recolección y adquisición de la evidencia, según la metodología planteada, se revisa si los hashes coinciden, para comprobar la integridad de la evidencia, se identifica información relevante, se recuperan archivos eliminados, se pueden emplear técnicas de minería de datos; según su criterio ¿la evidencia que se puede recolectar con esos criterios cumple con el principio de confiabilidad para ser admisible?

Sí

No

La respuesta a la pregunta cinco, indica que el 96,2% de los encuestados considera que la fase de recolección y adquisición de evidencia y sus criterios aportan confiabilidad y admisibilidad.

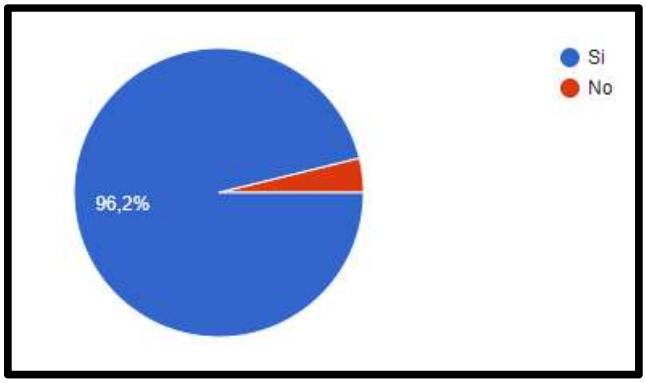


Figura 28. Respuestas de la fase de recolección y adquisición de evidencia

Fuente: autor

6. Una vez recolectada la evidencia digital, en la fase e Preservación y Conservación, se definen métodos de preservación, para garantizar la integridad y autenticidad, se generan respaldos, se sigue la cadena de custodia, se establece quien accede a la evidencia, se registran las tareas realizadas con la evidencia; con estos antecedentes la fase en mención ¿cumple con los criterios de admisibilidad de la evidencia?

Si

No

La respuesta a la pregunta seis, explica que el 88,5% de los peritos encuestados considera que la fase de preservación y conservación de la evidencia cumple con el principio de admisibilidad de la evidencia.

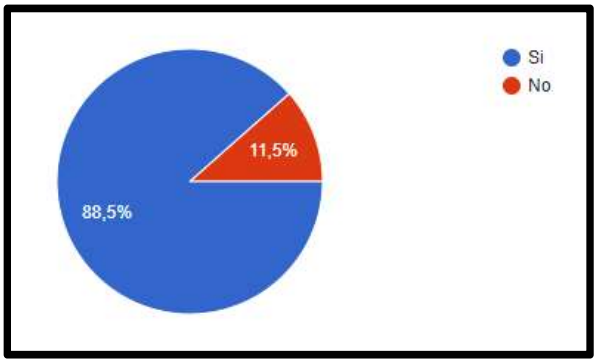


Figura 29. Respuestas de la fase de preservación y conservación de evidencia
Fuente: autor

7. La fase de Análisis de la evidencia, se basa en las mejores prácticas de las normas ISO 27037, RFC 3227, UNE 71505 (Sistema de Gestión de Evidencias Electrónicas) y UNE 71506 (Metodología para el Análisis Forense de las Evidencias Electrónicas); se trabaja con las copias de imágenes forenses, se identifica el autor de los hechos, se documenta la información relevante siguiendo la cadena de custodia entre otras actividades, según su criterio, ¿la fase de análisis en la metodología planteada es admisible?

1. Muy en desacuerdo
2. En desacuerdo
3. Indeciso
4. De acuerdo
5. Muy de acuerdo

La respuesta a los peritos en la pregunta siete manifiesta un 50% que está muy de acuerdo de que la metodología planteada en la fase de análisis de la evidencia, que junto con un 23% que está de acuerdo cuenta con un total de 73% de aceptación de la fase de análisis.

Tabla 28. Respuestas de la fase análisis de la evidencia

Fase de análisis de evidencia / Grado Satisfacción	**1**	**2**	**3**	**4**	**5**
Número de peritos	1	1	9	9	20
Porcentaje	2	2	23	23	50

Fuente: Encuesta a peritos informáticos El autor

8. Una vez expuestas las fases de la metodología propuesta: ubicación de la escena, asegurar y evaluar la escena, identificación de evidencias, recolección y adquisición, conservación y preservación; y análisis de la evidencia, las mismas que están basadas en normas internacionales como la ISO/IEC 27037:2012 y las mejores prácticas de metodologías de España, Argentina y Colombia; con estos criterios ¿la evidencia después de la etapa de análisis puede ser presentada en un tribunal como admisible?

