Universidad CENFOTEC

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Propuesta de un estándar nacional que facilite determinar la admisibilidad de la evidencia digital en delitos informáticos en Costa Rica.

Estudiantes:

Brandon Alvarez Gonzalez

Alex Villegas Carranza

Febrero, 2022

Declaratoria de derecho de autor

Se declara que el presente proyecto de investigación fue realizado por los autores Brandon Alvarez Gonzalez y Alex Villegas Carranza, fundamentando los diferentes capítulos del trabajo en diferentes fuentes bibliográficas, literatura citada, las cuales tienen su respectiva referencia, respetando los derechos de autor de dichos trabajos. De igual manera se tomó como referencia los datos recopilados, a través de los cuestionarios creados y las entrevistas realizadas, en las cuales se reflejan los comentarios de los profesionales entrevistados. Se autoriza la reproducción total o parcial de este trabajo, para ser usados como referencia de trabajos futuros de tipo académico y científico, en este caso, se solicita incorporar la referencia de este trabajo respetando los derechos de los autores.

Digitally signed by BRANDON GERARDO ALVAREZ GONZALEZ (FIRMA)
Date: 2022.04.05 18:01:19 -06'00'

ALEX DANIEL VILLEGAS CARRANZA (FIRMA)

Firmado digitalmente por ALEX DANIEL VILLEGAS CARRANZA (FIRMA)
Fecha: 2022.04.05 18:30:00 -06'00'

Agradecimientos

Queremos agradecer a todas las personas que han colaborado de diferentes maneras en el desarrollo de esta investigación: Muy especialmente, agradecemos a nuestro profesor tutor Miguel Pérez Montero, por su invaluable orientación y recomendaciones durante todo el proceso de investigación y desarrollo del trabajo final de graduación, las cuales fueron claves para la exitosa culminación del mismo.

A los señores Roberto Lemaître Picado, coordinador del Centro de Respuesta de Incidentes Informáticos de Costa Rica y a Luis Naranjo Zeledón, profesor de la Universidad Cenfotec, por sus aportes a la investigación, diferentes recomendaciones y su disposición de colaborar en el proceso de revisión y entrevistas que hicieron posible este trabajo. Al personal de Registro y Decanatura de la Universidad Cenfotec por su ayuda y facilitarnos los recursos necesarios para el cumplimiento del proyecto de investigación. Agradecemos asimismo a nuestras familias por su apoyo y comprensión durante toda la Maestría y por la motivación para culminarla de manera exitosa.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para los estudiantes: **Álvarez González Brandon** y **Villegas Carranza Alex Daniel**

MIGUEL PEREZ MONTERO (FIRMA)

M. Sc. Miguel Pérez Montero
Tutor

ROBERTO PAULO LEMAITRE PICADO (FIRMA)
PERSONA FISICA, CPF-01-1209-0757.
Fecha declarada: 14/03/2022 10:04:20 AM
Razón: Acta Aprobacion Tesis
Lugar: San José, Costa Rica Contacto: rlemaitre@ucenfotec.ac.cr

M. Sc. Roberto Lemaitre Picado
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)

Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2022.03.14 11:57:38 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 10 de marzo de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Tabla de Contenido

