Universidad Tecnológica ECOTEC

Título del Trabajo:

Guía auxiliar para fortalecer el tratamiento de evidencia digital en Ecuador

Línea de Investigación:

Gestión de las relaciones jurisprudenciales.

Modalidad de titulación:

Proyecto Integrador

Nombre de la Carrera:

Licenciatura en Criminalística

Título a obtener:

Licenciado/a en Criminalística

Nombre de las autoras:

Doménica Milena Robalino Macías.

Ruth Doménica Cordero Cedeño.

Tutor:

Abg. Miguel Leonardo Mora Romero Mgtr.

Ciudad:

Samborondón-Ecuador

Año:

2024

Dedicatoria

A mis padres, quienes con su amor y apoyo incondicional me han guiado a lo largo de mi vida académica, gracias por enseñarme el valor del esfuerzo, la perseverancia y la honestidad. Sin su ejemplo y sacrificio, este logro no habría sido posible.

A mis amigas y compañeras de carrera, su compañía y sus palabras de aliento han sido un pilar fundamental durante todo este proceso. A Carlos, quien siempre creyó en mí y estuvo presente en todo momento brindándome su apoyo incondicional.

Ruth Cordero Cedeño.

Dedicatoria

A mis amados padres, por su inmenso cariño y apoyo incondicional en cada paso de este arduo camino académico, gracias por no dejar que rinda a pesar de las adversidades. Este logro es por y para ustedes.

A Geanella, Naggely, Doménica y Arianna, quienes siempre han tenido fe en mí y me han acompañado en este proceso.

A mis amigas y compañeros de carrera, gracias por confiar en mí, por su apoyo en todos los momentos difíciles y por todos los lindos momentos vividos en la universidad.

A Matteo, por impulsarme en cada momento y siempre creer en mí. Eres lo mejor que pudo pasarme.

Y, especialmente, a todos los peritos en informática forense, entre ellos Mr. Emiliano Zárate, cuyo esfuerzo incansable y dedicación han inspirado esta investigación. Su labor meticulosa y compromiso con la justicia. Esta tesis es un homenaje a su perseverancia, profesionalismo y a su invaluable contribución académica.

Doménica Milena Robalino Macías.

Agradecimiento

Quiero expresar mi profundo agradecimiento a mi tutor de tesis, quien con su tiempo, paciencia y experticia nos guío para la realización de este trabajo.

A los docentes de la facultad, y al magister Diego Peña, durante este período sus enseñanzas han sido fundamentales en mi formación profesional y personal.

A mis tías Alexandra y Faviola, quienes han sido un pilar fundamental brindándome su apoyo para que mis estudios en la ciudad de Guayaquil sean posibles. A Carlos, gracias por ser mi refugio y mi fuerza en los momentos difíciles.

Ruth Cordero Cedeño.

Agradecimiento

Agradezco a Dios, por su infinito amor y bondad, por guiarme siempre en el camino correcto.

A mis padres, cuya infinita paciencia, amor y apoyo incondicional me han acompañado siempre. Gracias por creer en mí y por ser mi pilar en cada etapa de este proceso.

A mis docentes de titulación y de la facultad, por su compromiso y por compartir su vasto conocimiento. Sus enseñanzas han sido una fuente de inspiración y una base sólida para la construcción de esta tesis.

A mis amigos, por su constante ánimo y compañerismo. Gracias por estar a mi lado en los momentos de alegría y en los de dificultad, y por hacer este viaje más llevadero y memorable.

Y finalmente, a mi querido novio y mejor amigo Matteo, por su amor, comprensión y apoyo incondicional. Gracias por ser mi roca, por entender mis ausencias y por estar siempre dispuesto a ofrecer una palabra de aliento.

Doménica Milena Robalino Macías.

Certificado de Revisión Final

ANEXO No. 9

PROCESO DE TITULACIÓN
CERTIFICADO DE APROBACIÓN DEL TUTOR

Samborondón, 07 de agosto del 2024

Magister o Doctor
Andrés Madero Poveda
Unidad Académica: Facultad de Derecho y Gobernabilidad
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **GUÍA AUXILIAR PARA FORTALECER EL TRATAMIENTO DE EVIDENCIA DIGITAL EN ECUADOR**, fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, por lo que se autoriza al estudiante: **Ruth Doménica Cordero Cedeño, Y Doménica Milena Robalino Macias** para que proceda con la presentación oral del mismo.

ATENTAMENTE,

Abg. Miguel Leonardo MORA ROMERO Mgtr.
Tutor

Certificado de Porcentaje de coincidencias de plagio

Universidad Ecotec

ANEXO No. 10

PROCESO DE TITULACIÓN
CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS
DEL TRABAJO DE TITULACIÓN

Habiendo sido revisado el trabajo de titulación TITULADO: GUÍA AUXILIAR PARA FORTALECER EL TRATAMIENTO DE EVIDENCIA DIGITAL EN ECUADOR, elaborado DOMENICA MILENA ROBALINO MACIAS, y RUTH DOMENICA CORDERO CEDEÑO, fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del (8 %) mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del documento. Adicional se adjunta print de pantalla de dicho resultado.

https://app.compilatio.net/v5/report/9c7ec907bdb930575c6d8d6322894111ac1527d2/summary

ATENTAMENTE,

Abg. Miguel Leonardo MORA ROMERO Mgtr.
Tutor(a)

Resumen

El presente trabajo de investigación aborda el desarrollo de una guía auxiliar para fortalecer el tratamiento de evidencia digital, a través de la revisión bibliográfica de estándares internacionales y el registro oficial N° 318.

En el caso de estudio sobre grooming denominado “el Mangajo”, con número de proceso 1724320150004G, se determinan varias anomalías durante el proceso investigativo, cuyas consecuencias terminan en la pérdida de la evidencia digital, por lo que, la guía auxiliar propuesta fue realizada tomando en cuenta, cada vacío e inconveniente respecto al tratamiento de la evidencia digital desde que fue recolectada. El enfoque de la investigación se centra en la implementación de la guía con la necesidad de estandarizar procedimientos y ofrecer directrices claras para asegurar la integridad y validez de la evidencia digital en el sistema judicial ecuatoriano.

Se realizó una revisión exhaustiva de la literatura existente que comprende los manuales de estándares internacionales y nacionales como lo son: OSAC, AICEF, ENFSI, IFSA, la norma ISO 27037 y el registro oficial N°318, además de que se llevó a cabo un estudio de campo en donde se entrevistaron a profesionales como abogados, fiscales y peritos expertos en el área quiénes han llevado casos de informática y evidencia digital.

Los resultados de la entrevista revelan una serie de deficiencias en los procedimientos actuales indican una falta de procedimientos estandarizados y formación adecuada en el manejo de evidencia digital, lo cual compromete la integridad y validez de las pruebas presentadas en los procesos judiciales, de manera que, se propone una guía estructurada que incorpora mejores prácticas internacionales adaptadas a la realidad del perito para el correcto tratamiento de evidencia digital.

Palabras claves:

Tratamiento de evidencia digital, estándares internacionales, peritos, integridad, validez.

Abstract

This research paper addresses the development of an auxiliary guide to strengthen the treatment of digital evidence, through a bibliographic review of international standards and official registry No. 318.

In the case study on grooming called “el Mangajo”, with case number 1724320150004G, several anomalies were determined during the investigative process, the consequences of which ended in the loss of digital evidence, therefore, the proposed auxiliary guide was made considering each gap and inconvenience regarding the treatment of digital evidence since it was collected. The focus of the research is on the implementation of the guide with the need to standardize procedures and offer clear guidelines to ensure the integrity and validity of digital evidence in the Ecuadorian judicial system.

An exhaustive review of the existing literature was carried out, including international and national standards manuals such as: OSAC, AICEF, ENFSI, IFSA, ISO 27037 and official registry No. 318, in addition to a field study where professionals such as lawyers, prosecutors and expert witnesses in the area who have handled cases of information technology and digital evidence were interviewed.

The results of the interview reveal a series of deficiencies in current procedures, indicating a lack of standardized procedures and adequate training in the management of digital evidence, which compromises the integrity and validity of the evidence presented in judicial proceedings. Therefore, a structured guide is proposed that incorporates international best practices adapted to the reality of the expert for the correct treatment of digital evidence.

Keywords:

Digital evidence processing, international standards, experts, integrity, validity.

Índice

Dedicatoria 2

Dedicatoria 2

Agradecimiento 3

Agradecimiento 3

Certificado de Revisión Final 4

Certificado de Porcentaje de coincidencias de plagio 5

Resumen 6

1. CAPÍTULO I: 11

PLANTEAMIENTO DEL PROBLEMA 11

1.1 Contexto histórico social del objeto de estudio 12

1.2 Antecedentes 12

1.3 Planteamiento del problema 13

1.4 Pregunta científica 13

1.5 Objetivos 14

1.5.1 Objetivo General 14

1.5.2 Objetivos Específicos 14

1.6 Justificación 14

1.7 Introducción 15

2. CAPÍTULO II: 16

MARCO TEÓRICO 16

2.1 Evidencia digital 17

2.1.1 Definición 17

2.2 Admisibilidad de la evidencia digital 18

2.3 Principios de la evidencia digital 19

2.4 Análisis forense digital 20

2.5 Análisis forense de audio y video 21

2.6 Incumbencias periciales 21

2.7 Tratamiento de la evidencia digital según el Registro Oficial N° 318: Metodología en dispositivos encendidos y apagados 22

2.8 Tratamiento de evidencia digital según la OSAC 23

2.9 Tratamiento de evidencia según el Manual de buenas prácticas en la escena del crimen de la AICEF 26

2.10 Tratamiento de evidencia digital según el Manual del International Forensic Strategic Alliance (IFSA) 27

2.11 Tratamiento de evidencia digital según el Manual de la ENFSI 29

2.12 Tratamiento de la evidencia digital según la norma internacional ISO/ IEC 27037:2012 32

2.13 Cibercrimen/ Delito informático 35

2.13.1 Definición 35

2.13.2 Tipificación de los ciberdelitos 35

2.14 Cadena de custodia 36

2.15 Grooming 37

2.15.1 ¿Cómo se configura el delito del child grooming? 37

3. CAPÍTULO III: 38

MARCO METODOLÓGICO 38

3.1 Enfoque de la investigación 39

3.2 Tipo de investigación 39

3.3 Período y lugar donde se desarrolla la investigación 40

3.4 Universo y muestra de la investigación 40

3.5 Procesamiento y análisis de información 41

3.6 Métodos empleados 43

4. CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS .45

4.1 Entrevistas 46

4.2 Análisis e interpretación de resultados 46

5. CAPÍTULO V: PROPUESTA 49

5.1 Conclusiones 50

5.2 Recomendaciones 51

5.3 Propuesta 51

6. Referencias y bibliografía 52

Bibliografía 52

Anexos 55

Anexo 1: Propuesta “Guía auxiliar para fortalecer el tratamiento de la evidencia digital” 55

Anexo 2: Entrevistas 61

2.1 Entrevista: Ab. Héctor Alvear con 10 años de experiencia trabajando en la fiscalía. Asistente del fiscal. 61

2.2 Entrevista: Fiscal Alex Xavier López Ávila con 15 años de experiencia trabajando en la fiscalía. Asistente del fiscal. Docente en Ecotec. 64

2.3 Entrevista: Perito Argentina Pamela Ramírez sobre material de abuso sexual infantil (MASI). 8 años en el gabinete de análisis multimedial. 67

2.4 Entrevista: Perito Ecuatoriano Mario de la Cruz. Trabaja en todas las áreas de la criminalística. 70

2.5 Entrevista: Ab. Jhozman Yánez Trabaja en todas las áreas de la criminalística. 73

2.6 Entrevista: Perito Orly Cedeño. Trabaja en Audio, video y afines. 75

Anexo 3: Glosario 78

Anexo 4: Consulta de procesos judiciales 79

1. CAPÍTULO I:

PLANTEAMIENTO DEL PROBLEMA

Introducción y Generalidades

1.1 Contexto histórico social del objeto de estudio

La evolución de la tecnología de la información y la comunicación (TIC's) ha transformado profundamente diversos aspectos de la sociedad ecuatoriana, impactando desde la economía hasta la seguridad. Este incremento trajo consigo ciertos beneficios, sin embargo, también se desarrollaron nuevas formas de criminalidad.

Los primeros casos de delitos informáticos en el país incluyeron fraudes electrónicos y el acceso no autorizado a sistemas informáticos. En la actualidad estos delitos mencionados han tenido un crecimiento exponencial. Según la Dirección de Estadística y sistemas de información de la Fiscalía General del Estado: "En el 2018, se consumaron aproximadamente 215 casos de fraude electrónico y en julio del presente año se han consumado 520 casos. Mientras que, en el 2018 se consumaron 235 casos del delito de acceso no autorizado a sistemas informáticos y en julio del presente año ya se han consumado 486 casos."

Estas primeras manifestaciones de cibercriminalidad han destacado la necesidad de contar con protocolos y estándares adecuados para el tratamiento de evidencia digital, así como con profesionales capacitados en informática forense. La evidencia digital juega un papel crucial en la investigación y resolución de delitos modernos. Sin embargo, su naturaleza intangible y su susceptibilidad a la manipulación y deterioro plantean retos significativos para su manejo adecuado.

En Ecuador, el marco legal y procedimental para el tratamiento de evidencia digital aún se encuentra en proceso de desarrollo, y es indispensable contar con una guía auxiliar que estandarice y mejore las prácticas actuales. Esta necesidad se vuelve imperativa dada la creciente incidencia de delitos cibernéticos y el uso de tecnologías avanzadas por parte de los delincuentes.

1.2 Antecedentes

En nuestro país, como es de conocimiento la incidencia de delitos informáticos ha mostrado un aumento significativo en la última década, debido al acceso ilimitado a internet y a las diferentes tecnologías. Los delitos cibernéticos han evolucionado y se han convertido en acciones más complejas, por lo que, el estado ecuatoriano ha respondido con la creación de unidades especializadas y la implementación de marcos legislativos, como la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y más recientemente, la Ley Orgánica de Protección de Datos Personales.

El incremento en el uso de internet y dispositivos móviles en Ecuador ha sido un factor importante en el aumento de delitos informáticos. Según datos de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), el acceso a internet en el país ha aumentado significativamente, lo que ha facilitado tanto las actividades legítimas como las ilícitas en el ámbito digital. Esta conectividad ha provocado que, si no se tiene el debido cuidado, las personas sean más vulnerables a amenazas como el phishing, el ransomware, robo de identidad y fraude electrónico.

Actualmente, el marco normativo legal en Ecuador, para el manejo de evidencia digital está en proceso de evolución. Sin embargo, existe una necesidad urgente de consolidar y estandarizar las prácticas a través de una guía auxiliar que sea accesible y práctica para los profesionales del derecho, forenses digitales y fuerzas de seguridad.

Sin embargo, la eficacia en la resolución de estos delitos en los tribunales ecuatorianos, dependen de un adecuado manejo de la evidencia digital. La integridad, autenticidad y cadena de custodia de la evidencia digital son fundamentales para su admisibilidad en los tribunales y para asegurar que se haga justicia.

1.3 Planteamiento del problema

En Ecuador, a partir de la pandemia por Covid-19, existe un incremento exponencial en la proliferación de casos que involucran delitos cibernéticos o informáticos. La pérdida o alteración de la evidencia digital, constituye un gran problema debido a la naturaleza volátil de la información extraída de los diversos dispositivos electrónicos, donde puede ser el nexo causal entre el agresor y la víctima, el mismo que puede resultar en la absolución de individuos culpables, perjudicando la confianza en el sistema judicial y permitiendo la impunidad en los delincuentes cibernéticos.

El mal tratamiento de evidencia digital puede darse por errores en cadena de custodia o los limitados recursos tecnológicos del país. Por otra parte, la insuficiencia de protocolos actuales para la recolección, preservación y análisis de evidencias digitales no están adecuadamente adaptados para abordar las particularidades de estos fenómenos delictivos.

1.4 Pregunta científica

¿Cómo fortalecer el protocolo del Registro Oficial N° 318 en el tratamiento de evidencia digital en Ecuador?

1.5 Objetivos

1.5.1 Objetivo General

Elaborar una guía auxiliar para fortalecer el tratamiento de evidencia digital en base al Registro Oficial N° 318, tomando en consideración los estándares internacionales y la aplicación de la norma ISO 27037.

1.5.2 Objetivos Específicos

1. Identificar las similitudes y diferencias entre el Registro Oficial N° 318 y los estándares internacionales para el tratamiento de evidencia digital.
2. Definir los elementos clave de la guía para el tratamiento de evidencia digital a través de revisión bibliográfica.
3. Comparar la propuesta de una guía auxiliar en el tratamiento de evidencia digital mediante el análisis de casos de estudio de grooming en el Ecuador.

1.6 Justificación

El presente trabajo se realiza como un aporte práctico a la Criminalística en la rama de los Ciberdelitos. La evidencia digital presenta características únicas que la distinguen de la evidencia física tradicional. Su naturaleza volátil, la facilidad con que puede ser alterada, manipulada y pérdida puede presentarse en la diversidad de formatos que plantean retos específicos en su tratamiento.

El desarrollo de una guía auxiliar para el tratamiento de evidencia digital en Ecuador se justifica por varias razones indispensables. En primer lugar, la guía proporcionará la unificación de criterios e información útil que facilitará la capacitación y el desempeño de los profesionales involucrados en la cadena de custodia de la evidencia digital dentro de la escena del crimen.