1. Muy en desacuerdo
2. En desacuerdo
3. Indeciso
4. De acuerdo
5. Muy de acuerdo

Como respuesta en la pregunta ocho, los peritos informáticos del Consejo de la Judicatura indican con un 54% que están muy de acuerdo que junto con un 35% que están de acuerdo se cuenta con un total de 89% de aceptación para que la evidencia sea admisible para la presentación en un tribunal.

Tabla 29. Respuestas de criterio de admisibilidad de la evidencia

Fase posterior al análisis de evidencia / Grado Satisfacción	**1**	**2**	**3**	**4**	**5**
Número de peritos	0	1	3	14	22
Porcentaje	0	3	8	35	54

Fuente: Encuesta a peritos informáticos El autor

9. De acuerdo a la metodología planteada, una vez expuestas las fases de la misma, según su criterio ¿la metodología puede ayudar en mejorar la calidad probatoria considerando que está basado en el estándar ISO/IEC 27037:2012 y las mejores prácticas en países como España, Argentina y Colombia que son referentes en temas de informática forense?

1. Muy en desacuerdo
2. En desacuerdo
3. Indeciso
4. De acuerdo
5. Muy de acuerdo

En la pregunta nueve los peritos encuestados indican un 53% que están muy de acuerdo que junto con un 30% que están de acuerdo, se cuenta con un 83% que manifiestan que mejora la calidad probatoria con la metodología planteada.

Tabla 30. Respuestas referentes a la calidad probatoria con la metodología planteada

Criterio de la calidad probatoria/ Grado Satisfacción	1	2	3	4	5
Número de peritos	0	3	4	12	21
Porcentaje	0	8	9	30	53

Fuente: Encuesta a peritos informáticos El autor

10. ¿Considera que la metodología planteada, le ayuda a mejorar los tiempos de identificación, recolección, adquisición, preservación y análisis de la evidencia tomando en cuenta que durante todo el proceso se realiza un seguimiento de la cadena de custodia y se registran las fechas y tiempos desde que se inicia la investigación hasta que se obtiene resultados probatorios?

1. Muy en desacuerdo
2. En desacuerdo
3. Indeciso
4. De acuerdo
5. Muy de acuerdo

Según las respuestas de los peritos informáticos encuestados, en la pregunta diez se indica que un 50% está muy de acuerdo que junto con un 34% que está de acuerdo forman un total de 84% que está de acuerdo que mejoran los tiempos del manejo de la evidencia digital para obtener resultados probatorios.

Tabla 31. Criterio respecto a mejora de tiempos del manejo de evidencia

Criterio mejora de tiempos / Grado Satisfacción	1	2	3	4	5
Número de peritos	0	4	2	14	20
Porcentaje	0	11	5	34	50

Fuente: Encuesta a peritos informáticos El autor

11. Una vez revisado el diseño de la metodología basada en la Norma Internacional ISO/IEC 27037:2012, ¿cree que podría aportar calidad probatoria en la recolección de evidencia digital?

1. Muy en desacuerdo
2. En desacuerdo
3. Indeciso
4. De acuerdo
5. Muy de acuerdo

Con respecto a la pregunta once, se visualiza que en las respuestas de los peritos existe un total acuerdo del 87% que indica que la metodología aporta en calidad probatoria en la recolección de evidencia digital, dicho porcentaje está formado por un 53% que está muy de acuerdo junto con un 34% que está de acuerdo.

Tabla 32. Criterio de calidad probatoria en la recolección de evidencia digital

Criterio calidad probatoria en recolección de evidencia / Grado Satisfacción	1	2	3	4	5
Número de peritos	0	0	6	13	21
Porcentaje	0	0	13	34	53

Fuente: Encuesta a peritos informáticos El autor

12. La metodología propuesta, basada en la Norma Internacional ISO/IEC 27037:2012, y en las mejores prácticas de manejo de evidencia digital de países como España, Argentina y Colombia; según su criterio, ¿cumple con los principios de suficiencia, confiabilidad y admisibilidad?