Capítulo 1. Introducción **1**
1.1 Generalidades 1
1.2 Antecedentes del problema 1
1.3 Definición y descripción del problema 2
1.4 Justificación 2
1.5 Viabilidad 3
1.6 Objetivos 6
1.6.1 Objetivo general 6
1.6.2 Objetivos específicos 6
1.7 Alcances y limitaciones 7
1.7.1 Alcances 7
1.8 Marco de referencia organizacional y socioeconómico 7
1.8.1 Historia 8
1.8.2 Tipo de negocio y mercado meta 9
1.8.3 Misión, visión y valores 10
1.8.3.1 Poder Judicial 10
1.8.3.2 Ministerio Público 10
1.8.3.3 Organismo de Investigación Judicial 11
1.9 Estado de la cuestión 12
1.9.1.2 Selección de fuentes 15
1.9.1.2.1 Definición del criterio de selección de fuentes 15
1.9.1.2.3 Identificación de fuentes 16
1.9.1.2.5 Comprobación de las fuentes 17
1.9.1.3 Selección de los estudios 18
1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios 18
1.9.1.3.2 Definición de tipos de estudio 19
1.9.1.3.3 Procedimiento para la selección de los estudios 19
1.9.2 Ejecución de la revisión. 20
1.9.3 Resumen de los resultados 20
1.9.4 Legislación sobre delitos informáticos en Costa Rica 21
1.10 Requerimientos legales 23
1.10.1 Autorización legal 23
1.10.2 Relevancia de la evidencia digital 24
1.10.3 Autenticidad de la evidencia digital 27
1.10.5 Fiabilidad de la evidencia digital 30

Capítulo 2. Marco conceptual **33**
2.1 Conceptos sobre contenido 33

2.1.1 Cómputo forense 35
2.1.1.2 Evidencia digital 35
2.1.1.2.1 Reporte forense 36
2.1.1.2.2 Nivel de confianza 37
2.1.1.2.3 Admisibilidad 37
2.1.1.2.4 Trazabilidad 38
2.1.1.2.5 Manejo de la evidencia digital 39
2.1.1.2.6 Cadena de custodia 40
2.1.1.3 Marco de trabajo 40
2.1.1.5 Estándar 41
2.1.1.5.1 Metodología 41
2.1.1.5.2 Buenas prácticas 42
2.1.1.6 Proceso judicial 43
2.1.1.6.1 Procedimiento judicial 44
2.1.1.6.2 Delito informático 45

Capítulo 3. Marco metodológico 47
3.1 Tipo de investigación 47
3.2 Alcance investigativo 47
3.3 Enfoque 47
3.3.1 Dimensión epistemológica 48
3.3.2 Dimensión Ontológica 48
3.3.3 Dimensión Axiológica 49
3.4 Diseño 49
3.5 Población y Muestreo 51
3.6 Instrumentos de Recolección de Datos 51
3.6.2 Cuestionario 51
3.7 Técnicas de Análisis de Información 53

Capítulo 4. Análisis del diagnóstico 55
4.1 Aplicación de cuestionarios a expertos 55
4.1.1 Agrupación de la muestra de entrevistados 55
4.2 Respuestas de las entrevistas 56
4.3 Estándares y buenas prácticas internacionales aplicables a la investigación de delitos informáticos 64
4.4 Procedimientos que conforman la investigación de delitos informáticos en Costa Rica 66
4.5 Puntos de mejora en la investigación de delitos informáticos en Costa Rica 69
4.6 Determinar la admisibilidad de la evidencia digital. 71
4.6.1 Requerimientos técnicos 72
4.6.1.3 Cadena de custodia 73

4.6.1.4 Analista / experto en cómputo forense 73
4.6.1.5 Laboratorio de cómputo forense 73
4.6.1.6 Verificación de la integridad técnica 74
4.6.1.7 Testigo experto en cómputo forense 74
4.6.1.8 Reporte de la investigación de delitos informaticos 74
4.6.2 Requerimientos legales 75
4.6.2.1 Autorizacion legal 75
4.6.2.2 Relevancia de la evidencia digital 75
4.6.2.3 Autenticidad de la evidencia digital 76
4.6.2.4 Integridad de la evidencia digital 76
4.6.2.5 Fiabilidad de la evidencia digital 77

Capítulo 5. Propuesta de solución 78
5.1 Introducción 78
5.2 Fases 78
5.2.1 Reconocimiento 79
5.2.2 Recolección 86
5.2.3 Extracción 90
5.2.4 Protección 96
5.2.5 Análisis 100
5.2.6 Informe 103

Capítulo 6. Conclusiones y recomendaciones 110
6.1 Conclusiones 110
6.2 Recomendaciones 113