En segundo lugar, la adopción de mejores prácticas y procedimientos estandarizados contribuirá a la integridad y confiabilidad de las pruebas presentadas en los juicios, asegurando la fiabilidad durante el proceso.

La falta de procedimientos estandarizados y claros puede comprometer la integridad y autenticidad de esta evidencia, afectando su admisibilidad como prueba en los procesos judiciales. Por lo que, decidimos investigar a profundidad sobre los manuales que se manejan de manera nacional e investigar sobre todos los protocolos y manuales internacionales para

poder realizar una guía auxiliar en el tratamiento de la evidencia digital. Tenemos la meta de mejorar y fortalecer este proceso dada la gran cantidad de ciberdelitos en Ecuador.

1.7 Introducción

En la era digital, donde la información y las comunicaciones son predominantemente virtuales, la evidencia digital se ha convertido en un pilar fundamental para investigaciones criminales en todo el mundo (Casey, 2011).

En Ecuador, a partir de la pandemia del COVID-19 se ha manifestado una nueva escena del crimen, los delitos ahora usan las tecnologías de la información y la comunicación (TIC), revelando al mismo tiempo vulnerabilidades significativas para la Policía Nacional del Ecuador en cuanto a la gestión y preservación de la evidencia digital de los delitos informáticos (Zambrano Rendón, Loor Campúes, Zambrano Vera, & Párraga Vera, 2021).

La Policía Nacional de Ecuador indica que desde el 2020 hasta el 2022 se ha registrado un aproximado de 3183 delitos informáticos y va en incremento. Según Gonzalo García, jefe de la Unidad de ciberdelitos, indica que estos hechos delictivos ocurren porque actualmente las personas tienen mayor acceso a internet y redes sociales, por lo que, los delincuentes están aprovechando esta situación para delinquir mediante sistemas informáticos (El Comercio, 2022).

La Dirección de Estadística y Sistemas de Información pertenecientes a la Fiscalía General del Estado indica que desde el 2018 hasta el 11 de julio del presente año, se han consumado 150. 376 delitos informáticos en Ecuador, evidenciando un crecimiento exponencial entre los años 2021 y 2023.

Esta situación plantea un desafío crucial: ¿cómo asegurar la integridad y la admisibilidad de la evidencia digital en un entorno donde los protocolos adecuados son escasos o inexistentes?

En las prácticas investigativas desarrolladas, se evidencia la urgente necesidad de desarrollar una guía auxiliar para el tratamiento de evidencia digital. A través del análisis de casos y comparaciones internacionales, se busca identificar mejores prácticas y proponer recomendaciones concretas para fortalecer el sistema de justicia penal ecuatoriano en el contexto del tratamiento de evidencia digital.

2. CAPÍTULO II:

MARCO TEÓRICO

2.1 Evidencia digital

2.1.1 Definición

“Es un tipo de evidencia de naturaleza física, compuesta por campos magnéticos y pulsos electrónicos pueden ser recolectados y examinados con instrumentos y métodos especiales.” (Rosero, 2019 p. 21).

“Las pruebas digitales suelen ser intercambiables con las pruebas electrónicas, pero pueden utilizarse para referirse específicamente a información almacenada o transmitida en formato digital que sea relevante para una investigación o un asunto judicial.” (Alianza Estrategica Forense Internacional (IFSA), 2023)

Para salvaguardar cualquier tipo de escena es necesaria su protección, la primera persona que tome contacto con la escena, debe asegurarla con el fin de garantizar la integridad y las condiciones de los indicios. En el caso de los dispositivos digitales se deben mantener en su estado inicial y documentar si se encuentran encendidos o apagados. Luego, se prosigue con el levantamiento de huellas dactilares externas que se encuentren en la estructura del dispositivo, a continuación, se fija fotográficamente el indicio, se rotula y se embala para el traslado hacia los centros de acopio (IFSA, 2023).

La evidencia digital se considera a toda la información que sujeta a una intervención humana, informática y/o electrónica, tiene una procedencia de cualquier medio tecnológico como celulares, computadoras, cámaras de video digital, etc. Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales (Ministerio de Seguridad Argentina, 2021).

La evidencia digital se caracteriza por contener información volátil, anónima, duplicable, modificable o alterable y eliminable. Por lo cual, es fundamental que el proceso de extracción de información sea muy cuidadoso, dado que, si se realiza un procedimiento incorrecto existe el riesgo de que se pierda toda la información y no se mantiene la idoneidad del proceso forense (Hidalgo, Hidalgo, Yasaca, Hidalgo , & Aragadbay, 2020).

En cada medio digital o estructura informática, se encuentra información volátil y la extracción de esta, se convierte en evidencia digital. Algunos de los más conocidos son los siguientes (Rosero, 2019):

Medio Digital	Recurso	Evidencia
Computadoras de escritorio y personales	Discos rígidos internos (Disco duro)	-Archivos de log, cookies. archivos ocultos, navegación, spool de impresión, archivos temporales, archivos de

		SWAP, archivos comprimidos, archivos renombrados, archivos protegidos con contraseña.
Dispositivos con control de acceso	Pendrive 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, videos, sonidos, documentos.
Impresoras y Scanner	Tarjeta de memoria en scanner	Documentos.
Puntos de acceso de routers Wireless	N/A	Archivos de configuración.
Diskettes CD - DVD	N/A	Imágenes, videos, sonidos, documentos.
GPS-celulares	Memoria interna del dispositivo celular Tarjeta de memoria	SMS, WhatsApp, Telegram, fotos, emails, vídeos, notas de voz.

Tabla 1: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: (Rosero, 2019)

2.2 Admisibilidad de la evidencia digital

La evidencia digital, debe cumplir con ciertos requisitos mínimos de admisibilidad para poder ser presentada en un tribunal de justicia. Estos requisitos buscan asegurar su validez y utilidad probatoria ante la autoridad competente (Hidalgo, Hidalgo, Yasaca, Hidalgo , & Aragadbay, 2020).

El primer elemento es la autenticidad, se debe demostrar que la evidencia es real y surge en el lugar de hecho, o se encuentra relacionada con la respectiva diligencia de forma relevante. Además, que no exista alteración o manipulación en los medios tecnológicos originales comprobando su integridad que brinden mayor fuerza y solidez en el proceso judicial (Hidalgo, Hidalgo, Yasaca, Hidalgo , & Aragadbay, 2020).

El segundo elemento es la confiabilidad, hace referencia a la fiabilidad de la evidencia digital, debido a que su origen proviene de fuentes confiables y verificables que han seguido la respectiva cadena de custodia. Asimismo, es crucial que, al momento de recolectar y analizar los elementos potenciales de prueba, utilicen técnicas y herramientas adecuadas que brinden certeza del procedimiento efectuado (Hidalgo, Hidalgo, Yasaca, Hidalgo , & Aragadbay, 2020).

El tercer elemento es la suficiencia, indica que la información recopilada y presentada es suficiente para respaldar las conclusiones a las que se ha llegado en el caso. Es importante

recordar que debido a la insuficiencia de elementos probatorios se puede causar la dilación del proceso judicial (Hidalgo, Hidalgo, Yasaca, Hidalgo , & Aragadbay, 2020).

El cuarto y último elemento es la conformidad con las leyes y reglas de la administración de justicia, hace referencia a los procedimientos de tratamiento de evidencia digital por lo cual deben realizarse en conformidad con las leyes y reglamentos establecidos por las autoridades pertinentes (Hidalgo, Hidalgo, Yasaca, Hidalgo , & Aragadbay, 2020).

2.3 Principios de la evidencia digital

El tratamiento de la evidencia digital es una parte integral de la gestión de incidentes de seguridad, que permite entender la anatomía de los ataques internos y/o externos para desarrollar medidas correctivas y, en algunas ocasiones cuando es necesario, dar seguimiento a los procedimientos legales pertinentes (Ochoa P. , 2018).

Se encuentran establecidas cinco reglas que se encargan del tratamiento de la evidencia digital, esenciales a tener en consideración cuando se debe realizar la adquisición del indicio de forma adecuada; dichos principios, permiten conocer qué es lo que se puede hacer y lo que no se puede hacer cuando se trata con material digital (Ochoa P. , 2018).

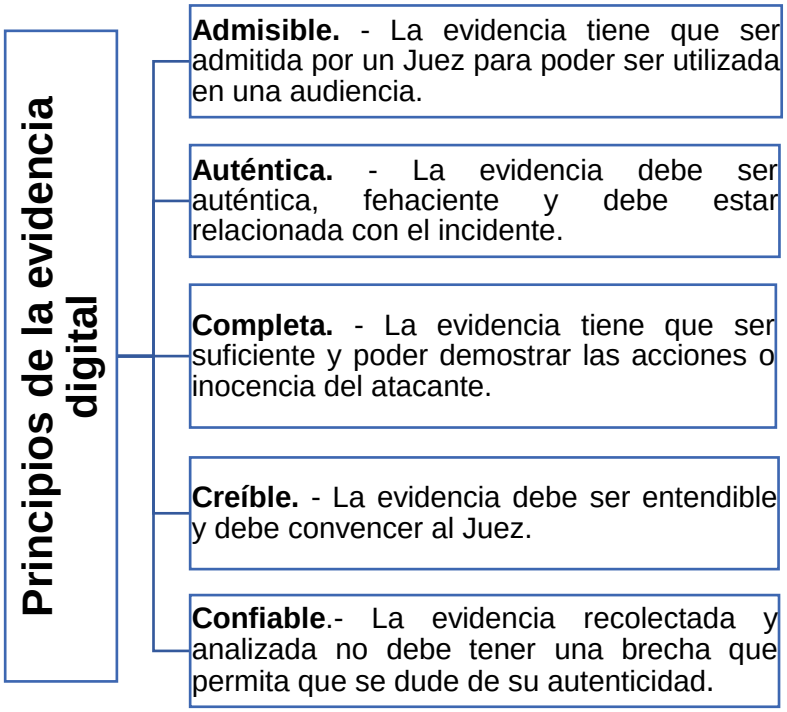


Gráfico 1: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: Ochoa P. , 2018

Los elementos potenciales de prueba digitales deben ser levantados con mucho cuidado, etiquetados y documentados de forma apropiada además de mantener la cadena de custodia en todo momento. Se recomienda que antes de realizar el análisis del dispositivo electrónico se realice una copia exacta de la evidencia original (Ochoa P. , 2018).

La siguiente guía cubre la fase de primera respuesta (Ochoa P. , 2018):

Documentación de la escena

- Se realiza la fijación fotográfica, escrita y planimétrica para recrear la escena del crimen. La documentación incluye la naturaleza de la evidencia, localización, posición de los equipos, etc.

Recopilación de la evidencia

- El levantamiento de evidencia adecuado, no permite la contaminación o daño de la evidencia. Se proporciona guías para el tratamiento de evidencia digital adecuado que no permita la contaminación o daño.

Preservación de la evidencia

- La preservación de evidencia digital, volátil por naturaleza, requiere un proceso embalaje especifico, debe estar etiquetado y documentado. Es fundamental que siempre se mantenga la cadena de custodia.

Gráfico 2: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: Ochoa P. , 2018

2.4 Análisis forense digital

El experto en análisis forense digital o informática forense, es un profesional especializado en seguridad informática y en la investigación de ciberdelitos, encargado de examinar dispositivos tecnológicos que pueden convertirse en pruebas sólidas que contribuyan en la decisión del Juez. La experiencia en informática forense engloba aspectos de software y hardware, redes, la seguridad, entre otros (Hidalgo, Yasaca, & Hidalgo , 2019).

Los expertos en análisis forense digital pertenecientes a la entidad gubernamental Interpol ofrecen a los países miembros, reuniones anuales internacionales de capacitación a expertos (INTERPOL, s.f.).

Desde el punto de vista pericial, se considera análisis forense digital a la aplicación de técnicas científicas y analíticas especializadas a una infraestructura tecnológica, la cual permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso judicial (Santos Tello, 2013).

La informática forense es una disciplina de la criminalística, en donde la policía científica enfocada en analizar los datos almacenados por medios electrónicos, extrae los datos de la evidencia, los transforman en información de utilidad operativa y presentan sus conclusiones en un informe (INTERPOL, s.f.). El procesamiento de los dispositivos electrónicos involucra varias etapas, iniciando con la adquisición del dispositivo, la preservación y el análisis. La etapa de análisis está enfocada en la recuperación de datos, el estudio de metadatos, empleando herramientas especializadas como FTK Imager y EnCase (Fruhlinger, 2019).

2.5 Análisis forense de audio y video

El análisis forense de audio y video es una disciplina de la criminalística. El análisis forense de audio, se enfoca en la identificación y análisis de las grabaciones de voz o sonido con el objetivo de obtener información relevante de una investigación criminal. Por lo que, se recopila diversas muestras de audio, mejorando la calidad de sonido y eliminando los ruidos para extraer características acústicas únicas del espectrograma de voz. El espectrograma será comparado con otras grabaciones para identificar similitudes y diferencias de las características acústicas y lingüísticas (Legalidad, 2023).

El análisis forense de video, se centra en examinar las grabaciones fotograma por fotograma para esclarecer un hecho delictivo e identificar a los sospechosos. En el análisis de las grabaciones se puede detectar que el video no esté manipulado, mejorar la calidad de la imagen y asimismo identificar detalles relevantes como rostros, matrículas de vehículos y otros elementos que permitan identificar (Quinto Huamán, 2020).

Este análisis comprende un estudio minucioso de imágenes y vídeos con el fin de esclarecer la autenticidad y el origen del contenido que se encuentre en el dispositivo del cual se esté realizando la pericia. Se utilizan técnicas específicas entre las cuales destacan: la fotogrametría, el análisis de movimiento y la interpolación de imágenes.

2.6 Incumbencias periciales

Las incumbencias periciales de informática forense y audio, video y afines que se llevan a cabo a nivel nacional son las siguientes (MANUAL DEL SUBSISTEMA DE INVESTIGACIÓN TÉCNICO CIENTÍFICA EN MATERIA DE MEDICINA LEGAL Y CIENCIAS FORENSES, 2022):

INFORMÁTICA FORENSE	AUDIO, VIDEO Y AFINES

✓ Peritaje de análisis y material del contenido digital, almacenado en fuentes informáticas, equipos, dispositivos y elementos de almacenamiento masivo de datos.	✓ Peritaje de análisis y material de archivos multimedia en dispositivos de almacenamiento digital, análogo y de sistemas embebidos.
✓ Peritaje para el estudio de sistemas de información, base de datos e infraestructuras tecnológicas.	✓ Peritaje para la transcripción de las emisiones lingüísticas de archivos de audio.
✓ Peritaje de análisis de código malicioso.	✓ Peritaje de descripción y/o categorización de objetos en archivos multimedia.
✓ Peritaje para el estudio de cuentas, clientes y servidores de correo electrónico con dominios corporativos o públicos.	✓ Peritaje de generación de fotogramas, secuencia de imágenes y descripción de acciones de archivos multimedia.
✓ Peritaje para el estudio y análisis de contenido digital registrado y publicado en sitios y páginas web.	✓ Peritaje para la determinación de la fidelidad, autenticidad e integridad de archivos digitales.
✓ Peritaje de análisis y material de datos almacenados en teléfonos celulares, tabletas digitales, teléfonos satelitales, sistemas de navegación GPS, smart watch, RPAS, y más tecnología digital de comunicación.	✓ Peritaje de análisis y materialización de archivos multimedia registrado y publicado en redes sociales, sitios y páginas web.
✓ Ejecutar la exhibición de contenido y evidencia digital almacenada en fuentes informáticas, equipos, dispositivos y elementos de almacenamiento masivos de datos en audiencia privada.	✓ Peritaje de mejoramiento digital de imágenes y videos.

Tabla 2: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: Manual de subsistema de investigación técnico científica en materia de medicina legal y ciencias forenses (2022)

2.7 Tratamiento de la evidencia digital según el Registro Oficial N° 318: Metodología en dispositivos encendidos y apagados

El registro oficial N° 318 es un documento que aborda varias disposiciones legales y normativas, entre ellas el tratamiento de indicios de todo tipo de naturaleza, en su acápite de la evidencia digital hace referencia a dispositivos encendidos y apagados, por lo cual nuestro proyecto enfatiza en un fortalecimiento del mismo a partir de una guía auxiliar del tratamiento de evidencia digital basada a la realidad ecuatoriana.

De acuerdo a lo establecido en el (SUPLEMENTO-REGISTRO OFICIAL N°318, 2014) se realiza lo siguiente:

Dispositivo apagado	Dispositivo encendido
Documentar descriptiva y fotográficamente los dispositivos y cables conectados al equipo, de acuerdo al instructivo.	Documentar descriptiva y fotográficamente los dispositivos y cables conectados al equipo, de acuerdo al instructivo.
Individualizar cada uno de los cables y dispositivos que almacenan información digital.	De ser necesario solicitar la ayuda de personal especializado con experiencia en captura y preservación de información volátil
Verificar si existen unidades de almacenamiento dentro de los dispositivos como CD, DVD, USB y otros	Desenchufar el cable o batería únicamente en los siguientes casos: • Si aparece en pantalla que el equipo fue borrado o formateado. • Si se observa que está en proceso de borrado o formateado el sistema de almacenamiento.
Registrar la marca, modelo, número de serie, y marcas distintivas del equipo.	No se debe desconectar la batería ni el cable de alimentación cuando: • La información que se muestra en la pantalla es de vital importancia para el proceso investigativo. • Si en la pantalla se muestran: salas de chats, redes sociales, comunicación interactiva, documentos encriptados, almacenamiento de datos remotos, documentos abiertos, considerado esto territorio digital Art. 460 numeral 8 COIP
Sellar con cinta de seguridad (cinta de evidencia) conectores de energía y puertos USB.	