1. Muy en desacuerdo
2. En desacuerdo
3. Indeciso
4. De acuerdo
5. Muy de acuerdo

Respecto a lo indicado por los peritos encuestados, se indica en la pregunta doce que existe un 46% que está muy de acuerdo, junto con un 38% que está de acuerdo, los

mismos que forman un total de 84% que manifiestan que la metodología planteada cumple con los principios de suficiencia, confiabilidad y admisibilidad.

Tabla 33. Criterio de cumplimiento de principios de manejo de evidencia

Criterio de cumplimiento de principios de manejo de evidencia / Grado Satisfacción	1	2	3	4	5
Número de peritos	0	3	4	15	18
Porcentaje	0	5	11	38	46

Fuente: Encuesta a peritos informáticos El autor

13. En comparación con otras metodologías de informática forense, la metodología planteada orienta a Especialistas en evidencia digital de Primera Intervención (DEFR), Especialistas en Evidencia Digital (DES), Especialistas en respuesta a incidentes y gerentes de laboratorios forenses; lo cual puede contribuir a su admisibilidad en procesos judiciales; según su criterio, la metodología planteada ¿se considera con alguna ventaja competitiva respecto a otras metodologías de informática forense que usted conoce?

1. Muy en desacuerdo
2. En desacuerdo
3. Indeciso
4. De acuerdo
5. Muy de acuerdo

Según las respuestas de los peritos informáticos en la pregunta trece, existe un 30% que está muy de acuerdo, junto a un 42% que está de acuerdo, que indican que un total de 72% están de acuerdo que la metodología tiene una ventaja competitiva respecto a otras metodologías de informática forense.

Tabla 34. Criterio en relación a las ventajas competitivas respecto a otras metodologías

Criterio en relación a ventajas competitivas respecto a otras metodologías / Grado Satisfacción	1	2	3	4	5
Número de peritos	0	3	9	16	12
Porcentaje	0	5	23	42	30

Fuente: Encuesta a peritos informáticos El autor

14. ¿Recomendaría la metodología planteada, para que sea utilizada a nivel nacional?

1. Muy en desacuerdo
2. En desacuerdo
3. Indeciso
4. De acuerdo
5. Muy de acuerdo

Finalmente en las respuestas de los peritos informáticos encuestados en la pregunta catorce, formado por 42% que están muy de acuerdo junto con el 46% indican con un total de 88% que recomiendan que la metodología planteada debe ser utilizada a nivel nacional.

Tabla 35. Criterio de recomendación de utilización de la metodología planteada

Criterio de recomendación de utilización de la metodología / Grado Satisfacción	**1**	**2**	**3**	**4**	**5**
Número de peritos	0	1	4	18	17
Porcentaje	0	3	9	46	42

Fuente: Encuesta a peritos informáticos El autor

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

La tecnología actualmente es un instrumento fundamental en los ámbitos social, personal y económico; cada vez existe más dependencia de equipos como tablets, celulares, computadores, cámaras de video vigilancia, entre otros dispositivos; el avance de la tecnología nos ha facilitado las cosas en varios aspectos, sin embargo también la tecnología se utiliza para realizar actividades ilícitas, entre ellas el fraude a entidades financieras, estafas, robo de información, contraseñas, acceso no consentido a un sistema. Es por eso que cada país ha adoptado leyes para protección de la información, además para sancionar los delitos informáticos; es por esto, que se diseñó la metodología para aportar con una mejora en el manejo de la evidencia digital, además de seguir una cadena de custodia que cumpla los principios de admisibilidad ante la justicia.

Ante los ataques informáticos, se crean leyes que permitan tipificar los delitos, en este espacio surge la necesidad que tienen los jueces de tener un criterio experto e independiente denominado peritaje informático, los peritos están facultados para identificar, recolectar, preservar, analizar y presentar potencial evidencia digital en casos judiciales; sin embargo para que las pruebas sean válidas deben cumplir procesos y procedimientos que garanticen y aseguren las características originales de la prueba, es precisamente eso lo que brinda el diseño de la metodología propuesta en el presente documento con el fin de que el perito sea un auxiliar de la justicia en los casos de delitos informáticos.