Glosario 115

Bibliografía 118

Anexos 124
Anexo A: Ejecución de la revisión de literatura 125
Anexo B: Legislación sobre delitos informáticos en Costa Rica 135
Anexo C: Boleta única de cadena de custodia de indicios 144
Anexo D: Documento de transporte de evidencia 146
Anexo E: Boleta de control de indicios 149
Anexo F: Plantilla dictamen pericial 151
Anexo G: Declaración Jurada - Protesta de cargo 156
Anexo H: Lista de recursos forenses 162

Capítulo 1. Introducción

1.1 Generalidades

Mucha de la información recopilada durante esta investigación sobre las prácticas utilizadas en Costa Rica para ejecutar una investigación en cómputo forense fue extraída de entrevistas a expertos y profesionales en el área. Esto se debe a que en Costa Rica la información pública sobre los procedimientos, técnicas o métodos a seguir en la investigación forense es escasa o inaccesible.

1.2 Antecedentes del problema

El teletrabajo ha sido una tendencia en crecimiento en los últimos años pero se acentúa desde inicios del 2020 debido a la pandemia por la Covid-19 (Pabilonia & Vernon, 2020). Desde ese contexto, surge la necesidad de migrar muchas labores hacia la virtualidad. Y como resultado de ello, se ha generado un ambiente perfecto para el incremento de los delitos informáticos (Ahmad, 2020). Algunos ejemplos de estos crímenes son el fraude, suplantación de identidades, extorsión, violación de datos personales, estafas, violación de comunicaciones e incluso, amenazas internas producto de la fuga de información.

Ante el aumento de los delitos informáticos, es necesario investigar los sistemas de información afectados pues es un proceso clave para las empresas, agencias gubernamentales, o partes involucradas en resolver un crimen donde la evidencia digital es fundamental.

En este ámbito, aparecen los peritos en cómputo forense. Su labor es ayudar en procesos judiciales que impliquen delitos informáticos pues son capaces de reconstruir lo que sucedió en los sistemas informáticos mediante técnicas. En otras palabras, permiten identificar, preservar, analizar y presentar la evidencia digital.

Los métodos y técnicas empleadas para analizar la evidencia digital son relativos a la naturaleza de cada caso. Por ejemplo, un mismo caso puede variar en metodología si es abordado por dos investigadores diferentes porque queda a discreción del profesional. Entonces, resulta difícil establecer un nivel de confianza sobre el trabajo de un perito en cómputo forense. ¿Cómo hacen los profesionales de

otras áreas ajenas al cómputo forense, tales como abogados, fiscales, jueces o magistrados para detectar si el trabajo expuesto por el perito en cómputo forense fue llevado apropiadamente? ¿Qué herramientas tienen para saber si el perito ha empleado una técnica o un método apropiado?

Un ejemplo donde se presenta este problema en Costa Rica es el caso de la Unidad Presidencial de Análisis de Datos (UPAD). En el 2020, los abogados del presidente Carlos Alvarado Quesada denunciaron que la Fiscalía secuestró información no relacionada con la investigación del caso pues incluía información de terceros sin relación o pertinencia alguna con la seguridad nacional, las relaciones internacionales y la salud pública de Costa Rica (Chinchilla, 2020).

Con lo anterior, se denota cómo el proceder de los peritos de la Fiscalía General generó dudas en cuanto a si realmente se procedió de la mejor forma. En este ejemplo concreto, si los peritos de la fiscalía pudieran demostrar que siguieron paso a paso los lineamientos desde un estándar nacional, difícilmente el presidente o las partes interesadas podrían presentar algún alegato.

1.3 Definición y descripción del problema

Este trabajo tiene como objetivo proponer un estándar nacional que facilite determinar la admisibilidad de la evidencia digital en delitos informáticos en Costa Rica. El documento define un conjunto de especificaciones técnicas mínimas para la práctica del cómputo forense en Costa Rica y sirve como documento soporte o guía para la construcción de una investigación forense auditable y de claro entendimiento para cualquiera de las partes interesadas.