Tabla 3: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: (SUPLEMENTO-REGISTRO OFICIAL N°318, 2014)

2.8 Tratamiento de evidencia digital según la OSAC

La Organización de los Comités del Área Científica de Ciencias Forenses también conocida por su abreviatura como OSAC, tiene como objetivo fortalecer el uso de la ciencia forense en el país a través de la publicación de estándares internacionales que contienen mejores prácticas, requisitos mínimos, protocolos estándar y terminología que promueven resultados forenses confiables, reproducibles y válidos.

Establece directrices rigurosas para el manejo de evidencia digital, asegurando su integridad y admisibilidad en procesos legales, y para lograr aquello también hace hincapié

sobre la constante capacitación hacia el personal experto forense sobre el uso de estas herramientas y métodos para garantizar que los datos sean recolectados y analizados de manera que sean válidos y confiables.

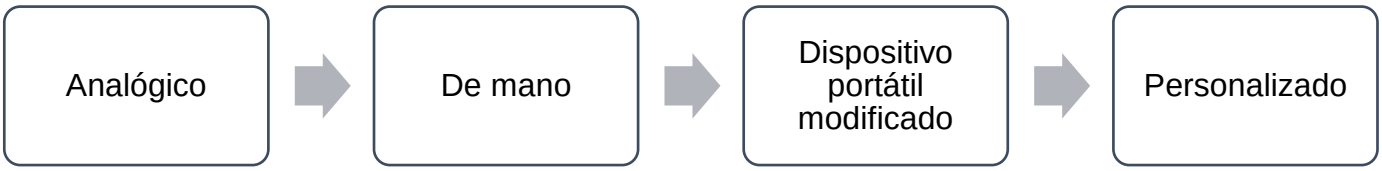
La OSAC fue creada en el 2014, con el trabajo conjunto del Departamento de Justicia de Estados Unidos (DOJ) y el Instituto Nacional de Estándares y Tecnología (NIST), buscando contribuir con sus aportes a la comunidad científica forense debido a la necesidad de establecer mejores prácticas y protocolos estándares. En la actualidad cuenta con aproximadamente 800 miembros que representan a los expertos en ciencia forense, investigadores académicos, gerentes de laboratorios, etc (OSAC, 2024).

El Registro OSAC hasta el 02 de julio de 2024, cuenta con 199 estándares de ciencia forense que involucran a disciplinas como balística, biología/ADN, antropología, investigación de la escena del crimen, odontología, toxicología, evidencia digital, entre otras disciplinas (OSAC, 2024).

La OSAC con respecto a la evidencia digital tiene 4 normas publicadas. El primer manual es sobre “Terminología estándar para el examen de la evidencia digital y multimedia”, es una recopilación de todos los términos y conceptualizaciones usados en el examen de evidencia digital y multimedia que incluye a la informática forense, análisis de vídeo, análisis de audio, análisis de imagen e identificación facial (ASTM-OSAC, 2019).

Se encarga de detallar diferentes terminologías y acrónimos de los documentos de referencia usados para la elaboración del manual mencionado. Las conceptualizaciones más fundamentales son las siguientes: La informática forense es el análisis científico de evidencia digital para asuntos legales; los datos volátiles son aquellos que se encuentran en un sistema activo y se pueden perder cuando el dispositivo se queda sin energía y la evidencia multimedia son los medios análogos o digitales como películas, cintas, medios ópticos y magnéticos que contienen información en ellos (ASTM-OSAC, 2019).

El segundo manual o norma es titulado “Práctica estándar para examinar lectores de tarjetas magnéticas” y trata sobre los “skimmers” que se usan con fines ilegales, también mencionan como realizar el proceso de adquisición y análisis del dispositivo. El skimmer es



usado con un propósito ilícito, es un lector de tarjetas magnéticas que obtiene el número de la tarjeta de crédito o débito, información del titular, el código CVV y el código CVV 2. Tiene 3 categorías que son (ASTM-OSAC, 2022):

Gráfico 3: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: ASTM-OSAC, 2022.

Al incautar este tipo de dispositivos hay que tener mucho cuidado en los siguientes casos (ASTM-OSAC, 2022):

Cuando dos equipos están unidos, uno que captura los datos del seguimiento de la tarjeta y el otro que por separado captura el PIN (puede ser por suposición de teclado o vídeo).

Si se observa una batería en el skimmer no moverla a excepción de que exista una demora significativa para el análisis.

Si el dispositivo está conectado a una bomba, es posible que este usando energía de la misma, no existirá inconveniente al desconectarlo.

Si el dispositivo usa una SD o una tarjeta de circuito integrado universal (UICC), está deberá ser retirada al momento de la incautación.

Si el dispositivo usa grabación de audio o video (a veces ambos) para capturar la información, está grabación puede seguir a pesar de que el aparato este incautado.

Es un desafío identificar estos dispositivos parásitos debido a que por su naturaleza de uso ilícito están diseñados para permanecer ocultos mientras extraen la información. La extracción de datos de los skimmers analógicos puede realizarse a través de modo de almacenamiento USB incorporado para adquirir la imagen forense usando las técnicas y procedimientos adecuados. En el caso de los skimmers digitales, se pasa en forma de onda de barrido analógica a un ADC que pueda producir una forma de onda digital la cual se pueda almacenar en un USB o memoria flash (ASTM-OSAC, 2022).

El tercer manual es titulado “Guía estándar para la instalación y el mantenimiento de laboratorios de audio forense” y se enfoca en el ambiente acústico de un laboratorio de audio forense como el conjunto de sonidos ambientales y factores que influyen (ecos, resonancias). Busca minimizar o eliminar las distracciones sonoras en el laboratorio las cuales pueden perjudicar la calidad del análisis de audio forense (ASTM-OSAC, 2023).

Asimismo, mencionan que es fundamental que el laboratorio se encuentre en una temperatura y humedad adecuada a las especificaciones de los equipos para la conservación y restauración de audio. También, la configuración del sistema en la disposición de los equipos, conectores, cables y software pueden interferir en la señal de audio (ASTM-OSAC, 2023).

Finalmente, el cuarto y último manual titulado “Requisitos mínimos para las herramientas de prueba utilizadas en análisis forense digital y multimedia”, recomienda requisitos mínimos que se deben tener en cuenta en condiciones operativas del análisis forense, la metodología a aplicar y determinar su validación o verificación. También, se enfoca

en las limitaciones de la investigación, debido a que, el documento no aborda variables como la velocidad del procesamiento, la facilidad de uso y si el personal se encuentra capacitado para usar estas herramientas de análisis forense (Scientific Working Group Digital Evidence (SWGDE), 2023).

Enfatiza sobre el adecuado uso de las herramientas forenses críticas y de adquisición. Las herramientas críticas son las interactúan directamente con la evidencia, algunas herramientas de preservación son los bloqueadores de escritura pueden ser de hardware o software y evitan cambios externos en la evidencia digital. Las herramientas de adquisición entre las que se puede obtener el cálculo Hash (MD5 y SHA1, etc.) (Scientific Working Group Digital Evidence (SWGDE), 2023).

2.9 Tratamiento de evidencia según el Manual de buenas prácticas en la escena del crimen de la AICEF

El "Manual de Buenas Prácticas en la escena del crimen" de la Academia Iberoamericana de Criminalística y Estudios Forenses (AICEF) establece una metodología general para el manejo de la evidencia, a diferencia del manual de la IFSA, este manual está dirigido para personal capacitado y no capacitado en lo que respecta al área forense.

El manual está enfocado en la necesidad de establecer protocolos estandarizados el cual pueda ser adaptados a diferentes contextos y situaciones, destacando la volatilidad y fragilidad de los potenciales elementos de prueba digitales. Es importante enfatizar la correcta preservación y tratamiento de la evidencia puede asegurar la integridad y trazabilidad de los indicios recolectados en el lugar de los hechos.

El tratamiento inadecuado de la evidencia en la etapa de levantamiento, puede llevar a la contaminación, pérdida, destrucción o daño de la evidencia; siendo una de las razones más comunes por las que no se pueden analizar en el laboratorio. Por ello, es fundamental aplicar las técnicas adecuadas y se evite consecuencias que impidan el análisis del material tangible (Academia Iberoamericana de Criminalistíca y Estudios Forenses (AICEF), 2010).

Las indicaciones del tratamiento de indicios o evidencias tomado del manual de la AICEF (Academia Iberoamericana de Criminalistíca y Estudios Forenses (AICEF), 2010):

• Se levanta toda la evidencia de valor significativo.
• La evidencia se categoriza de forma individual, dependiendo de su naturaleza, antes de realizar las fotografías respectivas.
• Se debe fotografiar la evidencia de forma precisa, tomando fotografías de conjunto, semi conjunto y de detalle. Importante que se reflejen los testigos métricos.
• La evidencia, se maneja sólo cuando es estrictamente necesario.

• Se colecta las evidencias de manera individual, teniendo en cuenta su naturaleza, evitando que se mezclen y se puedan alterar o dañar.
• Embalar la evidencia individualmente, asegurando que se preserve la integridad de su naturaleza. El embalaje se realiza siguiendo el procedimiento de la Unidad de Policía de su región.
• Cuando aparecen posibles señales de peligro físico o químico-biológico, se implementan medidas adecuadas de comunicación, aviso y protección para evitar el riesgo al que se expone el perito.
• El embalaje, debe estar etiquetado de forma adecuada, detallando toda la información de la evidencia. En este punto inicia la cadena de custodia de la evidencia.
• Evite contaminar la evidencia con las herramientas utilizadas para levantarla.
• Antes de embalar las evidencias húmedas, deben secarse a temperatura ambiente.
• Almacenar y conservar adecuadamente las evidencias colectadas.
• Para un adecuado tratamiento de evidencia, es muy importante el uso de elementos de bioseguridad que protegen contra los riesgos de contaminación cruzada.
• Alguno de los elementos de protección individual (EPI) que deben utilizar los profesionales son: guantes, mascarillas, gorros, gafas individuales, cubre zapatos, mascarillas con filtros, etc.

Tabla 4: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: Academia Iberoamericana de Criminalistíca y Estudios Forenses (AICEF), 2010

2.10 Tratamiento de evidencia digital según el Manual del International Forensic Strategic Alliance (IFSA)

La Alianza Estratégica Forense Internacional (IFSA) es una asociación multilateral entre redes regionales de laboratorios forenses operativos en todo el mundo, este manual de incumbencia pericial informática abarca directrices para el correcto manejo y procesamiento de evidencia digital. El manual proporciona el uso de métodos específicos para el análisis de diversos dispositivos y sus sistemas operativos.

Al mismo tiempo, brinda información a la comunidad de científicos sobre la preservación y cómo proteger los datos ante una pérdida, para un correcto análisis el manual informa sobre el uso de software forense validado para obtener los resultados esperados y, por ende, el informe final tenga la validez y fiabilidad del caso.

El proceso de recopilación de evidencia digital es identificar, preservar, adquirir, examinar, analizar; y realizar el Informe sobre evidencia digital (Alianza Estrategica Forense Internacional (IFSA), 2023).

“La evidencia electrónica consiste en datos generados o registrados en dispositivos electrónicos de muchas maneras. Los tipos de datos comunes que normalmente se identifican durante los exámenes de evidencia electrónica incluyen” (IFSA, 2023).

Los tipos de datos que incluyen son:

- Datos y metadatos activos/lógicos (estos son datos que son visibles para un usuario normal de un sistema.
- Metadatos de archivos integrados y metadatos de archivos/sistema operativo (esto incluye información sobre archivos almacenados por un sistema y puede incluir horas y fechas, ubicaciones y números de serie de hardware y software)
- Copias de seguridad
- Datos inactivos (eliminados)
- Datos volátiles (son datos que desaparecen cuando la computadora se apaga.)

Datos de telecomunicaciones (esto incluye el tráfico de red enviado y recibido como parte de la interacción de un sistema con Internet o intranet).

El analista forense digital, debe contar con documentación que certifique sus conocimientos y desarrollo profesional, así como tener la habilidad de ejecutar tareas sencillas del tratamiento de evidencia digital como la identificación, preservación, y levantamiento de la evidencia digital, adquisición de la imagen forense para la examinación, el uso del algoritmo hash para la validación de su autenticidad, la examinación de lo recopilado y la documentación de los hallazgos que puedan ser reproducibles (IFSA, 2021).

El software empleado para el material de audio y video permite mejorar sus condiciones cuando estas no son óptimas por ruido o la distorsión de la grabación de audio y video. El examinador debe explicar de manera detallada la metodología utilizada, su procesamiento y las limitaciones de la metodología al Juez (IFSA, 2023).

La evidencia digital posee ciertos elementos que la convierten en un desafío para los expertos investigadores como su naturaleza volátil, el anonimato, la facilidad para duplicarla, su naturaleza alterable o modificable y finalmente la susceptibilidad de ser eliminada (IFSA, 2021).

El análisis de la evidencia digital, se realiza una vez que se ha identificado la relevancia y el posible valor probatorio de los datos adquiridos o almacenados en un dispositivo, se desarrolla un proceso de extracción diseñado para optimizar la recolección de evidencia. Es primordial tener en consideración el volumen de datos, asegurar la preservación de los mismos, y evaluar los riesgos asociados con la posible pérdida o destrucción de datos (IFSA, 2023).

2.11 Tratamiento de evidencia digital según el Manual de la ENFSI

La Red Europea de Institutos de Ciencias Forenses, estableció 4 manuales muy importantes para el tratamiento de la evidencia digital. El primer manual fue publicado en el 2015, en el que aborda el proceso de levantamiento, recolección, análisis y por último presentación en tribunal de la evidencia digital.

En este manual, se destaca que el personal técnico forense tiene la responsabilidad de garantizar el cumplimiento de algunos requisitos mínimos internacionales como: el compromiso de mantenerse en vigencia de los avances técnicos y procedimientos actuales, comprender que la evidencia digital tiene ciertos requisitos a cumplir para ser aceptados en un juicio, mantener su portafolio de los casos que involucran evidencia digital y el procedimiento que se ejecutó (European Network of Forensic Science Institutes (ENFSI), 2015).

También es esencial que el experto en informática forense, lea revistas, libros y artículos científicos sobre lo relacionado con evidencia digital para estar actualizado, informar a su equipo de trabajo sobre los problemas encontrados durante el análisis y como se los superó y por último ayudar al desarrollo de procedimientos los cuales se adapten a su realidad local (ENFSI, 2015).

Es fundamental que el personal técnico forense este informado sobre los procedimientos y técnicas de evidencia digital actuales debido a que la tecnología avanza todos los días (ENFSI, 2015).

Se mantiene un inventario en el que se registra cada equipo, dado que luego será analizado en el laboratorio forense. Los datos que se deben registrar son el fabricante, modelo, número de serie único; fecha de compra y puesta en servicio; ubicación de cada equipo; y estado de mantenimiento y verificación (calibración). Además, es fundamental que se deje un registro de cualquier dato encontrado en los procedimientos mencionados con anterioridad (ENFSI, 2015).

Los equipos que se registren en el inventario, se deben dividir en 3 tipos: sistemas autónomos con firmware incorporado, los equipos eléctricos/ electrónicos, por último, en hardware y software lo restante. Entre el primero y el último no se realizan distinciones dado que deben ser analizados y verificados en un laboratorio. Todos los equipos tienen una vida útil aproximada de 1-5 años, dependiendo de los laboratorios y se determina con criterios de fiabilidad, capacidad de actualización, facilidad de uso, conectividad y actuación (ENFSI, 2015).

En relación con otros manuales sobre el tratamiento de evidencia digital, coinciden en que las etapas del tratamiento de la evidencia digital son las siguientes (ENFSI, Noviembre 2015):

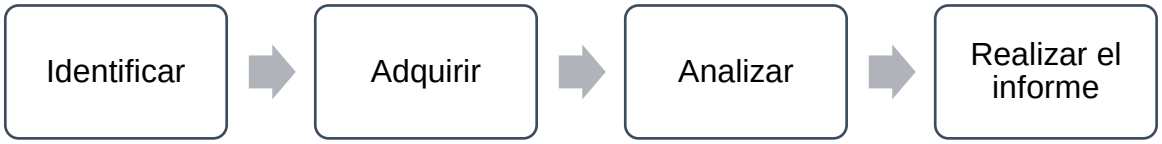


Gráfico 4: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: (ENFSI, 2015)

"Las buenas prácticas requieren una comprensión de los procesos seleccionados para realizar un análisis forense de la evidencia digital y el entendimiento del conocimiento por parte del destinatario del informe" (ENFSI, 2015). Un dato importante que lo diferencia del resto de manuales es que menciona el principio de incertidumbre, se debe tener en cuenta en todo el proceso, debido a que se puede generar en el software usado para analizar la evidencia digital que incluye las funciones forenses (instrumental y humana), identificación de equipos y elementos cifrados, adquisición de disco, redacción de informes y archivado (ENFSI, 2015).

El segundo manual de la ENFSI, publicado en el 2018, está enfocado en la imagen forense y en el análisis de la misma, también aborda la comparación facial, para que el contenido encontrado pueda ser presentado ante un Juez. Las limitaciones que presenta la incumbencia de comparación facial de imagen forense son el reconocimiento de rostros familiares, el uso de algoritmos automatizados para el reconocimiento facial, reconstrucción facial, progresión de edad en los rostros, origen étnico a través de las imágenes y arte forense (European Network of Forensic Science Institutes (ENFSI), 2018).