Se investigó el tratamiento de evidencias digitales en países como España, Argentina, Colombia; los países indicados tienen un avance significativo en temas de informática forense, siguen métodos que son válidos en sus jurisdicciones, estos sirvieron para diseñar una metodología propia para Ecuador, junto con las pautas y principios

indicados en la Norma ISO/IEC 27037:2012 que es una guía a nivel internacional para identificar, recolectar, adquirir y preservar evidencia digital.

Se diagnosticó por medio de una encuesta el manejo de la evidencia digital en Ecuador, el análisis indica que en Ecuador no se sigue métodos estandarizados para la gestión de la evidencia probatoria, es por eso que al diseñar la metodología propuesta esta orienta en la actividad pericial para la identificación, recopilación, obtención y conservación de la evidencia digital; en la que se siguen métodos menos intrusivos, procedimientos que han sido validados, en los que se preserva la originalidad de la prueba, se realiza respaldos correspondientes, para que a posteriori pueda ser admisible dicha prueba ante un tribunal.

Se realizó la difusión del diseño de la metodología planteada a peritos calificados en el Consejo de la Judicatura a nivel nacional, en la que se concluyen los siguientes resultados: 92,3% de peritos encuestados opina que considera suficiente para detallar la localización de la escena; 88,5% de peritos que indica que la fase de aseguramiento de la escena de los hechos de la metodología planteada es confiable; 76,9% de encuestados indica que la fase identificación es admisible; 92,3% de los peritos informáticos encuestados, considera que la fase de identificación de la evidencia, aporta validez e integridad a la evidencia; 96,2% de los encuestados considera que la fase de recolección y adquisición de evidencia y sus criterios aportan confiabilidad y admisibilidad; 88,5% de los peritos encuestados considera que la fase de preservación y conservación de la evidencia cumple con el principio de admisibilidad de la evidencia; 73% de aceptación de la fase de análisis; 89% de aceptación para que la evidencia sea admisible para la presentación en un tribunal; un 83% que manifiestan que mejora la calidad probatoria con la metodología planteada; 84% que está de acuerdo que mejoran los tiempos del manejo de la evidencia digital para obtener resultados probatorios; 87% que indica que la metodología aporta en calidad probatoria en la recolección de evidencia digital; 84% que manifiestan que la metodología planteada cumple con los principios de suficiencia, confiabilidad y admisibilidad; 72% están de acuerdo que la metodología tiene una ventaja competitiva respecto a otras metodologías de informática forense; finalmente el 88% que recomiendan que la metodología planteada debe ser utilizada a nivel nacional.

4.2 RECOMENDACIONES

Se recomienda la aplicación de la metodología diseñada y validada en el presente documento de tesis de fin de carrera de máster, a los peritos informáticos de Ecuador, sin embargo puede extenderse su validez a nivel internacional en caso que las distintas jurisdicciones decidan adoptarla y la consideren idónea para su aplicación, se debe tomar en cuenta que está basada en estándares internacionales como es la Norma ISO/IEC 27037:2012 que maneja principios de aplicación de métodos, procesos auditables, reproducibles y defendibles.

La norma ISO/IEC 27037:2012 proporciona procedimientos específicos para cada proceso del manejo de evidencia digital, en los que tiene como competencia; a las personas interesadas en aplicar la metodología propuesta, se recomienda definir las responsabilidades a las personas autorizadas establecidas en la norma: DEFR (Especialistas en evidencia digital de primera intervención), DES (Especialistas en evidencia digital), Especialistas en respuestas a incidentes y gerentes de laboratorios forenses, con el fin de que se garantice la gestión de la potencial evidencia digital de forma aceptable, íntegra y auténtica.

BIBLIOGRAFÍA:

Acurio, S. (2006). Introducción a La Informática Forense. In *Introduccion a la Informática Forense* (p. 64). Quito. https://doi.org/10.1157/13068212

Almeida, O. R. (2011). *Metodología para la implementación de Informática Forense en sistemas operativos Windows y Linux*. UNIVERSIDAD TECNICA DEL NORTE.

Álvarez Serna, A. F., Rivera, O. D. M., & Morales, J. D. V. (2012). Framework para la computación forense en Colombia. *Ingenierías USBMed*, *3*(2), 61–69. https://doi.org/10.21500/20275846.276

Armilla, N., Panizzi, M., Eterovic, J., & Torres, L. (2017a). Buenas prácticas para la recolección de la evidencia digital en la Argentina. *XXIII Congreso Argentino de Ciencias de La Computación*, 10.