1.4 Justificación

Si bien, a nivel nacional existen peritos en cómputo forense capaces de entregar un dictamen pericial respaldado por una investigación forense consistente. Lo cierto es que en general existen pocos profesionales en esta área en Costa Rica y es poco lo que se conoce sobre cómo manejar la evidencia digital en una investigación forense. Las partes interesadas no tienen la capacidad de distinguir si los procedimientos llevados a cabo en la investigación de delitos informáticos son los

correctos. Por ende, el presente proyecto servirá de partida para la creación de un estándar nacional sobre el manejo de la evidencia digital en el cómputo forense y con ello evitar que futuros procesos judiciales se vean afectados por la ruptura de la cadena de custodia, el mal manejo de la evidencia digital o por conclusiones en un dictamen pericial que no tenga un fundamento sólido.

La propuesta de esta investigación beneficiará a los diferentes peritos en cómputo forense, fiscales, jueces, magistrados y demás interesados en la integridad de la evidencia digital durante el proceso judicial.

1.5 Viabilidad

A pesar de que a nivel nacional en Costa Rica no existe un estándar sobre cómo se realizan las investigaciones de cómputo forense, hay esfuerzos similares en otros países. Tal es el caso de Colombia donde cuentan con un marco de trabajo sobre cómputo forense adaptado al marco jurídico nacional (Serna, Rivera, & Morales, 2012) o en Ecuador que cuenta con un marco de trabajo que alinea las buenas prácticas y métodos para el cómputo forense con el marco jurídico del país (Loarte, 2019). A continuación, se desarrollan los motivos técnicos, operativos y económicos por los que se considera que el desarrollo del proyecto de investigación es viable.

1.5.1 Punto de vista técnico

Como futuros másteres en Ciberseguridad y certificados por American Council For Cybersecurity And Computer Forensic (ACCCF) los autores cuentan con el conocimiento para dirigir investigaciones forenses sobre diferentes tipos de delitos informáticos, como denegación de servicios, fuga de información, activos comprometidos, actividad ilegal, hacking o ataques internos/externos, malware, correos electrónicos, violaciones de política, entre otros.

Los autores observaron la necesidad de un estándar nacional para investigación de delitos informáticos que ayude a determinar la admisibilidad de la

evidencia digital. Este documento ofrece buenas prácticas para la recolección, preservación, análisis y presentación de la evidencia digital en procesos judiciales en Costa Rica.

1.5.2 Punto de vista operativo

Al tratarse de una investigación a nivel país que cuenta con poca documentación al respecto, la mayoría de las fuentes son entrevistas a profesionales en ciberseguridad, respuesta a incidentes, personas que han desempeñado el cómputo forense desde la función pública y privada costarricense.

1.5.3 Punto de vista económico:

Debido a la naturaleza de este proyecto, el cual se propone tener un impacto a nivel país, el costo teórico implicado en su desarrollo, las horas de investigación, capacitaciones, software, hardware entre otros gastos asociados, son costeados por los autores de este proyecto.

De acuerdo con el Ministerio de Trabajo y Seguridad Social (MTSS), en Costa Rica un programador cobra por hora la suma de ¢13.872,70. Dado que ambos consultores se dedican en tiempo completo a ser programadores, el monto a cobrar será ese monto base que se estipula de la siguiente forma:

Salario Anual	Salario Mensual	Salario Diario	Salario por hora
¢ 59.930.064	¢ 4.994.172	¢110.981,6	¢13.872,70

Tabla 1: Desglose de salarios

Fuente: Elaboración propia basada en la información de (MTSS, n.d.)

Consultor	Horas Semanales	Duración TFG Meses	Duración TFG Horas	Costo Estimado Horas Consultor
Alex Villegas	16	4	256	¢ 13.872,70
Brandon Alvarez	16	4	256	¢ 13.872,70

Tabla 2: Costo de horas consultor.

Fuente: Elaboración propia basada en la información de (MTSS, n.d.).