El análisis facial debe realizarse por profesionales expertos, quienes poseen una amplia gama de conocimientos y experiencia, se encargarán de comparar la imagen cuestionada con una imagen de referencia mediante un software que les permita procesar estas imágenes digitales. La observación e interpretación del observador es fundamental para el informe pericial, así como detallar los métodos de comparación ejecutados (ENFSI, 2018).

El análisis de imágenes y vídeos forenses se divide en 3 técnicas esenciales:

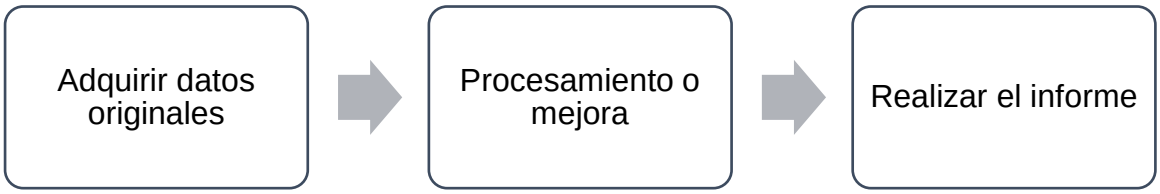


Gráfico 5: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: (ENFSI, 2018)

La experticia del analista forense digital, se ve reflejada al adquirir de manera adecuada la primera copia de imagen y vídeo analizando la estructura de sus datos y exportación. En el caso del procesamiento o mejora de los datos de imagen y video se utiliza un software forense que mejore la nitidez y disminuya el desenfoque de la imagen o video y a su vez permita identificar o vincular el contenido con la investigación. Finalmente, se realiza el informe proporcionando los resultados de la investigación, las técnicas, procesos adecuados respetando los parámetros legales (ENFSI, 2018).

Asimismo, se mantiene un registro de los componentes de cada equipo como el hardware de la computadora y software de sistema, el almacenamiento, sistemas de gráficos-códecs, dispositivos de salida gráfica como pantallas e impresoras y dispositivos de entradas gráficas como el escáner (ENFSI, 2018).

Por otro lado, el análisis de los metadatos y la verificación hash son relevantes para cotejar la procedencia de la información a examinar, todo debe ser debidamente documentado para evitar el surgimiento de duda sobre la autenticidad de los datos de la investigación (ENFSI, 2018).

La Red Europea de Institutos de Ciencias Forenses, publicó en el 2018, el Manual de mejores prácticas de imagen forense y mejora de vídeo corrigiendo el brillo, contraste, ajuste de enfoque, estabilización de vídeo y reducción de ruido. Este trabajo está destinado a expertos forenses que tienen como objetivo estandarizar sus métodos de trabajo, recalcando la necesidad de procedimientos consistentes y confiables para obtener resultados precisos los cuales sean reproducibles (European Network of Forensic Science Institutes (ENFSI), Junio 2018).

Intenta mejorar la calidad de la imagen o el video sin alterar su contenido inherente, manteniendo la integridad de la evidencia, para la recolección de imágenes y videos, asegurando que estos se mantengan en su estado original para evitar cualquier alteración involuntaria, además, mencionan técnicas avanzadas como la interpolación de imágenes y el uso de algoritmos de procesamiento digital para mejorar la calidad visual de las evidencias sin comprometer su autenticidad (ENFSI, Junio; 2018).

La validación y verificación de las técnicas mencionadas en el manual aseguran que los resultados sean confiables. Esto incluye pruebas rigurosas y comparaciones con métodos estándar para garantizar la calidad del trabajo forense (ENFSI, Junio; 2018).

El cuarto manual de la ENFSI, publicado en el 2021, está enfocado en las buenas prácticas para la autenticación de archivos digitales de imagen forense, utiliza 3 métodos como el análisis del contenido de la imagen, la estrategia, análisis de datos auxiliares y revisión de pares. En la estrategia se analiza su contexto, fuente, integridad y procesamiento, además se puede detectar si existe manipulación en la imagen (European Network of Forensic Science Institutes (ENFSI), 2021).

Con respeto a los archivos de imagen se pueden hallar metadatos que pueden usarse con fines de verificación o comparación en la autenticación de imagen, además estos datos sobre otros datos contienen información vital como el nombre del archivo, la ubicación del archivo, fecha, hora, coordenadas GPS (variable), tamaño, marco del dispositivo y modelo del dispositivo. Los formatos de imágenes más comunes son: JFIF(JPEG), TIFF, BMP, HEIF y PNG. Y describe los métodos para la recolección, almacenamiento y preservación de imágenes digitales, enfatizando la cadena de custodia y la integridad de los datos (ENFSI, 2021).

El análisis de contenido visual puede ser de ayuda cuando captura una escena real se pueden extraer los datos y compararlos usando un software validado en la comunidad forense. Se centra en identificar inconsistencias visuales, tales como sombras, reflejos, desenfoques y la presencia de objetos transparentes o reflectantes que pueden indicar manipulación (ENFSI, 2021).

2.12 Tratamiento de la evidencia digital según la norma internacional ISO/ IEC 27037:2012

Las normas ISO son un conjunto de normativas internacionales que fueron creados por la Organización Internacional de Estandarización. En específico la norma ISO 27037, está orientada al procedimiento de la actuación pericial para la obtención y recopilación de la evidencia digital que tienen valor probatorio. Debido a que fundamenta la validez y confiabilidad de la evidencia digital presentada en procesos judiciales (Organización Internacional de Estandarización [ISO], 2012).

A diferencia de las otras normativas, la norma internacional ISO/IEC 27037 enfatiza en que la evidencia obtenida sea válida y admisible en procesos judiciales. El documento destaca la importancia de una metodología sistemática que permita a los investigadores seguir un enfoque estructurado, minimizando el riesgo de alteraciones o pérdidas de datos.

Además, se recalca la necesidad de documentar cada paso del proceso, lo que incluye la cadena de custodia y las técnicas utilizadas, para asegurar la integridad de los indicios (ISO, 2012).

Se aplicará en diferentes dispositivos tecnológicos como equipos de almacenamiento y dispositivos periféricos, computadoras y dispositivos conectados a la red, dispositivos móviles, asistentes digitales personales (PDA), tarjetas de memoria, sistemas de navegación móviles, cámaras fotográficas y de video digitales (incluye CCTV), redes con conexiones TCP/IP y dispositivos con funciones similares a las mencionadas (ISO, 2012).

La evidencia digital consta de 3 principios fundamentales que son relevancia, confiabilidad y suficiencia. La relevancia es demostrar que la evidencia digital recopilada es relevante para la investigación y contiene información valiosa que ayudará a la resolución de la investigación, tiene que ser auditable y justificable ante el Juez. La confiabilidad es que cualquier proceso utilizado para el tratamiento de la evidencia tiene que ser auditable, reproducible y repetible. Para finalizar, la suficiencia hace referencia a que el primer respondiente a la escena tiene que haber reunido suficiente material para poder llevar a cabo la respectiva investigación y debe ser auditable y justificable (ISO, 2012).

Con relación al principio de relevancia, es crucial para recopilar evidencia digital que esté relacionada directamente con el caso de investigación. El principio de confiabilidad tiene la finalidad de garantizar de que la evidencia sea lo que pretende ser, es decir, que sea auténtica e íntegra. Y que los resultados de la aplicación de procesos de análisis sean reproducibles. El principio de suficiencia se refiere a que deben reunir suficiente material para poder ejecutar la investigación respectiva (ISO, 2012).

Existe 4 aspectos básicos en el manejo de la evidencia digital y son: auditable, reproducible, repetible, justificable en diversas circunstancias. En el caso del aspecto auditable es que se pueda evaluar y comprender el motivo de las tareas realizadas por el primer respondiente a la escena y el analista digital forense.

La reproducibilidad es la reproducción de los resultados bajo el uso de diversos instrumentos y condiciones, mientras que, el que sea repetible es la producción de los mismos resultados usando los mismos instrumentos y condiciones. Por otro lado, es justificable cuando el primer respondiente a la escena, puede probar sus acciones y métodos utilizados en el manejo de la evidencia digital, validando su actuación (ISO, 2012).

El procedimiento que mantiene este manual para el tratamiento de la evidencia digital es (ISO, 2012):

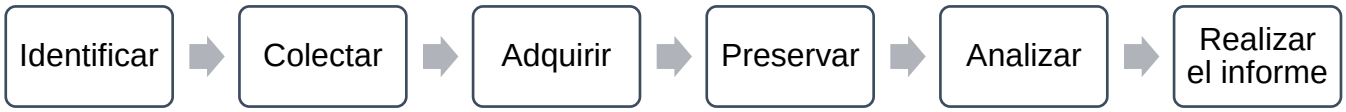


Gráfico 6: Elaborado por Doménica Robalino y Ruth Cordero. Fuente: (ISO, 2012).

El primer respondiente a la escena tiene la obligación de asegurar y proteger la ubicación de las posibles pruebas digitales, asegurando el área que contiene los dispositivos, determinando el responsable del lugar, fijar mediante fotografía y/o video la escena además de sus componentes digitales, documentar a todos los que tengan acceso al lugar, sobre todo debe verificar si el dispositivo está encendido no se lo apague y si está apagado no se lo encienda (ISO, 2012).

En la adquisición de la evidencia digital se debe maximizar la cantidad de datos recopilados, priorizando la naturaleza volátil de estas estructuras tecnológicas debido al potencial valor probatorio. Se recomienda ejecutar un software que permita obtener una imagen forense (bit a bit) de la información del posible hecho delictivo. La preservación implica proteger la evidencia digital recolectada y adquirida para asegurar que permanezca inalterada a lo largo del tiempo mediante un almacenamiento seguro, la documentación de su manejo y la implementación de controles de acceso adecuados para evitar su manipulación no autorizada (ISO, 2012).

En su contenido resalta a 2 figuras: el primer respondiente de la evidencia digital en inglés Digital Evidence First Responder (DEFR) y el especialista en evidencia digital en inglés Digital Evidence Specialist (DES). La primera figura es la del primer respondiente de la evidencia digital (DEFR), todas las organizaciones tienen un experto que está autorizado y habilitado para la actuación de una escena del crimen en la cual la evidencia digital sea parte del material probatorio (ISO, 2012).

La segunda figura es el especialista de la evidencia digital (DES), lo podríamos denominar perito informático, tiene las mismas habilidades que el primer respondiente, sin embargo, cuenta con habilidades y conocimientos específicos sobre equipos tecnológicos y procesamiento de evidencia digital (ISO, 2012).

Para concluir, la norma ISO/IEC 27037:2012 aborda varios escenarios sobre el tratamiento de la evidencia digital de manera técnica y sistemática, manteniendo su integridad y valor probatorio, causando que aumente su admisibilidad en proceso judiciales (ISO, 2012).

2.13 Cibercrimen/ Delito informático

2.13.1 Definición

En relación con las ciencias forenses, el delito informático se define como un “acto u actuación humana culpable ejecutado mediante el uso de herramientas informáticas, que vulnera bienes jurídicamente protegidos, y que se encuentra regulado y penado en la norma jurídica”. Se ha clasificado como un delito moderno y/o delito nuevo que se comete empleando dispositivos tecnológicos (Narvaez Montenegro, 2015).

Desde el punto de vista histórico - informático, la terminología del delito fue adaptándose al desarrollo de los equipos tecnológicos como de sus sistemas operativos, los entornos virtuales y a la evolución de la sociedad se determinaron nuevas y avanzadas formas de infracciones cometidas en el ciberespacio. Así, en el año de 1970 se introdujo el término delito informático, y fue acuñado por primera vez por el académico D.B. Parker (1976, citada en Holt y Bossler 2016) para referirse al mal uso de las computadoras (Ochoa A. , 2021)

La definición de cibercrimen depende del alcance de la legislación interna que tipifique aquellas infracciones, como también del avance del tratamiento jurídico a las conductas que utilicen estas herramientas para violar cualquier tipo de derecho. Los delitos pueden ser de distinta índole desde el robo de datos, manipulación, extorsión, fraude hasta daño o intromisión a sistemas (Ochoa A. , 2021).

El delito informático o ciberdelito es una forma infringir adquiriendo información y/o datos personales del ciberespacio, daños patrimoniales tanto personales como empresariales, producidos por el abuso de datos extraídos. Estos delitos cibernéticos tienen una naturaleza transfronteriza por el territorio donde se desarrollan con el objetivo de provocar filtraciones de información, datos bancarios, personales (Acosta, Benavides, & García, 2020).

2.13.2 Tipificación de los ciberdelitos

En cuanto a la diversidad de los delitos informáticos existentes, entre los más conocidos se incluyen:

El fraude informático, el espionaje informático, el sabotaje informático y el acceso no autorizado a sistemas de información, robo de software y robo de servicios (Chávez, 2022).

El fraude informático hace referencia a las distintas maneras en las que se obtiene información personal, datos bancarios con finalidad ilícita; así como la modificación y/o manipulación no autorizada, suplantación de identidad. Emplea elementos el phishing, troyanos, etc (Alvear Chalco, 2020).

El espionaje informático tiene como finalidad publicar o ventilar datos que una empresa o institución gubernamental y no gubernamental prefieren mantener con carácter reservado (Alvear Chalco, 2020).

El sabotaje informático es modificar, alterar o suprimir información, archivos o programas de los equipos que tiene como finalidad impedir el funcionamiento normal. En ocasiones, se emplea para causar conmoción o desestabilizar a un país o entidad. Para lograrlo se aplican elementos como virus, bomba lógica o cronológica, gusano, etc (Alvear Chalco, 2020).

El acceso no autorizado a sistemas de información hace referencia al ingreso ilícito a sistemas electrónicos protegidos, que busca alterar, modificar o interceptar estos archivos, como el uso de las llamadas “puertas falsas” (Alvear Chalco, 2020).

El robo de software está relacionado con la piratería y a la distribución ilegitima de un software que tiene otro propietario (Alvear Chalco, 2020).

El robo de servicios son las acciones ilegítimas de una persona que manipula un sistema para tener acceso a un servicio digital, aprovechar de manera ilegal los recursos y se facilita el acceso a un tercero (Alvear Chalco, 2020).

2.14 Cadena de custodia

“La cadena de custodia es el conjunto de procedimientos que buscan garantizar la adecuada preservación de los indicios encontrados en el lugar de los hechos; durante todo el proceso investigativo, y en la etapa del juicio, este procedimiento servirá como prueba que determinará la responsabilidad o inocencia del acusado.” (Fiscalía General del Estado, 2014)

La cadena de custodia no es nada más que, los procesos que conlleva a una correcta preservación y tratamiento de indicios desde que son levantados en la escena hasta su traslado a los laboratorios para su análisis, para que no se altere la integridad de los mismos (Fiscalía General del Estado, 2014).

El personal multidisciplinario del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses a nivel nacional, son los responsables de la cadena de custodia de todos los indicios y/o evidencia que son ingresados en el Centro de Acopio

temporal o definitivo y las maniobras procedimentales de cadena de custodia, a fin de asegurar su autenticidad e integridad (Fiscalía General del Estado, 2014).

2.15 Grooming

La etimología Child Grooming proviene, del verbo “to groom” que significa “preparar” o “entrenar a alguien para algo”, para un futuro rol o función. Actualmente, la acción “to groom”, ha adquirido un significado jurídico-penal, cuando un adulto está atraído sexualmente hacia los niños. En este sentido, al ser un delito de peligro concreto, el sujeto activo (indeterminado), prepara, embauca o seduce a los menores por medios telemáticos o electrónicos para fines sexuales (Feijoo, Tipan, & Rodriguez, 2020).

El grooming se refiere al conjunto de estrategias que una persona utiliza para establecer una relación de confianza con un menor de edad a través de engaños, usando las TIC´S (Tecnologías de información y comunicación) con el objetivo de obtener favores sexuales o imágenes de índole sexual. El sujeto activo, usa las redes para captar de forma rápida a las víctimas en páginas de juegos, redes sociales, salas de chat, etc (Mirarchi, 2019).

2.15.1 ¿Cómo se configura el delito del child grooming?

En el Código Orgánico Integral Penal (COIP), se configura el delito de Child Grooming o “Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos” en el artículo 173 (CÓDIGO ORGÁNICO INTEGRAL PENAL "COIP", 2014). Se detalla la comprensión del artículo 173:

En el primer inciso que se trata de un tipo penal básico, de delito en concreto, cuya sanción oscila dentro de un intervalo de uno a tres años de pena privativa de libertad. El segundo inciso es un subtipo agravado de resultado, que agrega elementos descriptivos, debido a que exige el “acercamiento” logrado mediante el empleo de “coacción” e “intimidación”. Su sanción oscila dentro de un intervalo de tres a cinco años de pena privativa de libertad (Feijoo, Tipan, & Rodriguez, 2020).

El tercer inciso, que menciona el artículo 173 es sobre la suplantación de identidad, falsificación y uso de documento falso, con material de niños menores a dieciocho años y/o discapacidad. Acto que, en caso de haberse ejecutado, tiene una sanción que oscila dentro de un intervalo de tres a cinco años de pena privativa de libertad (Feijoo, Tipan, & Rodriguez, 2020)

3. CAPÍTULO III:

MARCO METODOLÓGICO

3.1 Enfoque de la investigación

El enfoque adaptado para la investigación fue de carácter cualitativo. Este tipo de enfoque se centra en estudiar la complejidad de fenómenos sociales y humanos en una determinada situación. El análisis de los datos cualitativos es interpretativo y busca identificar patrones, temas y significados subyacentes (Piña-Ferrer, 2023).