Armilla, N., Panizzi, M., Eterovic, J., & Torres, L. (2017b). Buenas prácticas para la recolección de la evidencia digital en la Argentina, 10.

Arnedo, P. (2014). *Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos*. *Universidad Internacional de la Rioja*. Universidad Internacional de la Rioja. Retrieved from https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo blanco.pdf?sequence=1

Cano, J. (2017). La evidencia digital en el Código General del Proceso. *Evento CEDEVAL*, 1–21.

COIP. (2014). *Código Orgánico Integral Penal*. *Registro Oficial - Ógano del Gobierno del Ecuador*. Retrieved from https://www.mendeley.com/import/

De León, F. (2009). *Estudio de metodologías de análisis forense digital*. Instituto Politécnico Nacional.

García, J. (2015). *Informe sobre el Peritaje Informático*. Universidad Carlos III de Madrid.

Ghosh, A. (2004). Guidelines for the Management of IT Evidence. *APEC Telecommunications and Information Working Group*, (March), 0–26.

Gitec. (2012). *Manual de buenas prácticas en la escena del Crimen*. Retrieved from http://www.inacipe.gob.mx/stories/publicaciones/descargas_gratuitas/12Manual1aReimp.pdf

Gómez, S. (2014). Procedimientos Internos y Guías Operativas. *Departamento de Informática Forense Poder Judicial de Rio Negro*, 1–17.

Granda, G. E. (2015). *Metodología para el análisis forense de datos e imágenes de acuerdo a las leyes del Ecuador*. *Universidad Politécnica Salesiana*. Universidad Politécnica Salesiana Sede Cuenca.

Guerrero, J., & Sanchez, L. (2013). Requerimientos para el diseño de un laboratorio de análisis forense digital enfocado a pequeñas y medianas empresas de Colombia, 171.

Guerron, Y. (2018). *Diseño e implementación de un procedimiento para la recolección, cadena de custodia y uso de evidencia digital en la gerencia departamental Valle del Cauca de la Contraloría General de la República*. Universidad Nacional Abierta y a Distancia UNAD.

Igarza, A., Gioia, C., & Eterovic, J. (2018). *Análisis del Marco Normativo Legal para el Ciclo de Vida de la Evidencia Digital*.

Iguarán, M. (2004). *Manual de Procedimientos para Cadena de Custodia*. (C. Barrerra Barinas, Rodrigo; Días Vásquez, Ed.). Bogotá.

Iorio, A. (2015). *Guía Integral de Empleo de la Informática Forense en el Proceso Penal*. *Info-Lab* (primera ed). Mar del Plata: Universidad FASTA. Retrieved from http://www.info-lab.org.ar/images/pdf/14.pdf

ISO/IEC. (2012). INTERNATIONAL STANDARD ISO / IEC: Information technology — Security techniques — Guidelines for cybersecurity. *Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, *2011*, 9.

Jaramillo, D., & Torres, M. (2016). *Estado del análisis forense digital en Colombia*. *ESTADO DEL ANALISIS FORENSE DIGITAL EN COLOMBIA*. UNIVERSIDAD MILITAR NUEVA GRANADA.

Judicatura. (2016). Reglamento del sistema pericial integral de la funcion judicial. Quito.

Lasso, V. (2017). *Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia*. Universidad Nacional Abierta y a Distancia, UNAD. https://doi.org/10.1111/j.1469-7610.2010.02280.x

LEY DE COMERCIO ELECTRONICO. (2002). Ley de comercio electrónico, firmas electrónicas y mensajes de datos (p. 17). Quito.

Mesa, A. (2015, June). La evidencia digital eximiente de violación a la protección del

dato personal a partir. *Revista Academia & Derecho, 6(10), (119-156).*, *10*, 119–156.

Mukasey, M., Sedgwick, J., & Hagy, D. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. *National Institute of Justice*, 74. Retrieved from http://www.iacpcybercenter.org/prosecutors/litigation-resources/

Navarro, J. (2016). *Guía actualizada para futuros peritos informáticos. Ultimas herramientas de análisis forense digital. Caso práctico*. *Guía actualizada para futuros peritos informáticos. Ultimas herramientas de análisis forense digital. Caso práctico*. Universitat Politecnica de Valencia.