1.6 Objetivos

Esta investigación utilizó la taxonomía de Bloom original de 1956 porque su modelo escalonado facilita la definición de los objetivos específicos Es así como se lleva desde el nivel general a lo más específico, aparte de ser ampliamente utilizada y recomendada.

1.6.1 Objetivo general

Proponer un estándar nacional que facilite determinar la admisibilidad de la evidencia digital en delitos informáticos.

1.6.2 Objetivos específicos

- Conocer los estándares y buenas prácticas internacionales aplicables a la investigación de delitos informáticos.

- Comprender las secciones relacionadas al delito informático en el marco jurídico de Costa Rica y los procedimientos que conforman su investigación.

- Demostrar los puntos de mejora en la investigación de delitos informáticos en Costa Rica, enfocados en los procedimientos del cómputo forense.

- Desarrollar un estándar que facilite determinar la admisibilidad de la evidencia digital dentro de la legislación costarricense.

1.7 Alcances y limitaciones

1.7.1 Alcances

Se propone este documento como un estándar nacional que facilite determinar la admisibilidad de la evidencia digital en delitos informáticos.

Se insta al sector público, privado y académico a tomar esta propuesta en consideración cuando su implementación represente ganancia para las partes involucradas en una investigación de delitos informáticos, con especial interés en dar un uso apropiado a la evidencia digital aportada.

1.8 Marco de referencia organizacional y socioeconómico

Costa Rica es una república de tipo unitaria cuyos gobernantes son elegidos cada cuatro años por medio del sufragio secreto y universal. Se cuenta con pluralismo político, es decir, hay diferentes partidos que conforman la Asamblea Legislativa, ente encargado de la creación y aprobación de leyes. Existe una división de poderes. De ahí surgen los conocidos como órganos constitucionales: el Poder Ejecutivo, Poder Legislativo, Poder Judicial, el Tribunal Supremo de Elecciones y la Contraloría General de la República.

El Poder Judicial es el encargado de impartir justicia en la sociedad costarricense mediante aplicación de normas y principios jurídicos en la resolución de conflictos. Para cumplir sus funciones, el Poder Judicial de Costa Rica está estructurado en tres ámbitos: jurisdiccional (magistrados y jueces), administrativo (consejo superior, dirección ejecutiva, departamento de proveeduría, entre otros) y auxiliar de justicia (Organismo de Investigación Judicial, Ministerio Público, Departamento de Defensores Públicos, entre otros).

Tanto Jueces como miembros del Organismo de Investigación Judicial tienen que interactuar con casos judiciales donde se involucran delitos informáticos y es necesario el cómputo forense. De la misma manera, las partes involucradas en los casos también deben estudiar la evidencia digital recabada.

1.8.1 Historia

El 24 de septiembre de 1824 la Asamblea Nacional Constituyente de Costa Rica acuerda la división del Estado en tres poderes: Ejecutivo, Legislativo y Judicial. Sin embargo, la concreción constitucional del Poder Judicial se daría hasta el 25 de enero de 1825 con la Ley Fundamental del Estado Libre de Costa Rica.

Después de ello, la administración de la justicia se impartirá de acuerdo a las Leyes de Indias creadas por España. Pero en 1841 se emitió el Código General el cual comprendió tres partes: el código civil, penal y de procedimientos.

En los años posteriores, se dará una serie de cambios debido a la creación de nuevas Constituciones Políticas, entre ellos la creación de la Corte Suprema de Justicia, la emisión de la Ley Orgánica del Poder Judicial, la creación de la Sala Primera y Segunda, la adición de más magistrados y el establecimiento de la independencia del Poder Judicial.

En 1948, se estableció una nueva Constitución Política que es la que rige hasta el día de hoy. Esta introduce cambios en el Poder Judicial tales como la potestad para auto-organizarse y nombrar su propio personal sin la intervención de los otros poderes del Estado.