La perspectiva cualitativa permitió explorar las prácticas actuales respecto a la evidencia digital mediante entrevistas a expertos y revisión bibliográfica de revistas científicas, guías y manuales de tratamiento de evidencia digital. La finalidad de la investigación que se realizó fue identificar las necesidades y proponer el uso de una guía auxiliar para mejorar la gestión del tratamiento de evidencia digital en el contexto ecuatoriano.

3.2 Tipo de investigación

El presente trabajo de investigación se clasificó en dos tipos principales: descriptivo y exploratorio.

Los estudios de alcance exploratorio se llevaron a cabo con el fin de examinar problemas de investigación poco estudiados o novedosos, sobre los cuales existen muchas interrogantes (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014). En cambio, los estudios de alcance descriptivo buscan describir situaciones, fenómenos y contextos, detallando cómo son y cómo se manifiestan (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014).

La investigación exploratoria se centró en una revisión exhaustiva de la literatura existente sobre el tratamiento de la evidencia digital, la cual, debido a su volatilidad, está expuesta a la pérdida y/o alteración de información. Este es un tema del cual se dispone de poca información en el país. Por otro lado, con el alcance descriptivo se pudo especificar y comprender por qué no se ha implementado una metodología adecuada para prevenir la pérdida y/o alteración de la evidencia digital.

Se llevaron a cabo entrevistas con peritos, abogados y fiscales involucrados en procesos investigativos inmersos en el área de ciberdelitos, con la finalidad de identificar los principales desafíos en el tratamiento de la evidencia digital. Además, se realizó un análisis de casos y una comparación de la literatura de textos importantes como el Registro Oficial 318, la norma ISO 27037, el manual de la AICEF, el manual ENFSI y el manual IFSA.

El alcance exploratorio y descriptivo de esta tesis permitió identificar y comprender las complejidades del tratamiento de la evidencia digital en Ecuador, así como describirlas detalladamente para desarrollar una guía auxiliar adaptada a la realidad ecuatoriana, destinada al tratamiento adecuado de la evidencia digital.

3.3 Período y lugar donde se desarrolla la investigación

Esta investigación se desarrolló en el Ecuador en un periodo de ocho meses, mismos que contemplaron septiembre, octubre, noviembre y diciembre del año 2023 y, mayo, junio, julio y agosto del presente año (2024).

3.4 Universo y muestra de la investigación

Las unidades de muestreo, también conocidas como "muestra", son los participantes del evento o situación que estamos investigando. El planteamiento y el alcance de la investigación dependen de ellos, ya que se recolectarán datos que deben definirse y delimitarse dentro de este subgrupo (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014).

Los sujetos a estudio se dividieron en diferentes categorías de acuerdo al método investigativo implementado. Se realizaron entrevistas para profundizar en los mismos. Para las entrevistas, la muestra de estudio es direccionada a personas encargadas del sistema legal judicial como:

Abogado Héctor Vladimir Alvear Chalco, con 10 años de experiencia trabajando en la fiscalía como agente del fiscal.

Fiscal Alex Xavier López Ávila con 15 años de experiencia trabajando en la fiscalía como agente fiscal y docente en la Universidad Tecnológica Ecotec.

Perito Pamela Ramírez, proveniente de Argentina, 8 años de experiencia en el gabinete de análisis multimedial sobre material de abuso sexual infantil (MASI).

Perito Sargento Mario de la Cruz, experiencia en todas las áreas de la criminalística, actualmente trasladado al departamento de criminalística Riobamba.

Perito Sargento Orly Miguel Cedeño Anchundia, sargento de la policía nacional del Ecuador, perito en el área de audio, video y afines.

3.5 Procesamiento y análisis de información

Una vez realizada la debida recolección de datos a través de las entrevistas, se procedió a examinar el caso del Mangajo, cuyo número de proceso según la fiscalía general del Estado es 1724320150004G, para evaluar las circunstancias y las dificultades durante el proceso investigativo respecto al tratamiento de la evidencia digital.

La entrevista de acuerdo a su formato es semiestructurada, se realizaron diferentes preguntas a cada experto, a continuación, se muestran las interrogantes realizadas:

ABOGADOS

- Usted ha tenido inconvenientes al presentar evidencia digital ¿cuáles?
- ¿Cómo se asegura de que la evidencia digital recolectada cumple con los requisitos legales para ser admitida en el juicio?
- ¿Qué pasaría en el caso de que la información del dispositivo electrónico se pierda por la demora en la emisión de una orden judicial?
- ¿Qué desafíos ha encontrado en la presentación de evidencia digital en los tribunales?
- ¿Cómo evalúa la capacitación actual de los abogados en el manejo y presentación de evidencias digitales?
- ¿Cómo se asegura de que las evidencias digitales recolectadas sean presentadas de manera comprensible y efectiva en los tribunales?

FISCALES

- ¿Cuántos casos ha procesado? ¿Cuál ha sido el resultado más común en estos casos (condenas, absoluciones, etc.)?
- ¿Qué estrategias utiliza para presentar la evidencia digital de manera efectiva ante el tribunal?
- ¿Qué tipo de pruebas digitales considera más cruciales en un caso de grooming?
- ¿Cómo coordina la recolección y análisis de evidencia con la policía y peritos informáticos?
- ¿Cuáles son los principales desafíos que enfrenta en la obtención y uso de evidencia digital en estos casos?
- ¿Qué protocolo sigue para asegurar la integridad de la evidencia desde su recolección hasta su presentación en juicio?

PERITOS

- ¿Cuál es su formación académica y experiencia profesional en análisis de evidencia digital?
- ¿Ha trabajado anteriormente en casos de grooming? Si es así, ¿cuántos y cuál fue su rol específico?
- ¿Cómo asegura la validez y precisión de los datos obtenidos?
- ¿Cómo se realiza el proceso de recolección, preservación y análisis de evidencia digital en casos de grooming en Ecuador?
- ¿Cuáles son los desafíos más comunes que enfrenta en el análisis de evidencia digital?
- ¿Qué protocolo sigue para asegurar la integridad de la evidencia desde su recolección hasta su presentación en juicio?
- ¿Qué mejoras considera necesarias en los protocolos de manejo de evidencia digital para fortalecer los procesos judiciales?
- ¿En Argentina también se espera la orden judicial para la extracción de información?
- ¿Ha realizado alguna extracción de información de consola de videojuegos?

Caso de estudio de grooming en el Ecuador: “El Mangajo”

J. Andrés Vintimilla Vega, alias “El Mangajo”, un cuencano de 36 años, acostumbraba a seducir a los menores con engaños y regalos. Vintimilla operaba a través de al menos cinco perfiles de redes sociales. En uno de sus perfiles aparecía con su verdadera identidad, en otro suplantaba y/o aparentaba ser un adolescente y en otro decía que tenía una pareja estable.

"El Mangajo” así como lo denominó la fiscalía general del estado con el número de proceso 1724320150004G, acudía a los colegios privados de Cuenca en búsqueda de sus víctimas, debido a que, este individuo pertenecía a la clase acomodada de la ciudad y deslumbraba a las adolescentes con regalos, autos de lujo y salidas costosas. Se esparció el rumor de que inició su vida delictiva entre las familias de la élite cuencana, debido a que no lo acusaban por vergüenza a lo que estarían expuestos. Desde ese momento cambió su grupo de interés a las estudiantes de las instituciones de educación públicas.

El Sr. Veintimilla se encargaba de documentar de sus víctimas todo mediante fotos y vídeos en su computadora y celular. En las redes sociales que manejaba demostraba su libertinaje, publicando fotografías de menores de edad con los uniformes de sus colegios, armas de fuego, ramo de billetes de cien dólares, bebidas alcohólicas e incluso tenía fotografías de menores de edad paradas en la pared con su mano en la parte baja de su espalda.

También le gustaba publicar sus últimas violaciones mediante una red anónima como Ask fm. Veintimilla, compartía respuestas a preguntas como “a quién desvirgó hoy”. Él respondía: no puedo decir, pero tiene 15 años. Su preferencia de víctimas son las mujeres menores de edad. Y con sus recursos se las arregló para que no lo atraparan pronto con medidas antiforenses como manipular las placas de su vehículo, tarjetas de SIM con números extranjeros para que no lo puedan rastrear.

Juan A. Veintimilla alias “El Mangajo” tiene cuatro condenas hasta el momento: dos por violación, una por pornografía infantil y otro por distribución de material pornográfico de niñas, niños y adolescentes (véase en el anexo 4). También tiene un proceso por tenencia de armas. Por estas sentencias deberá pasar 40 años en prisión. Además, tiene 10 denuncias en su contra y enfrenta en total seis procesos penales.

“Solo un año después de la detención de Vintimilla Vega, cuando la fiscal Ledesma ya estaba a cargo del caso, el teléfono de Martina fue analizado. Pero la mayor parte de las pruebas se habían perdido. Arizaga dice que esto sucede porque los celulares se ponen en modo avión y al estar más de un año en cadena de custodia, y sin actualizar las aplicaciones, todo los mensajes y fotografías enviadas a través de las aplicaciones, desaparecen.”

3.6 Métodos empleados

En el presente proyecto hemos realizado la correspondiente investigación y recolección de datos, se procedió a la utilización de métodos empíricos, tales como entrevistas semi estructuradas a expertos que por sus labores conocen directa o indirectamente el tratamiento de evidencia digital.

Para lograr los objetivos que se propusieron en este proyecto, en primer lugar, nos encargamos de buscar y descargar a través del internet el acuerdo ministerial 318, las normas ISO 27037 y los manuales del IFSA, ENFSI, AICEF, OSAC. Luego, se identificaron similitudes y diferencias sobre los manuales mencionados para el tratamiento de evidencia digital.

En segundo lugar, se definieron los componentes esenciales de las guías de tratamiento de evidencia digital, revisando diversos manuales que encontramos en internet.

Se verificó que los dividen en: la evidencia digital en dispositivos apagados, dispositivos encendidos; también consta un acápite de capacitación al personal.

Finalmente, en tercer lugar, comparamos la propuesta realizada por nosotras sobre la guía auxiliar en el tratamiento de evidencia digital, analizando el caso de grooming “El Mangajo” sobre el tratamiento de evidencia digital que se dio en el mismo.

4. CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Entrevistas

Se realizaron entrevistas a profesionales como abogados, fiscales y peritos con la finalidad de resolver un listado de interrogantes claves sobre el tratamiento de la evidencia digital en Ecuador.

En las entrevistas realizadas, la pregunta que trata sobre los desafíos que existe con respecto a la evidencia digital, los entrevistados indican que son diversos. En el que más coinciden es que las víctimas no quieren entregar el dispositivo que se debe analizar y eso complica el proceso de extracción de la información.

En otra pregunta tratamos sobre cómo se asegura que la evidencia digital cumpla con los requisitos legales para ser admitida en un juicio, todos los entrevistados respondieron que para lograr esto se debe respetar la cadena de custodia y ser muy minuciosos al detallarla y ejecutarla con los indicios digitales.

En la pregunta que cuestiona sobre el protocolo que se sigue para asegurar la integridad de la evidencia desde su recolección hasta su presentación en juicio, los entrevistados respondieron que se rigen bajo la cadena de custodia asegurando la integridad de cada uno de los indicios levantados en la escena.

Entre los principales desafíos que enfrentan en la obtención y el tratamiento de evidencia digital, los entrevistados concluyeron que debe asegurarse la integridad del indicio ya que al tratarse de un indicio digital consta de información volátil que puede perderse, cuando la evidencia digital está sobre grabada le resta fiabilidad al archivo y puede existir el desfase en la grabación, cuando no se emite la orden y la información puede perderse.

La interrogante acerca de las mejoras necesarias en los protocolos de tratamiento de evidencia digital para fortalecer los procesos judiciales, los expertos han coincidido en qué debe existir una cooperación interna en donde haya comunicación efectiva, mejorar el protocolo de cadena de custodia en donde el perito informático acuda al lugar de los hechos junto con el perito en criminalística y de esta manera realizar un trabajo en conjunto que permita un resultado falible. Así como es esencial que se permita realizar una imagen o copia forense de todo medio tecnológico por precaución.

4.2 Análisis e interpretación de resultados

El presente trabajo de titulación para la obtención del título de la licenciatura en Criminalística, propusimos el planteamiento de una guía auxiliar para el tratamiento de la evidencia digital, la cual fue realizada por Ruth Doménica Cordero Cedeño y Doménica Milena Robalino Macías. Se realizó una revisión de literatura exhaustiva del Registro Oficial 318,

manual de tratamiento de evidencia digital IFSA, AICEF, ENFSI, OSAC y las normas ISO/IEC 27037.

El manual del Registro Oficial 318 de Ecuador, detalló una normativa para el levantamiento y recopilación de la evidencia digital en investigaciones forenses. Este documento estableció procedimientos específicos para la identificación, recolección, preservación y análisis de datos digitales, con la finalidad de asegurar la integridad y validez de la evidencia en el contexto legal ecuatoriano. El documento detalló los protocolos que debían seguirse para la recolección de evidencia de diversos dispositivos digitales, cuando se encuentran en estado encendido y apagado.

El manual del IFSA, proporcionó una guía detallada sobre las prácticas en informática forense, enfocándose en la recolección, preservación y análisis de evidencia digital. Este documento destacó la importancia de implementar procedimientos estandarizados para garantizar la integridad de los datos durante todo el proceso de investigación.

El manual de Tratamiento de la Evidencia Digital según la norma internacional del AICEF (Asociación Internacional de Examinadores de Crimen Informático) ofrece directrices detalladas y procedimientos específicos para el manejo de la evidencia digital. Uno de los principios fundamentales del manual, es la rigurosa documentación de cada paso del proceso de manejo de la evidencia. Desde la identificación y recolección hasta la preservación y análisis

El manual del ENFSI de 2015 proporcionó una guía exhaustiva sobre las mejores prácticas en informática forense, enfocado en los procedimientos de recolección, preservación y análisis de evidencia digital. Este documento destacaba la importancia de seguir protocolos estrictos para garantizar la integridad de los datos y prevenir su alteración durante la recolección.

Además, se enfatizaba la necesidad de utilizar herramientas y técnicas validadas científicamente para llevar a cabo análisis forenses, con el fin de asegurar la fiabilidad y la reproducibilidad de los resultados obtenidos. El manual de 2018, se actualizó su manual para incorporar la comparación de imagen forense, mejorar su calidad de imagen y vídeo hasta la presentación del informe pericial en el tribunal.

El manual de la ISO/IEC 27037, ofreció una guía integral para la identificación, recolección, adquisición y preservación de evidencia digital. Este estándar fue diseñado para ayudar a los profesionales de la informática forense y de la seguridad de la información a manejar evidencia digital de manera adecuada y sistemática. Se detallaron procedimientos específicos para garantizar que la evidencia fuera tratada con integridad y se mantuviera su autenticidad durante todo el proceso de investigación.

El manual de Tratamiento de la Evidencia Digital conforme a la norma internacional OSAC (Organización de Ciencia Forense de los Estados Unidos), enfatiza la importancia de

una cadena de custodia ininterrumpida y bien documentada. proporciona un marco exhaustivo para el tratamiento de la evidencia digital, asegurando que los procedimientos sean realizados de manera profesional y estandarizada. La norma OSAC subraya la importancia de la capacitación continua para los profesionales forenses.

Además, analizamos un caso de grooming en el que existió perdida de evidencia digital por diversas eventualidades, las mismas que fueron tomadas en cuenta para ponerlas a prueba con la guía planteada, es decir, se hizo una comparación sobre que se hizo y que se debió hacer con la guía auxiliar para el tratamiento de evidencia digital.

5. CAPÍTULO V: PROPUESTA

5.1 Conclusiones

La presente investigación tuvo como propósito analizar la importancia de la evidencia digital en el contexto de los delitos informáticos en Ecuador, destacando su trascendencia para la resolución de casos aplicando un adecuado tratamiento de la evidencia digital. A través de un análisis detallado del Registro Oficial N° 318 y los estándares internacionales para el tratamiento de evidencia digital, se ha identificado elementos esenciales que deben incluirse en una guía práctica para el tratamiento de evidencia digital. Buscando que la guía propuesta no solo sea completa, sino adaptable a la realidad ecuatoriana.

Los hallazgos más significativos de esta investigación son la identificación de elementos esenciales que deben incluirse en una guía promoviendo así mejores prácticas en el tratamiento de la evidencia digital. Como la realización de la imagen o copia forense de todo dispositivo tecnológico, la obtención del cálculo hash y la adecuada realización de la cadena de custodia.

Se realizó la revisión bibliográfica de diversos manuales para la definición de los componentes que usamos en nuestra propuesta de guía auxiliar abarcando el alcance de la misma, las actuaciones fundamentales en la escena del crimen y en el laboratorio, así como también las limitantes que se presentan en el tratamiento de la evidencia digital.

Al analizar el caso de estudio sobre grooming en Ecuador, hemos observado cómo la implementación de la guía auxiliar puede transformar positivamente el tratamiento de evidencia digital promoviendo una extracción de información bajo los estándares internacionales ya estudiados.

Los resultados de este estudio indican que en Ecuador la gestión del tratamiento de evidencia digital es un desafío significativo como se mencionó en los hallazgos previos para hacerle frente a diversas dificultades como la pérdida o alteración de la evidencia digital, la falta de recursos y la necesidad constante de actualización de competencias debido a la evolución constante de las tecnologías de la información y comunicación.