Osorio, H. (2012). *El peritaje de los delitos informaticos*. Universidad de San Carlos de Guatemala.

Parada, R. (2018). *Cibercrimen y delitos informáticos*. Buenos Aires.

Puig, S. (2014). *La prueba electrónica: sus implicaciones en la seguridad de la empresa*. *LA PRUEBA ELECTRÓNICA: SUS IMPLICACIONES EN LA SEGURIDAD DE LA EMPRESA*. Universitat Ramon Llull.

Ramírez, D., & Castro, E. (2018). *Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia*. Universidad Nacional Abierta y a Distancia UNAD.

Rivas, C. G. (2014a). *Metodología para un análisis forense*. *Metodología para un análisis forense*. Universitat Oberta de Catalunya. Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

Rivas, C. G. (2014b). Metodología para un análisis forense. *Metodología Para Un Análisis Forense*, 55. Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

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

Rodríguez. (2011). *La Informática Forense: El Rastro Digital del Crimen*. *Derecho y Cambio Social* (Vol. 25). Retrieved from http://www.derechoycambiosocial.com/revista025/informatica_forense.pdf

Rodríguez, C. (2018). *Introducción a la Informática Forense : Legal , teórica y práctica*. Universitat Oberta de Catalunya.

Semprini, G. (2016a). El análisis integral de la evidencia digital. *El Análisis Integral de*

La Evidencia Digital, 12. Retrieved from http://www.clei2017-46jaiio.sadio.org.ar/sites/default/files/Mem/SID/sid-07.pdf

Semprini, G. (2016b). El análisis integral de la evidencia digital. *SID, Simposio Argentino de Informática y Derecho*, 12. Retrieved from http://www.clei2017-46jaiio.sadio.org.ar/sites/default/files/Mem/SID/sid-07.pdf

Taribó, H. (2016). Caso pr actico de informe experto de an alisis forense digital, 110.

Veber, J., & Smutny, Z. (2015). Standard ISO 27037:2012 and collection of digital evidence: Experience in the Czech Republic. In *European Conference on Information Warfare and Security, ECCWS* (Vol. 2015-Janua, pp. 294–299).

Velázquez, R. (2016). Evidencia digital, clave en la resolución de los procesos judiciales. *Red Seguridad*, *73*, 84. Retrieved from http://www.redseguridad.com/revistas/red/073/files/assets/common/downloads/files/red073_blq.pdf

EFE. (2005, 25 junio). El asesino en serie de EEUU BTK se declara culpable de 10 muertes. El mundo, p. 1. Recuperado de https://www.elmundo.es/elmundo/2005/06/27/sociedad/1119887368.html

López, R.(2012). Perito Informático y Tecnológico-PeritoIT.Obtenido de PeritoIT:https://peritoit.com

Salmerón, A.(2017). Informática Forense y Pericial.Obtenido de Informática Forense:http://www.forense.info

ANEXO A

RESUMEN DE LAS FASES Y SUB FASES DE LA METODOLOGÍA PROPUESTA

Tabla 36. Síntesis de las fases y sub fases de la metodología propuesta

Fases	Sub fases
Ubicación de la Escena	Localización de la escena, Institución donde se desarrollan los hechos, Fijación Fotográfica, Fijación Video gráfica.
Asegurar y Evaluar la Escena	Seguir procedimientos para asegurar las escenas del crimen, Asegurar de inmediato todos los dispositivos electrónicos, Directivas para asegurar la evidencia en la escena.
Identificación de las evidencias	Verificar el estado del ordenador, Realizar el análisis de volatilidad, Realizar imágenes forenses, Preservar Imágenes forenses, Identificar los requerimientos del caso, Identificar posibles herramientas, Verificar existencia de software de borrado.
Recolección y Adquisición	Autorizaciones para realizar la pericia sobre un equipo, Montar Imagen Forense, Recuperar archivos eliminados, Recolección de potencial evidencia digital.
Conservación y Preservación	Definir métodos de preservación de evidencia, Generar Respaldos de la evidencia, Se realiza un seguimiento de la cadena de custodia
Análisis de la Evidencia	Disponer un escenario de trabajo apropiado a las necesidades del acontecimiento, Identificar el autor o autores de los hechos investigados, Documentar la información relevante encontrada en relación al caso investigado, Preservar la cadena de custodia durante todo el proceso de la investigación.