En la década de los setentas, se promulgan el Código Penal y el Código Procesal Penal. Estos establecen un nuevo sistema procesal penal en el país. Es así como se lleva a la práctica el concepto constitucional de “justicia pronta y cumplida”. En 1973, la Asamblea Legislativa aprobó la Ley 5229 en la que se crea el Organismo de Investigación Judicial; quien dependerá de la Corte Suprema de Justicia. Como resultado, el Poder Judicial asume la función de investigación y se le adiciona la labor de acusación con la creación del Ministerio Público. Como punto adicional, en 1997 el Organismo de Investigación Judicial constituye la Sección de Delitos Informáticos. En él se utilizan técnicas de cómputo forense en la recolección, preservación y análisis de indicios para garantizar la cadena de custodia.

En cuanto a la legislación sobre delitos informáticos en Costa Rica, su historia se ve marcada por la carencia de leyes. En 1980, se da una serie de denuncias ante el Ministerio Público sobre delitos con tarjetas de crédito y cajeros automáticos. Ante la ausencia de tipos penales específicos, se intenta infructuosamente hacer pasar

estos actos como hurtos o estafas (Lopez & Torres). Tales denuncias van en aumento, costando el desembolso de altas sumas de dinero en protección por parte de los ciudadanos, bancos y empresas. En 2001 y 2010 se reforma el Código Penal agregando el concepto de delito informático y regulaciones al respecto. En 2012 se promulga la Ley nº 30.096 reformando la sección de Delitos Informáticos del Código Penal con el fin de

> (...) *prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia* (*Ley N° 9048*, 2012).

1.8.2 Tipo de negocio y mercado meta

El Poder Judicial de Costa Rica tiene la obligación de hacer respetar las leyes y administrar la justicia, objetivo fundamental que le confiere la Constitución Política. Asimismo, se rige por las directrices legales establecidas en la Ley Orgánica del Poder Judicial que establece:

> "...Corresponde al Poder Judicial, además de las funciones que la Constitución le señala, conocer de los procesos civiles, penales, penales juveniles, comerciales, de trabajo, contencioso-administrativo y civiles de hacienda, constitucionales, de familia y agrarios, así como de las otras que establezca la Ley; resolver definitivamente sobre ellos y ejecutar las resoluciones que pronuncie, con la ayuda de la Fuerza Pública si fuere necesario".

Por su parte, el Organismo de Investigación Judicial es una organización auxiliar, asesora y de consulta de las autoridades judiciales competentes. Su objetivo principal es colaborar con el descubrimiento y verificación científica de los delitos y sus presuntos responsables.

Por otra parte, el Ministerio Público tiene la función de requerir ante los tribunales penales la aplicación de la ley, mediante el ejercicio de la acción penal y la realización de la investigación preparatoria en los delitos de acción pública.

1.8.3 Misión, visión y valores

A continuación, se presenta la misión, visión y valores del Poder Judicial, Ministerio Público y del Organismo de Investigación Judicial.

1.8.3.1 Poder Judicial

- **Misión**: Administrar justicia pronta, cumplida y accesible, de conformidad con el ordenamiento jurídico para contribuir con la democracia, la paz social y el desarrollo sostenible del país.
- **Visión**: Ser un Poder Judicial que garantice al país, pleno acceso a la justicia, que resuelva los conflictos de manera pacífica, eficaz, eficiente, transparente y en apego a la ley, con personas servidoras comprometidas con su misión y valores, consciente de su papel en el desarrollo de la sociedad.
- **Valores**: Iniciativa, Integridad, Compromiso, Honradez, Responsabilidad, Excelencia.

1.8.3.2 Ministerio Público

- **Misión**: Proteger los derechos de las personas, requiriendo de los tribunales la aplicación de la ley para contribuir con la paz social.
- **Visión**: Ser un Ministerio Público eficaz, oportuno, y objetivo en la persecución de la criminalidad.
- **Valores**: Compromiso, Integridad, Iniciativa, Verdad, Discreción, Vocación de servicio, Lealtad, Valentía.