Las limitaciones de esta investigación incluyen la disponibilidad de datos específicos y detallados sobre tratamiento de la evidencia en casos de delitos informáticos, así como la posibilidad de acceder a todas las instituciones y profesionales relevantes para entrevistas y encuestas al personal experto debido a procesos internos de su entidad gubernamental. Además, también está la rápida evolución de la tecnología lo que significa que se va a necesitar ajustes frecuentes para la guía y así se pueda mantener su vigencia y relevancia.

5.2 Recomendaciones

La dinámica del principio de intercambio en la evidencia digital no fue profundizada en la investigación actual. Al recolectar y analizar evidencia digital, es fundamental reconocer que cada interacción con un dispositivo puede alterar la información contenida. Por lo tanto, se recomienda que los profesionales peritos en informática forense utilicen herramientas forenses especializadas que permitan la captura de datos sin alterar el estado original del dispositivo.

El error humano, que puede resultar en la pérdida o alteración de datos cruciales, es uno de los mayores riesgos en el manejo de evidencia digital. Se recomienda implementar una serie de técnicas y procedimientos estandarizados para reducir este riesgo en un nivel moderado.

La capacitación continua del personal en el uso de herramientas forenses, el uso de manuales y protocolos sobre las mejores prácticas de manejo de evidencia y el uso de tecnologías automatizadas que reducen la necesidad de intervención manual son algunos de estos.

5.3 Propuesta

La propuesta en el presente proyecto es la creación de una guía auxiliar para el tratamiento de evidencia digital. Véase en el anexo 1 con mayor detalle.

6. Referencias y bibliografía

Bibliografía

Academia Iberoamericana de Criminalistíca y Estudios Forenses (AICEF). (2010). *Manual de buenas prácticas en la escena del crimen.*

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89). Obtenido de https://www.redalyc.org/journal/290/29062641023/html/

Alianza Estrategica Forense Internacional (IFSA). (2021). *Requerimientos mínimos para la investigación de la escena del crimen.* Obtenido de https://www.ifsa-forensics.org/wp-content/uploads/2021/11/IFSA-MRD-Crime-Scene-2021-Spanish.pdf

Alianza Estrategica Forense Internacional (IFSA). (2023). *Requerimientos mínimos para evidencia digital y multimedia.*

Alvear Chalco, H. (2020). CIBERATAQUE - CIBERGUERRA EN AMERICA LATINA Y SU AFECTACIÓN EN INSTITUCIONES DEL ESTADO ECUATORIANO. *(Tesis de Maestría).* Universidad Guayaquil, Guayaquil, Ecuador. Obtenido de https://es.scribd.com/document/516512640/Tesis-Alvear-Chalco-Hector-Vladimir

ASTM-OSAC. (2019). *Standard Terminology for Digital and Multimedia Evidence Examination.* E2916 − 19E1.

ASTM-OSAC. (2022). *Standard Practice for Examining Magnetic Card Readers.* E3017-19.

ASTM-OSAC. (2023). *Standard Guide for Forensic Audio Laboratory Setup and Maintenance.* E3150 − 18 .

Casey, E. (2011). *Digital evidence and computer crime: Forensic Science, Computers, and the Internet.* Baltimore, Maryland, USA: Elsevier Inc. Obtenido de https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf

Chávez, G. (2022). La penalización de los delitos informáticos en el COIP. *(Tesis de Magister en derecho mención derecho procesal).* UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL, Guayaquil, Ecuador. Obtenido de http://repositorio.ucsg.edu.ec/bitstream/3317/20177/1/T-UCSG-PRE-MDDP-144.pdf

El Comercio. (25 de Julio de 2022). 3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020. *El Comercio*. Obtenido de https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

European Network of Forensic Science Institutes (ENFSI). (2015). *Best Practice Manual for the Forensic Examination of Digital Technology.* Obtenido de http://www.enfsi.eu/

European Network of Forensic Science Institutes (ENFSI). (2018). *Best Practice Manual for Facial Image Comparison.* Obtenido de http://www.enfsi.eu/documents

European Network of Forensic Science Institutes (ENFSI). (2021). *Best Practice Manual for Digital Image Authentication.* Obtenido de http://enfsi.eu/wp-content/uploads/2022/12/1.-BPM_Image-Authentication_ENFSI-BPM-DI-03-1.pdf

European Network of Forensic Science Institutes (ENFSI). (Junio 2018). *Best Practice Manual for Forensic Image and Video Enhancement.* Obtenido de http://enfsi.eu/wp-content/uploads/2017/06/Best-Practice-Manual-for-Forensic-Image-and-Video-Enhancement.pdf

Feijoo, A., Tipan, S., & Rodriguez, D. (mayo de 2020). Child Grooming. *Perfil Criminológico-Fiscalía General del Estado*, 27. Obtenido de https://www.fiscalia.gob.ec/pdf/politica-criminal/revista-Perfil-Criminologico-julio-2020.pdf

Fiscalía General del Estado. (2014). *Protocolo del Centro de Acopio.* Obtenido de https://www.fiscalia.gob.ec/wp-content/uploads/2014/08/files_archivos%20AC_COIP%20073%20FGE_Area%20de%20Cadena%20de%20Custodia_14__Protocolo_del_Centro_de_Acopio.pdf

Fiscalía General del Estado. (2014). *SUPLEMENTO-REGISTRO OFICIAL N°318.* Quito, Ecuador. Obtenido de https://www.cienciasforenses.gob.ec/wp-content/uploads/downloads/2017/10/registro-oficial-318-MANUALES-PROTOCOLOS.pdf

Forenses, S. N. (2022). *MANUAL DEL SUBSISTEMA DE INVESTIGACIÓN TÉCNICO CIENTÍFICA EN MATERIA DE MEDICINA LEGAL Y CIENCIAS FORENSES.* Quito.

Fruhlinger, J. (23 de Marzo de 2019). *Computerworld.es*. Obtenido de https://www.computerworld.es/article/2127567/que-es-el-analisis-forense-digital.html

Fuentes Moreno, L. &. (2021). Infancia amenazada: Guerra cultural y erotización temprana. *Sexología y Sociedad*, 19.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodología de la Investigación.* México: McGRAW-HILL / INTERAMERICANA EDITORES.

Hidalgo, I., Hidalgo, B., Yasaca, S., Hidalgo , D., & Aragadbay, D. (2020). *Evidencias digitales en la investigación informática forense.* Escuela Superior Politécnica de Chimborazo (ESPOCH), Riobamba, Ecuador. Obtenido de http://cimogsys.espoch.edu.ec/direccion-publicaciones/public/docs/books/2024-01-22-174703-evidencias_digitales.pdf

Hidalgo, I., Yasaca, S., & Hidalgo , B. (2019). *EVIDENCIAS DIGITALES EN LA INVESTIGACIÓN FORENSE INFORMÁTICA.* ECUADOR-ESPOCH.

Hütt Herrera, H. (09 de Febrero de 2012). LAS REDES SOCIALES: UNA NUEVA HERRAMIENTA DE DIFUSIÓN. *Reflexiones, 91*(2), 121-128. Obtenido de https://www.redalyc.org/pdf/729/72923962008.pdf

INTERPOL. (s.f.). *Análisis forense digital*. Obtenido de https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital#:~:text=El%20an%C3%A1lisis%20forense%20digital%20es,datos%20almacenados%20por%20medios%20electr%C3%B3nicos.

Legalidad. (04 de Agosto de 2023). *Acústica Forense*. Obtenido de https://acusticaforense.com/analisis-de-voz-acustica-forense/

Lituma Díaz, D. S. (28 de February de 2023). *El Delito de Child Grooming en el Código Orgánico Integral Penal.* Recuperado el 29 de May de 2024, de Universidad de Cuenca: http://dspace.ucuenca.edu.ec/bitstream/123456789/41179/1/Trabajo-de-Titulaci%C3%B3n.pdf

Martin, A. (2021). *Análisis Forense de Imágenes.*

Massó, J. (23 de Enero de 2023). *Repasamos la historia de Internet.* Obtenido de Fundación iSYS: https://www.fundacionisys.org/es/blogs/social/sociedad/928-repasamos-la-historia-de-internet

Ministerio de Seguridad Argentina. (2021). *Protocolo de actuación para la investigación científica en el lugar del hecho.* Buenos Aires, Argentina. Obtenido de https://www.conicet.gov.ar/wp-content/uploads/anexo_6486329_1.pdf

Mirarchi, E. A. (2019). El Grooming: Un delito que vulnera el principio de proporcionalidad de la pena. Obtenido de https://repositorio.21.edu.ar/bitstream/handle/ues21/17970/MIRARCHI%20ELIZABETH%20ANDREA%20RITA.pdf?sequence=1

Mora, J. (4 de Agosto de 2023). *INTERNXT*. Obtenido de https://blog.internxt.com/es/tipos-de-ciberdelincuencia/

Narvaez Montenegro, D. B. (Abril-Junio de 2015). El delito informático y su clasificación. *Uniandes Episteme. Revista digital de Ciencia, Tecnología e Innovación, 2*(2), 158-173. Obtenido de https://www.redalyc.org/pdf/5646/564660011007.pdf

Nass de Ledo, I. (2019). LOS CINCUENTA AÑOS DE INTERNET. *Revista Venezolana de Oncología, 31*(3). Obtenido de https://www.redalyc.org/articulo.oa?id=375659062001

Ochoa, A. (2021). *Repositorio UASB.* Obtenido de https://repositorio.uasb.edu.ec/handle/10644/7919

Ochoa, P. (03 de Julio de 2018). *EL TRATAMIENTO DE LA EVIDENCIA DIGITAL, UNA GUÍA PARA SU ADQUISICIÓN Y/O RECOPILACIÓN*. Obtenido de Scielo: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2477-90752018000200035

Organización Internacional de Estandarización [ISO]. (2012). *Norma ISO/IEC 27037*. Obtenido de https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

OSAC. (12 de Julio de 2024). *National Institute of Standards and Technology (NIST)*. Obtenido de https://www.nist.gov/organization-scientific-area-committees-forensic-science/osac-registry

Piña-Ferrer, L. S. (Enero-Junio de 2023). El enfoque cualitativo: Una alternativa compleja dentro del mundo de la investigación. *Revista Arbitrada Interdisciplinaria Koinonía, 8*(15), Venezuela. doi:https://doi.org/10.35381/r.k.v8i15.2440

Plaza, A., Ramos, M., & Pascual, A. (2020). El Perfil del Consumidor de Imágenes de Abuso Sexual Infantil: Semejanzas y Diferencias con el Agresor offline y el Delincuente Dual. *Anuario de Psicología Jurídica, 30*, 9. Obtenido de https://www.redalyc.org/journal/3150/315062345003/315062345003.pdf

Quinto Huamán, C. (2020). Técnicas forenses y anti-forenses para el análisis de la integridad del contenido y de la fuente de adquisición en vídeos digitales de dispositivos móviles. *[Tesis Doctoral]*. Universidad Complutense de Madrid, Madrid. Obtenido de https://docta.ucm.es/entities/publication/9609c1ee-e1f6-4d83-ac56-0f599cbd9dd3

REGISTRO OFICIAL – SUPLEMENTO: Año I -Nº 180. (2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL "COIP"*. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

REGISTRO OFICIAL – SUPLEMENTO: Año I -Nº 180. (2014). *COIP*. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Revista Seguridad 360. (28 de Diciembre de 2021). *¿Cuáles son los tipos de delitos cibernéticos más comunes?. Recomendaciones para no ser víctima de la ciberdelincuencia*. Obtenido de https://revistaseguridad360.com/destacados/tipos-de-delitos-ciberneticos/

Rosero, D. S. (2019). 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. *(Tesis de Maestría).* Universidad Internacional SEK, Quito, Ecuador. Obtenido de https://repositorio.uisek.edu.ec/bitstream/123456789/3609/1/Tesis_David_Rosero_UISEK_Metodologia_Norma_ISO27037.pdf

Rouse, M., & Rosencrance, L. (11 de Abril de 2024). *¿Qué es internet?: Definición y conceptos clave.* Recuperado el 29 de Abril de 2024, de Techopedia: https://www.techopedia.com/es/definicion/internet

Scientific Working Group Digital Evidence (SWGDE). (2023). *Minimun Requirements for Testing Tools used in Digital and Multimedia Forensics.*

Zambrano Rendón, A., Loor Campúes, F., Zambrano Vera, W., & Párraga Vera, R. (2021). *Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López".* Obtenido de DELITOS INFORMÁTICOS EN TIEMPOS DE COVID: REVISIÓN LITERARIA ECUADOR: https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s3/CIV52EIT24.pdf

Anexos

Anexo 1: Propuesta "Guía auxiliar para fortalecer el tratamiento de la evidencia digital"

Propuesta de guía auxiliar en el tratamiento de evidencia digital

Alcance

La presente guía auxiliar está dirigida a expertos en la materia y a conocedores del tema. Se centra en la identificación, recolección, preservación y análisis para el tratamiento de la evidencia digital, basándose en dispositivos móviles, computadoras, consolas de juego, entre otros.

Asegurando que todos los profesionales manejen esta evidencia de manera efectiva, evitando la perdida, alteración o destrucción de evidencia digital; conforme a las mejores prácticas de los estándares internacionales aplicándolo a la realidad ecuatoriana.

Objetivo

El objetivo principal de esta guía es establecer un estándar de excelencia en el tratamiento de evidencia digital en Ecuador, asegurando que todos los profesionales involucrados en el proceso judicial cuenten con las herramientas y conocimientos necesarios para manejar esta evidencia de manera efectiva y conforme a las mejores prácticas internacionales.

HARDWARE

Hardware son los componentes físicos y tangibles de una computadora y sistema informático. Incluye cualquier parte del sistema que se puede palpar. Ej: disco duro, CPU, periféricos y memoria.

En la escena del crimen

En Ecuador, generalmente los primeros respondientes son la policía nacional urbana, tiene puntos importantes a tomar en cuenta:

1. Protección y preservación de la escena, en especial, la evidencia física como los dispositivos tecnológicos encontrados en la escena del crimen, asegurarse de llevar el instrumental necesario.
2. Observación meticulosa de la escena, identificar todos los dispositivos electrónicos en la escena tales como: computadoras, dispositivo móvil, disco duro, USB, etc.
3. Fijación de los equipos informáticos mediante fotografía, como el estado inicial del equipo (encendido o apagado), componentes y conexiones.

4. Si es un dispositivo móvil, se debe extraer la tarjeta SIM, si en una laptop o computadora de escritorio se extrae la memoria RAM. El dispositivo tecnológico no debe tener acceso a la red, al WI-FI y bluetooth.
5. Realizar la imagen forense o copia bit a bit de la información del equipo informático.
6. Obtener el Hash de la información que se debe extraer del equipo informático.
7. Recolección de indicios sin afectar la integridad del dispositivo.
8. En caso de que el dispositivo esté conectado a una red, anotar la dirección IP.
9. El embalaje del dispositivo debe realizarse en bolsas antiestáticas para casos de disco duro, celulares, USB. En caso de dispositivos más grandes se debe realizar en un contenedor resistente para evitar daños en su estructura.
10. El rotulado y etiquetado se realizará en cada dispositivo, conexión y componente. Se debe detallar quién, qué, cuándo y cómo se recolectó el indicio.
11. Realizar el respectivo formulario de cadena de custodia con cada indicio electrónico para su análisis y su traslado al centro de acopio correspondiente.

IMPORTANTE:

-Enviar peritos informáticos expertos a la escena para realizar la extracción de información de los dispositivos informáticos.

-Siempre el personal que ingrese a la escena del crimen debe contar con el instrumental respectivo y la protección de bioseguridad adecuada (usar guantes).

-La fijación no debe ser sólo fotográfica, también videográfica, escrita y planimétrica para que no exista duda sobre la pertinencia de la evidencia digital recolectada de la escena del crimen.

-Asegurar los equipos de terceras personas con la finalidad de evitar intervención física o electrónica de la evidencia digital.

-En caso de que una laptop no se apague cuando se desconecta, localizar y remover su batería para evitar el encendido accidental.

-Si existe un CD, Cinta, disquete u elemento de almacenamiento dentro del dispositivo electrónico, debe ser retirado con mucho cuidado y guardarlo en una bolsa de papel con el

rotulado respectivo. Luego, se procede a bloquear el acceso a esta parte el equipo, colocando una cinta de evidencia.

-Sellar cada entrada o puerto de información.

En el laboratorio

1. Verificar la integridad de los dispositivos y registrar cualquier anomalía presentada de manera documental y fotográfica.
2. Realizar copias bit a bit de los dispositivos originales utilizando software FTK Imager para análisis posterior, evitando la manipulación directa del dispositivo original.
3. Utilizar algoritmos hash (como MD5 o SHA-256) para verificar que las copias forenses son idénticas a los originales.
4. Utilizar el software forense para recuperar información relevante que haya sido eliminada.
5. Realizar el informe pericial acorde lo solicitado por la autoridad competente.

SOFTWARE

Es la parte intangible del dispositivo electrónico, es un conjunto de programas y procedimientos necesarios para que una computadora realice funciones específicas.

En la escena del crimen

1. Preparar el equipo y herramientas necesarias (hardware, software forense, medios de almacenamiento).
2. En caso que el dispositivo se encuentre ENCENDIDO, no debe ser apagado. Y si el dispositivo se encuentra APAGADO, no debe ser encendido, fijar mediante fotografía.