Fuente: Elaborado por autor

ANEXO B

PRINCIPIOS QUE GOBIERNAN LA EVIDENCIA DIGITAL

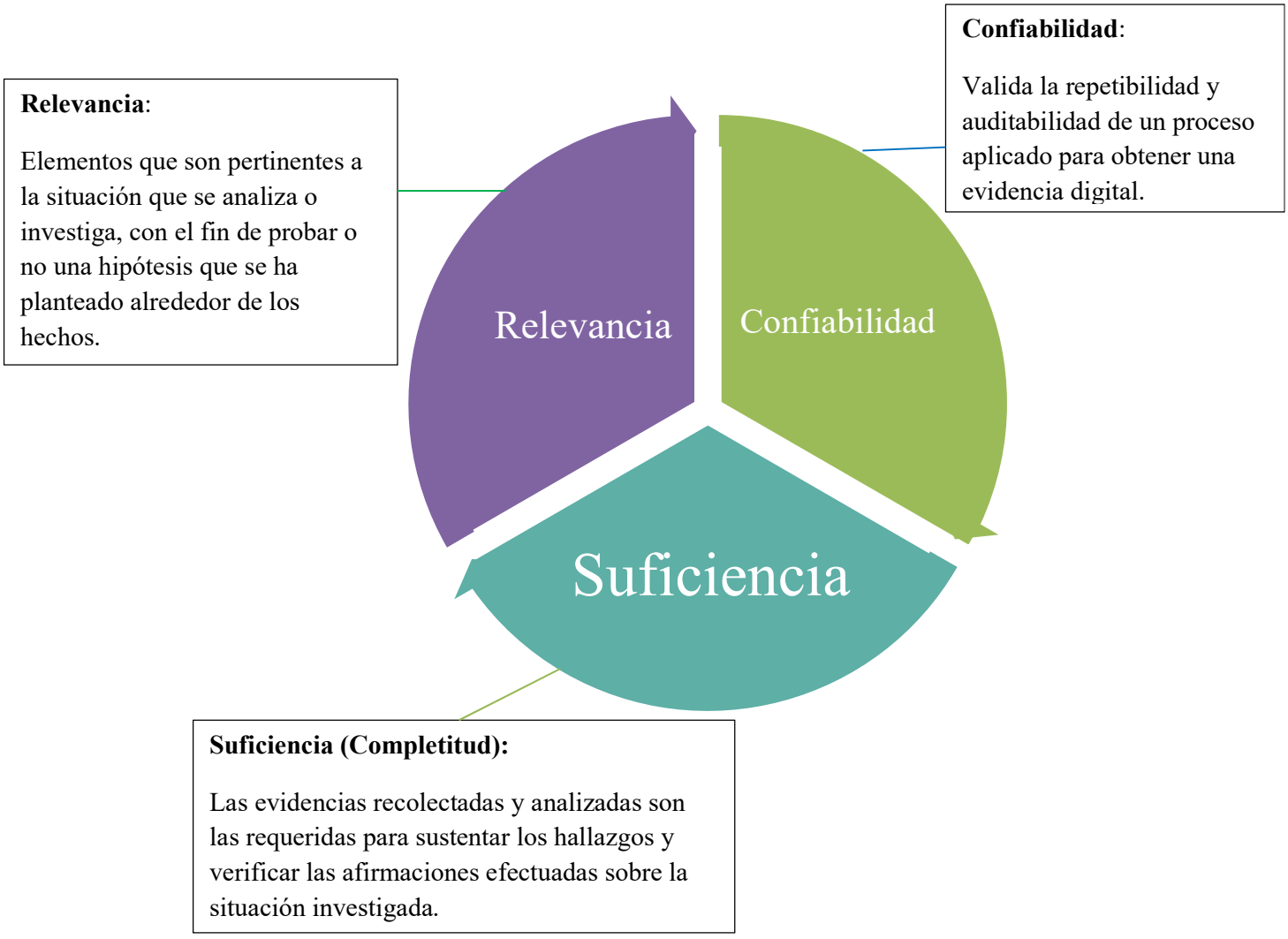


Figura 30. Principios que gobiernan la evidencia digital

Fuente: Tomado de ISO/IEC 27037:2012. Tecnología de la información – Técnicas de seguridad – Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital. (Cano, 2017)Elaborado por autor.