1.8.3.3 Organismo de Investigación Judicial

- **Misión**: Somos una organización encargada de investigar delitos con probidad y excelencia para servir y proteger a Costa Rica.
- **Visión**: Ser reconocidos como una policía líder, transparente y confiable, que aplique técnicas de investigación criminal modernas para enfrentar las nuevas técnicas delictivas.
- **Valores**: Mística, Objetividad, Disciplina, Excelencia, Lealtad, Efectividad, Honradez.

1.9 Estado de la cuestión

Así como se ha mencionado anteriormente en cuanto a la escasa información en el país del tema del manejo de la evidencia digital en delitos informáticos; a nivel internacional se han realizado esfuerzos en diferentes países para crear un documento que defina las buenas prácticas y procedimientos a seguir al realizar una investigación que envuelva evidencia digital y que refleje el marco jurídico local de cada caso. En el caso de Costa Rica, se realizó una búsqueda exhaustiva de la información necesaria para el desarrollo de la investigación y su posterior identificación, selección y análisis.

Problema

En Costa Rica los métodos empleados para analizar la evidencia digital quedan a discreción del profesional. Esta carencia de un referente en cuanto al procedimiento a seguir, lleva a disputas entre las partes por el manejo de la evidencia digital. Para los profesionales fuera del área del cómputo forense, resulta difícil evaluar el trabajo de un perito sin contar al menos con una referencia entendible sobre cómo debió realizarse la investigación forense. La presente investigación se enfoca en los esfuerzos que se han realizado en otros países para la creación de un documento de referencia en cuanto a la investigación de delitos informáticos, así como los procedimientos actuales que se ejecutan en Costa Rica.

Pregunta

¿Se puede implementar un estándar que facilite establecer la admisibilidad de la evidencia digital para la investigación de delitos informáticos, basándose en estándares internacionales, buenas prácticas y metodologías que a su vez se respalden dentro de la legislación nacional?

Palabras clave y sinónimos

Se hizo un listado de palabras clave que se utilizaron para la búsqueda e

identificación de documentos y trabajos relacionados con la investigación. Algunas de estas palabras están en el inglés. Esto se debe a que hay una gran cantidad de publicaciones en ese idioma. Se muestran en la siguiente tabla.

Palabra	Equivalente en Inglés
Cómputo forense	Computer Forensics
Proceso judicial	Legal Case
Casos criminales	Criminal Cases
Cadena de Custodia	Chain of Custody
Trazabilidad	Traceability
Estándar	Standard
Evidencia digital	Digital Evidence
Nivel de confianza	Confidence Level
Mejores prácticas	Best Practices
Marco de trabajo	Framework
Investigación forense digital	DFI
Modelo de investigación forense digital	DFI Model
Admisibilidad	Admissibility
Delito Informático	Cybercrime
Proceso de manejo de la evidencia digital	Digital Evidence Management Process
Procedimiento legal	Legal procedure

Metodología	Methodology
Reporte forense	Forensic Report
Datos	Data

Tabla 3: Listado de palabras.

Intervención

Ver los resultados de cómo la utilización de un documento de referencia sobre la investigación de delitos informáticos ayuda a los jueces o a las partes interesadas en un caso judicial. Así se logra determinar si el proceso fue realizado correctamente, es decir, siguiendo las buenas prácticas. Además, ayuda a obtener los documentos de mayor relevancia para la investigación y analizar los resultados obtenidos.

Control

Al iniciar la investigación, no se contaba con ninguna base de información. Se empezó con una búsqueda desde cero a partir de las palabras clave definidas y entrevistas a expertos en el área de cómputo forense.

Efectos

Se obtiene la documentación suficiente con las búsquedas realizadas para entender cuáles son los procedimientos y buenas prácticas para la realización de una investigación de delitos informáticos. Además, se genera una noción de los esfuerzos que se han realizado hasta la fecha en Costa Rica y fuera del país en este campo.

Medida de salida

Para la documentación encontrada se realizó una revisión de su calidad en sitios web especializados para tal fin.

Población

La población de esta investigación está conformada por partes interesadas en un proceso judicial donde se aborde la evidencia digital (jueces, magistrados, OIJ, peritos, demandantes, demandados, Ministerio Público, entre otros).