3. Si el dispositivo se encuentra en estado ENCENDIDO se debe realizar la captura de la memoria RAM usando herramientas como FTK Imager, también se debe obtener el HASH de la información que se extrae para esto se puede usar herramientas como MD5 y SHA-1.
4. Si el dispositivo se encuentra en estado APAGADO, se realiza un duplicado bit a bit del disco duro o de los medios de almacenamiento usando herramientas de imagen forense como EnCase. También se debe obtener el algoritmo HASH.
5. Documentar la estructura de los archivos y directorios del software, capturar el estado de las licencias y configuraciones de seguridad.
6. Asegurar que todos los dispositivos de almacenamiento estén etiquetados y en condiciones óptimas.
7. Almacenar los duplicados obtenidos en un medio de almacenamiento protegido con cifrado para mantener la confiabilidad de los datos recolectados.

En el laboratorio

1. Asegurarse de recibir la evidencia digital de forma adecuada según su naturaleza y verificar que este documentado con la cadena de custodia respectiva como quién la recolectó, la fecha y la hora de recepción.
2. Identificar los tipos de dispositivos y software que están involucrados, incluyendo sistemas operativos, consolas de juego, aplicaciones y dispositivos de almacenamiento.
3. Se define la diligencia que vamos a realizar según el objeto de pericia solicitado, para la extracción de datos específicos se verificará primero la integridad de la evidencia.
4. Utilizar herramientas forenses especializadas para adquirir copias bit a bit (imagen forense) de la evidencia digital. Asegurarse de que las herramientas sean compatibles con los sistemas y dispositivos involucrados.

5. Registrar todas las actuaciones realizadas durante la adquisición de la información de los dispositivos, incluyendo técnicas usadas, registros de actividad, fecha y hora y cualquier anomalía que se presente en el procedimiento.
6. Realizar análisis de la adquisición para detectar la presencia de malware o cualquier actividad maliciosa que pueda comprometer la integridad de la evidencia o el sistema.
7. Documentar todos los hallazgos en un informe pericial detallado, incluyendo la metodología utilizada, los resultados del análisis, las conclusiones y cualquier recomendación para acciones futuras. Siempre respetando el objeto de pericia.

IMPORTANTE:

-Guardar las copias de la evidencia y los informes forenses en un sistema de almacenamiento seguro y accesible solo para personal autorizado.

-Para la sustentación del informe pericial informático o de audio, video y afines, el perito debe estar preparado y estar seguro de lo que está informando usando un lenguaje claro para todos los presentes.

-La eliminación o destrucción segura de la información del dispositivo debe ser realizada cuando exista una autorización del Juez.

Limitantes

- En cada escena del crimen, lo ideal es que el perito experto en el área a la que corresponde la pericia acuda a la misma, para poder realizar el levantamiento de los indicios de una manera óptima.

- La contaminación de la escena es una gran limitante, ya que esto a su vez, lleva a la contaminación y/o alteración de los indicios, ya sea por factores ambientales, entrada de personas no autorizadas, etc.
- Recursos limitados respecto a equipos y tecnologías para el análisis de los indicios y el presupuesto que conlleva la adquisición de esos equipos.
- Falta de capacitación y actualización de conocimientos en nuevas técnicas y métodos del tratamiento de la evidencia digital.
- La ausencia de procedimientos estandarizados nacionales, puede llevar a inconsistencias en la recolección y manejo de la evidencia.
- La falta de claridad o actualización en las normativas y leyes relacionadas con los ciberdelitos y el tratamiento de evidencia digital puede interferir en la admisibilidad en los tribunales.

Anexo 2: Entrevistas

2.1 Entrevista: Ab. Héctor Alvear con 10 años de experiencia trabajando en la fiscalía. Asistente del fiscal.

Usted ha tenido inconvenientes al presentar evidencia digital ¿cuáles?

-Cuando el delito informático no es flagrante, sino que el denunciante se acerca a fiscalía a solicitar la investigación. Se presenta el inconveniente que no desea entregar el dispositivo electrónico (celular, laptop), debido a que teme que no se lo devuelvan y a su vez no lo considera fundamental dado que todo está en redes. Sin embargo, esta situación presenta un inconveniente fundamental para el análisis de la evidencia digital.

-También cuando la evidencia digital se “pierde” o desaparece antes del juicio.

- Cuando el perito, como acto de buena fe, realizó una copia o respaldo sin autorización del Juez.

¿Cómo se asegura de que la evidencia digital recolectada cumple con los requisitos legales para ser admitida en el juicio?

Se asegura la evidencia digital cuando se sigue de inicio a fin la cadena de custodia. Para periciar este tipo de delito se debe obtener una orden judicial que permita extraer la información. Incluye extracción de información de cámaras de vídeo, audios para evitar que se viole el derecho a la intimidad o privacidad.

¿Qué desafíos ha encontrado en la presentación de evidencia digital en los tribunales?

Cuando se extrae la información del dispositivo y se ha realizado la pericia respectiva. En el juicio, se exhibe la información en un proyector a los jueces. Si este dispositivo se pierde y alguien menciona que se realizó una copia, dan nulidad a la prueba.

¿Qué pasaría en el caso de que la información del dispositivo electrónico se pierda por la demora en la emisión de una orden judicial?

En estos casos, el perito informático debe detallar la información que ha encontrado y lo que no ha encontrado. Así mismo, el perito debe informar si por el paso del tiempo se volatizó la información.

-En Ecuador no existe la meta pericia, lo que se puede dar es una revalorización del peritaje.

¿Cómo evalúa la capacitación actual de los abogados en el tratamiento y presentación de evidencias digitales?

Considero que es complejo, en muchos casos no están actualizados sobre el proceso de la evidencia digital, sin embargo, tampoco buscan capacitarse.

¿Cómo se asegura de que las evidencias digitales recolectadas en casos de grooming sean comprensibles en los tribunales?

El perito debe expresarse en un lenguaje comprensible para el juez, explicando la terminología y el proceso que se ha realizado.

-Cada país tiene una realidad distinta, por lo que, en ocasiones los manuales internacionales no son admitidos en el juicio.

¿Cuántos casos de grooming ha procesado? ¿Cuál ha sido el resultado más común en estos casos (condenas, absoluciones, etc.)?

No existe un número aproximado, sin embargo, son muy pocas los que obtienen sentencia condenatoria.

¿Qué tipo de pruebas digitales considera más cruciales en un caso de grooming?

La información que se extrae de los dispositivos tecnológicos, mensajería instantánea, mensajes de voz. Se realizan pericias de audio y video y de las que se encarga el perito informático.

¿Cómo coordina la recolección y análisis de evidencia con la policía y peritos informáticos?

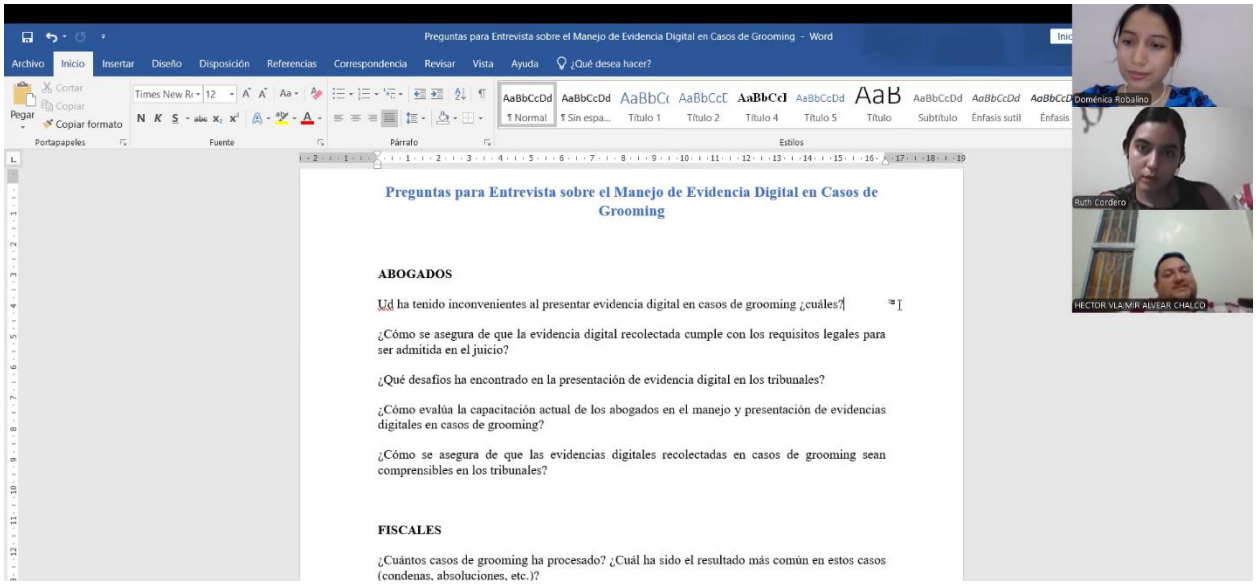
El fiscal, se coordina con ambos, dependiendo de la teoría del caso que mantenga y de la evolución de la investigación.

¿Qué estrategia utiliza para vincular al posible agresor con la evidencia digital obtenida?

Depende del fiscal, en ocasiones pueden tener sólo una prueba relevante. En casos de violencia sexual o física, el testimonio de la víctima es una prueba fundamental o de suma importancia.

¿Qué mejoras considera necesarias en los protocolos de tratamiento de evidencia digital para fortalecer los procesos judiciales?

Se recomienda mejoras interinstitucionales, es decir, cooperación interna entre las delegaciones fiscales en las que exista comunicación.



2.2 Entrevista: Fiscal Alex Xavier López Ávila con 15 años de experiencia trabajando en la fiscalía. Asistente del fiscal. Docente en Ecotec.

¿Cuántos casos de grooming ha procesado? ¿Cuál ha sido el resultado más común en estos casos (condenas, absoluciones, etc.)?

El grooming no es un delito formalmente tipificado, sino un medio de comisión del delito puede ser acoso, violación, hostigamiento, entre otros.

¿Qué tipo de evidencia digital considera más cruciales en un caso de grooming?

Es importante mencionar que existen 3 tipos de prueba según el COIP: testimonial, documental y pericial. En la prueba documental ingresa la evidencia digital que deben seguir una regla para ingresar al proceso. Y se extrae la información de dispositivos como tablets, celulares, computadoras, entre otros.

¿Cómo coordina la recolección y análisis de evidencia con la policía y peritos informáticos?

Primero se recolecta el dispositivo, luego de debe analizar el mismo respetando la cadena de custodia. También se debe enviar al agente investigador informático que tenga conocimientos más profundos de este tipo de evidencia.

Recordemos el artículo 456 establece lo que es la cadena de custodia, cada evidencia debe tenerla y ajustarse a sus parámetros, para que pueda ser considerada válida en un juicio, como realizar el código Hash. Y es la autenticidad de este tipo de información que fiscalía debe justificar, la evidencia debe ser recolectada en el lugar de los hechos y con las técnicas forenses e informáticas especificadas para este procedimiento. También la evidencia digital puede ingresar por cadena de custodia en fiscalía por flagrancia. Necesito este dispositivo, sino tengo este dispositivo no se puede proceder.

¿Cuáles son los principales desafíos que enfrenta en la obtención y el tratamiento de evidencia digital?

-Los principales desafíos que puedo indicar, es que no existe una base adecuada y completa para el cotejamiento de voces, debido a que sólo se emplea para personas detenidas y cuando el aparato se descompone no se puede seguir ingresando.

-También el proceso de tratamiento de evidencia digital debería ser mejor regulado, sería muy bueno que el experto informático sea quien extraiga la información de dispositivos en la escena del crimen.

-Tener en cuenta que muchos indicios digitales son asociativos que refuerza lo encontrado en alguna otra prueba, aquí se aplica otras técnicas de investigación como el seguimiento, la vigilancia, entre otras.

Usted ha tenido inconvenientes al presentar evidencia digital ¿cuáles?

En casos específicos de grooming no, sin embargo, si en otros casos que involucran evidencia digital.

-Los usuarios presentan chat que no guardan la cadena de custodia, lo que significa que no contiene autenticidad.

-En ocasiones también la cantidad de información es demasiada y el perito no alcanza a analizar toda la información. Y si demora mucho tiempo, la prueba puede tener nulidad.

-Cuando la víctima no desea dar los dispositivos para el análisis, dado que, se entrega cuando la cadena de custodia culmina bajo orden de la autoridad competente. Y recién se puede emitir la orden de devolución.

¿Qué protocolo sigue para asegurar la integridad de la evidencia desde su recolección hasta su presentación en juicio?

La fiscalía emite un protocolo de cómo se recolecta los indicios. No hay un protocolo especifico que este consolidado para este tipo de procedimiento.

¿Qué estrategia utiliza para vincular al posible agresor con la evidencia digital obtenida?

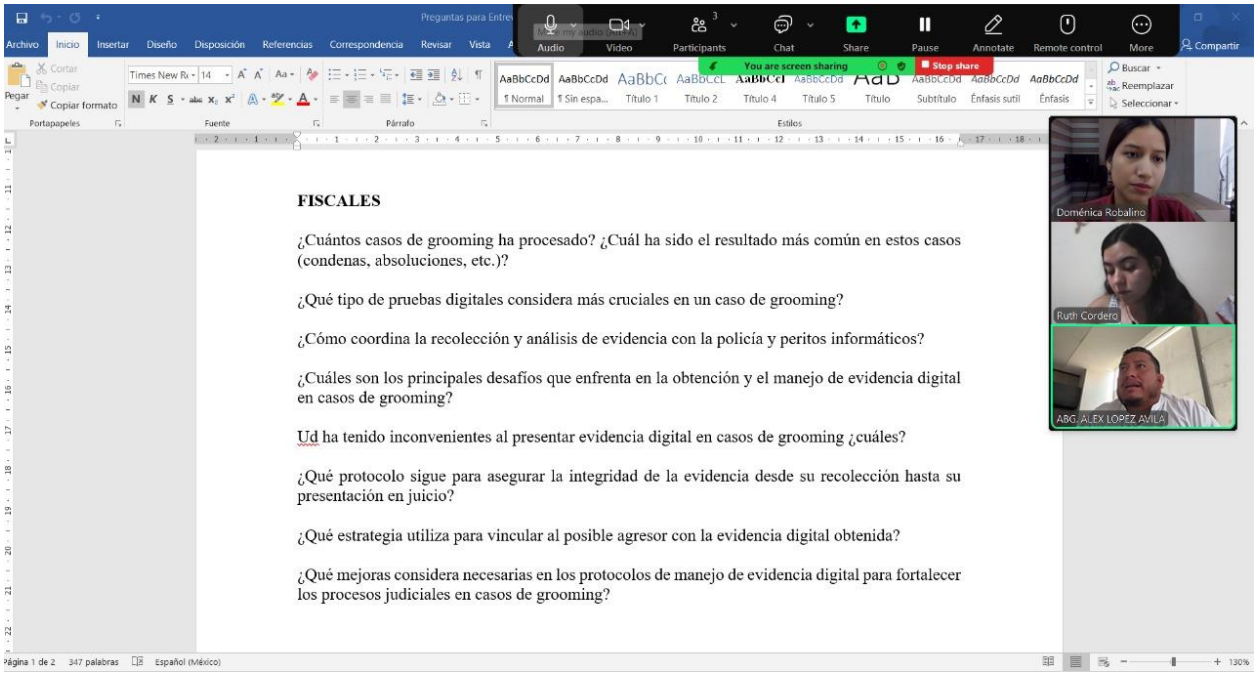
El fiscal buscará asociar el indicio con el posible agresor usando las versiones o testimonios sobre donde fue recolectado el elemento digital, tal vez en el momento de la aprehensión, la conexión de la evidencia digital con un email o número telefónico. También se puede reforzar esto con técnicas investigativas como seguimiento, vigilancia.

¿Qué mejoras considera necesarias en los protocolos de tratamiento de evidencia digital para fortalecer los procesos judiciales?

Mejorar los protocolos de tratamiento de evidencia digital, pero si recomiendo que el perito de criminalística este acompañado de un perito informático. Para que no lo realice el

policía de servicio urbano que en ocasiones no tiene conocimiento profundo sobre la adecuada recolección de la evidencia digital.

También manejar una misma línea de información e investigación, con un mismo protocolo de evidencia digital, para que no exista el inconveniente del litigio como que en Guayaquil no es lo mismo que litigar en Quito.



2.3 Entrevista: Perito Argentina Pamela Ramírez sobre material de abuso sexual infantil (MASI). 8 años en el gabinete de análisis multimedial.

¿Cuál es su formación académica y experiencia profesional en análisis de evidencia digital?

Estoy por finalizar mi licenciatura en criminalística, técnica en hemoterapia, actualmente labora en un gabinete de medicina legal donde se especializa en el análisis multimedia de material de abuso sexual infantil. Se especializa en cotejo morfo comparativo en imágenes basándose en la escala de tanner y la individualización de una persona.

¿Ha trabajado anteriormente en casos de grooming? Si es así, ¿cuántos y cuál fue su rol específico?

Sí, he trabajado en casos de grooming. Me tocó realizar el análisis de imagen para determinar si era menor de edad.

¿Cómo asegura la validez y precisión de los datos obtenidos?

Nosotros usamos un software (Amplifier) que tiene un mecanismo que permite todos los mejoramientos de una imagen como ampliación, focalización, etc. Este software es como una cadena de custodia dado que tiene una trazabilidad y hace un exporte en pdf que detalla todas las modificaciones realizadas a la imagen. Se puede obtener los metadatos al inicio y luego con el exporte en pdf, se aclara el proceso que se ha mantenido.

¿Cómo se realiza el proceso de recolección, preservación y análisis de evidencia digital?

Existe un área específica que es el laboratorio de informática forense, ellos se encargan de iniciar la cadena de custodia y usan para la extracción de información un aparato denominado UFED. Y mi gabinete de información analiza el material multimedia que se obtuvo de la extracción.

¿Cuáles son los desafíos más comunes que enfrenta en el análisis de evidencia digital?

Uno de los mayores desafíos es la individualización de la persona y determinar la minoría de edad en la víctima. Dependiendo de esto, siguen buscando otras evidencian que fundamenten la investigación.

¿Qué protocolo sigue para asegurar la integridad de la evidencia desde su recolección hasta su presentación en juicio?

Se sigue una cadena de custodia, toda evidencia digital debe tener el hash correspondiente que certifique autenticidad.

¿Qué mejoras considera necesarias en los protocolos de tratamiento de evidencia digital para fortalecer los procesos judiciales?

Se hace mucho hincapié en el proceso de cadena de custodia, dado que, si no es respetado se cae todo el proceso judicial.

¿En Argentina también se espera la orden judicial para la extracción de información?

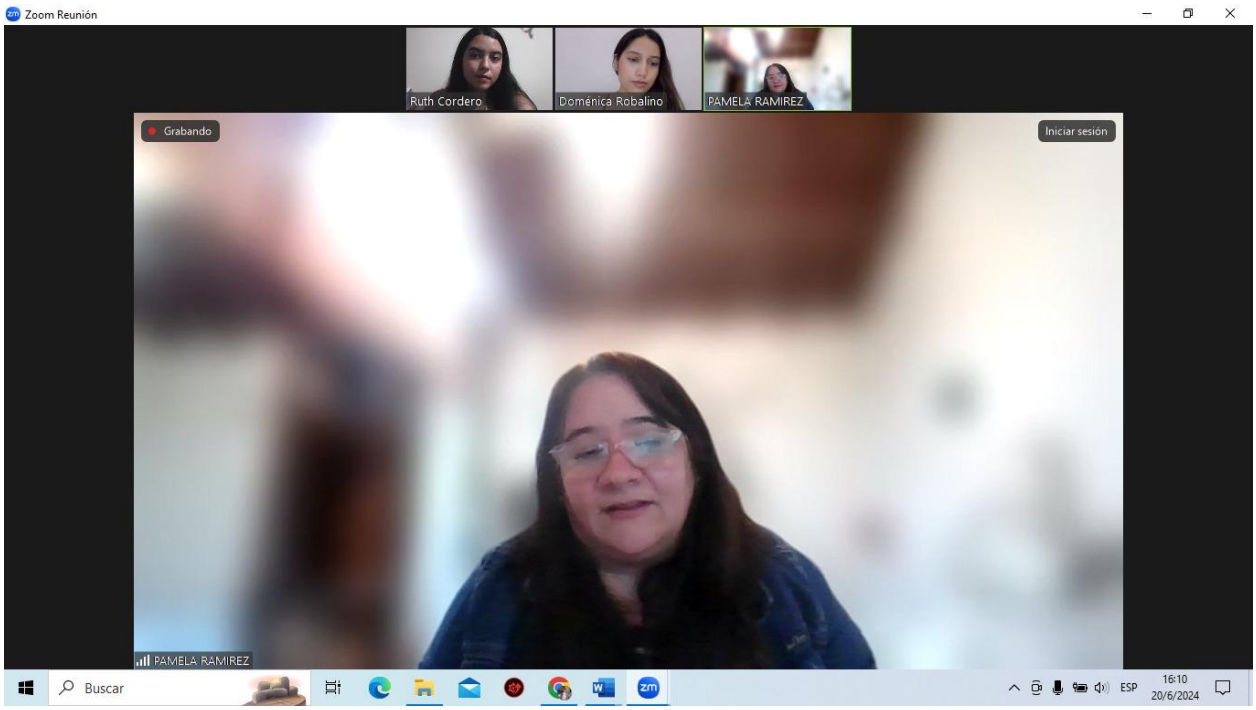
Sí, también debemos esperar la orden judicial. Cuando existe un menor en riesgo, tenemos una prioridad 1 para la investigación.

¿Ha realizado alguna extracción de información de consola de videojuegos?

Se que en otros gabinetes han tenido este tipo de casos que involucran los videojuegos con casos de grooming, sin embargo, no he realizado ninguna pericia sobre esto por el momento.

¿Qué impacto ha generado en usted el analizar material de abuso sexual infantil?

El impacto visual del material que analizamos puede generar un estrés post traumático. Incluso tenemos un programa psicológico que se brinda a cada uno de los investigadores que se llama “Cuidar a los que cuidan”. No todas las personas pueden realizar este tipo de trabajo, debido a que repercute bastante en la estabilidad mental del investigador.



2.4 Entrevista: Perito Ecuatoriano Mario de la Cruz. Trabaja en todas las áreas de la criminalística.

¿Cuál es su formación académica y experiencia profesional en análisis de evidencia digital?

Perito criminalístico, actualmente ha trabajado 6 meses en el área de informática forense con evidencia digital.

¿Ha trabajado anteriormente en casos de grooming? Si es así, ¿cuántos y cuál fue su rol específico?

Sí, he trabajado en casos de grooming he tenido un aproximado de 6 a 10 casos, cumpliendo las respectivas incumbencias periciales.

¿Cómo asegura la validez y precisión de los datos obtenidos?

Se asegura manteniendo una cadena de custodia adecuada que permita garantizar la trazabilidad y autenticidad de los indicios que van a ser analizados.

¿Cómo se realiza el proceso de recolección, preservación y análisis de evidencia digital?

El proceso de preservación y conservación que realizan los expertos de inspección ocular técnica que tienen información básica al respecto. Pueden ejercer 2 tipos de conservación en dispositivos móviles como celulares: obteniendo el chip o colocando en modo avión para neutralizar al dispositivo móvil y evitar la pérdida de la información que queremos analizar.

En casos de computadoras portátiles, no que se hace es sellar los puertos de ingreso, donde es la lectura de dispositivos.

En ambos casos la recolección y etiquetado debe ser minuciosa y cuidadosa porque el material que se va a transportar contiene información volátil, para el traslado se usan unas bolsas plásticas.

¿Ha realizado alguna extracción de información de consola de videojuegos?

No hemos tenido aún casos en consolas de videojuego.

¿Cuáles son los desafíos más comunes que enfrenta en el análisis de evidencia digital?

Verificar que los dispositivos estén adecuadamente conservados para el posterior análisis. Con la orden judicial se realiza la explotación del dispositivo tecnológico.

¿Qué protocolo sigue para asegurar la integridad de la evidencia desde su recolección hasta su presentación en juicio?

Se debe de seguir la cadena de custodia, también tenemos un proceso de apertura de la funda de cadena de custodia que va en sentido horario, cada vez que se presenta la evidencia en un juicio está se actualiza.

¿Qué mejoras considera necesarias en los protocolos de tratamiento de evidencia digital para fortalecer los procesos judiciales?

-Considero que el usar un mejor material para guardar este tipo de evidencia digital puede fortalecer el proceso judicial debido a que se asegura de mejor forma la misma.

-También sería importante que las personas que van a manejar este tipo de evidencia digital, mantengan el protocolo de apertura de la cadena de custodia. No todas las delegaciones la realizan por lo que se debería priorizar este tratamiento.

¿En qué protocolos se basa para el tratamiento de evidencia digital?

Tenemos el manual elaborado en el año 2012 que se implementó en la jefatura de criminalística.

¿Qué pericias se realizan en la evidencia digital?

Se pueden realizar incumbencias periciales de audio, video y afines. Y también se realizan incumbencias periciales correspondientes a informática forense.

2.5 Entrevista: Ab. Jhozman Yánez Trabaja en todas las áreas de la criminalística.

Usted ha tenido inconvenientes al presentar evidencia digital ¿cuáles?

Dentro de los procesos penales, la evidencia digital suele ser de las más importantes, pero también es de las más difíciles de poder presentar porque para eso se debe realizar la explotación del dispositivo. En ocasiones no tenemos el dispositivo a explotar queda invalidada porque no tenemos como corroborar que el material es fidedigno.

¿**Cómo se asegura de que la evidencia digital recolectada cumple con los requisitos legales para ser admitida en el juicio?**

Para la admisión de la evidencia digital en un juicio se trata de que cumpla con todos los requisitos legales que se encuentran detallados en el COIP. En el caso de la evidencia digital, se debe tener los dispositivos que se encuentren relacionados con algún tipo de delito, como celulares, computadoras, la dirección IP, etc. También es fundamental seguir la cadena de custodia porque por algún error puede quedar invalidada la evidencia digital.

¿Cómo evalúa la capacitación actual de los abogados en el manejo y presentación de evidencias digitales?

Considero que los abogados egresados hace aproximadamente unos 5 años atrás tenemos un poco más de noción de los conceptos de evidencia digital, por lo que, tenemos mayor responsabilidad en los temas procesales que los involucren.

¿Cómo se asegura de que las evidencias digitales recolectadas sean comprensibles en los tribunales?

Buscamos llevar lo que nosotros queremos mostrar a los tribunales, adaptándonos a lo que indican las pericias correspondientes y como se relacionan con nuestro objetivo. Es muy importante verificar, que se siga la cadena de custodia.

¿Cuántos casos que involucren evidencia digital ha procesado? ¿Cuál ha sido el resultado más común en estos casos (condenas, absoluciones, etc.)?

He tenido alrededor de 25 a 30 casos que han involucrado la evidencia digital en temas penales. En este momento tengo un caso en el que toda la evidencia estaba en el celular y no teníamos el acceso disponible.

¿Qué tipo de pruebas digitales considera más cruciales?

La evidencia digital más común es la de dispositivos móviles, porque se encuentran conversaciones en redes sociales como WhatsApp y llamadas, debido a que muchos ciudadanos tienen poca conciencia digital entonces quedan huellas.

¿Ha tenido algún caso en el que hayan tenido que extraer información de una consola de videojuego?

Por el momento, no he tenido ningún caso que involucre ese tipo de extracción de información.

¿Cómo coordina la recolección y análisis de evidencia con la policía y peritos informáticos?

En las ocasiones que hemos tenido este tipo de casos, se ha recurrido a peritos informáticos de Quito, se establecen los viáticos y todo. Además, es bueno coordinar todo el proceso con la Policía Nacional por el factor tiempo y debido a que se involucra información volátil. Siempre el abogado debe trabajar de la mejor manera para que los resultados de la pericia puedan ser usados en el tribunal.

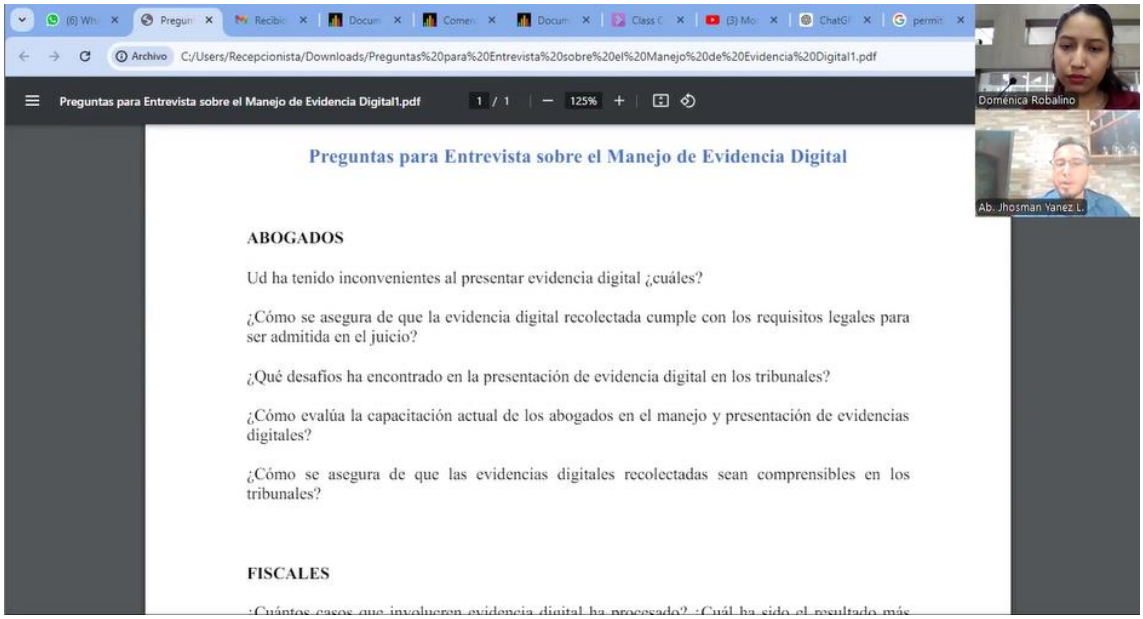
¿Qué estrategia utiliza para vincular al posible agresor con la evidencia digital obtenida?

La estrategia siempre la manejamos de acuerdo a lo que ha sucedido y a que versión las personas vinculadas de la parte actora y acusada emiten. En un caso reciente de

secuestro, el fiscal solicitó ver los nexos de redes sociales, y rastrear las llamadas de las partes.

¿Qué mejoras considera necesarias en los protocolos de manejo de evidencia digital para fortalecer los procesos judiciales?

Considero que deben ser un poco más confidenciales y que sólo fiscalía pueda manejar la evidencia digital para las pericias respectivas.



2.6 Entrevista: Perito Orly Cedeño. Trabaja en Audio, video y afines.

¿Cuáles son los procedimientos adecuados para la recolección y preservación de evidencia digital, específicamente en formato de audio y video, para garantizar su admisibilidad en un juicio en Ecuador?

Se maneja los principios de la norma ISO 27037, en la que nos indican el manejo adecuado de la evidencia digital. El primer paso es la identificación del dispositivo a periciar, la fase de adquisión, la preservación, el análisis y la presentación en un informe pericial.

¿Qué técnicas utiliza en la evidencia digital para la extracción de material de audio y video?

En la Policía usamos programas de software abierto, son programas de uso libre, se llama FTK Imager. Y la herramienta quennt aylor para sacar el hash

¿Qué consecuencias legales y técnicas puede acarrear la alteración o pérdida de evidencia digital en casos de delitos cibernéticos en el contexto ecuatoriano?

Nosotros como peritos no caemos sobre este tipo de delito, lo que puede ser es que no tengamos una orden judicial para el dispositivo en la pericia. Lo que puede ocurrir es que se dañe en tus manos el dispositivo.

¿Cómo se puede asegurar la autenticidad e integridad de archivos de audio y video utilizados como evidencia digital en investigaciones forenses en Ecuador?

En el Manual de Policías, tenemos las incumbencias periciales que podemos realizar entre esas tenemos una en la que debemos verificar la autenticidad antes de la pericia.

¿Qué herramientas y métodos son recomendables para la recuperación de evidencia digital dañada o eliminada, especialmente en casos relacionados con delitos cibernéticos en Ecuador?

Usamos FTK Imager, herramienta de uso forense para realizar la pericia y permite recuperar archivos eliminados.

¿Cuál es el impacto de la normativa ecuatoriana en la gestión y análisis de evidencia digital en investigaciones criminales, y cómo afecta la capacidad para procesar adecuadamente archivos multimedia como pruebas?

La normativa es clara en el art 616 del COGEP se debe garantizar la autenticidad de estos archivos. En audio y video generalmente obtenemos de material multimedia.

¿Cuáles son los desafíos más comunes que enfrenta en el análisis de evidencia digital?

Cuando la evidencia digital está sobre grabada le resta fiabilidad al archivo y puede existir el desfase en la grabación. Es un video sobre una grabación, no se puede demostrar la integridad del video.

¿Cómo se logra vincular a una persona con la evidencia digital en un delito?

Demostrar que se cometió el delito y como se distribuye la información

¿Qué mejoras considera necesarias en los protocolos de manejo de evidencia digital para fortalecer los procesos judiciales?

Que exista un lineamiento claro para la adquirió de la información y la presentación de la evidencia digital y que sea de conocimiento de abogados y policías.

Anexo 3: Glosario

Glosario

- Adquisición: En informática forense es el proceso de usar una interfaz para leer los datos de un dispositivo digital y tener un objeto de destino.
- Hash: Es un cálculo numérico utilizado para comprobar la integridad de la evidencia digital.
- Metadatos: Son los datos incrustados dentro de un archivo o sobre otro dato.
- Skimmer: Es el lector de tarjetas magnéticas.
- Datos volátiles: Son los datos que se pueden perder cuando el dispositivo pierde energía.
- CD: disco compacto
- IP: protocolo de internet
- AICEF: Academia Iberoamericana de Criminalística y Estudios Forenses
- ENFSI: Red Europea de Institutos de Ciencias Forenses
- IFSA: Alianza Estratégica Forense Internacional
- TIC: Tecnologías de la Información y las Comunicaciones
- EPI: elementos de protección individual.
- PEP: potencial elemento de prueba.
- OSAC: Organización de Comités de Áreas Científicas para Ciencias Forenses

Anexo 4: Consulta de procesos judiciales

Nombres y Apellidos del Demandado/Procesado: VEINTIMILLA VEGA JUAN ANDRES

Registros encontrados: 6

No.	Fecha de ingreso	No. proceso	Acción /Infracción	Detalle
1	10/02/2015	17243201500004G	DEPRECATORIO	
2	10/01/2015	17241201500001G	DEPRECATORIO	
3	17/10/2014	17248201400004G	DEPRECATORIO	
4	18/04/2013	17241201300007C	DEPRECATORIO	
5	23/03/2012	0190320120040	TENENCIA DE ARMAS	
6	03/10/2011	0165320118967	TENENCIA DE ARMAS	

*Imagen 1: Procesos registrados en **E-SATJE 2020** - CONSULTA DE PROCESOS JUDICIALES ELECTRÓNICOS*