Aplicación

Este tipo de investigación puede resultar de utilidad para cualquiera de las partes interesadas en un proceso judicial, así como estudiantes o profesionales en el área de seguridad de la información.

Diseño experimental

Esta parte consiste en hacer el análisis y clasificación de los estudios recopilados, basándose en la calidad y relevancia del contenido encontrado para esta investigación. De este modo, se garantiza que la documentación encontrada es de la mayor confianza posible para la investigación.

1.9.1.2 Selección de fuentes

Esta sección describe el procedimiento de selección de fuentes utilizado para identificar los estudios primarios estudiados durante la investigación.

1.9.1.2.1 Definición del criterio de selección de fuentes

Para determinar cuáles fuentes seleccionar se tomaron en cuenta los siguientes factores:

- Número de resultados al aplicar cadenas de búsqueda.
- Reputación de la fuente en la comunidad científica.
- Facilidad de acceso.

1.9.1.2.2 Lenguaje de estudio

Debido a la naturaleza del tema en cuestión se tuvo la necesidad de emplear

en su mayoría el inglés al realizar las búsquedas. También se realizaron en español, con lo que se logró aumentar la cantidad de resultados disponibles.

1.9.1.2.3 Identificación de fuentes

A continuación, se describe el proceso de selección de las principales fuentes:

Recopilación de fuentes:

En primera instancia se obtuvo un conjunto de posibles fuentes. Los elementos de este conjunto fueron seleccionados basándose en la popularidad de la fuente, sus referencias en internet y en un estudio del año 2014 sobre cuáles son las mejores bases de datos para artículos sobre ciencias de la computación (Cavacini, 2014). Las fuentes obtenidas fueron:

- INSPEC
- Scopus
- Web of Science
- DBLP
- Google Scholar
- Springer
- Microsoft Academic
- IEEE Xplore Digital Library
- ACM Digital Library
- Research Gate.

Cadenas de búsqueda:

La siguiente es una lista de las cadenas de búsqueda utilizadas en la recopilación de información:

- "digital forensics" AND "legal framework"
- ("digital evidence" OR “digital forensics”) AND "confidence level"
- "digital forensics" AND ("standard" OR “methodology”)
- (“digital forensics” OR “digital evidence”) AND “guidelines”
- ("digital evidence" OR "computer forensics") AND litigation
- ("computer forensics" OR "digital forensics") AND "criminal cases"
- ("digital forensics" OR "digital evidence") AND "chain of custody"
- "evidencia digital' AND "metodologia"
- "cómputo forense" AND "judicial"
- "cómputo forense" AND ("cadena de custodia" OR "penal")
- "evidencia digital" AND juez

Selección de fuentes:

En base al criterio de selección de fuentes definido en la sección **1.9.1.2.1**, se refinó el conjunto de fuentes. Se tomó en cuenta además, que algunas fuentes contenían todos los resultados presentes en otras, por lo que estas últimas fueron desestimadas. Por lo tanto, se seleccionaron las fuentes **IEEE Xplore Digital Library** y **Scopus**.

1.9.1.2.5 Comprobación de las fuentes

Los investigadores no contaban inicialmente con un criterio experto con respecto a la selección de fuentes. No obstante, se realizó un esfuerzo para revisar la literatura disponible al respecto además de consultar a investigadores y profesores universitarios. Se buscó conseguir un criterio experto que conlleve a la modificación de la lista de fuentes de ser necesario.

1.9.1.3 Selección de los estudios

Una vez definidas las fuentes, se determinó cuáles documentos encontrados en las búsquedas formarían parte del análisis final.

1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios

En base a los siguientes criterios se determinó qué documento fue incluido o descartado para esta investigación.

Pregunta de Investigación	Término principal para Criterio de Inclusión	Criterio de Exclusión
¿Qué documentos de referencia existen sobre la investigación de delitos informáticos que establezcan niveles de confianza, mejores prácticas, metodologías o que reflejen la legislación local?	"Cómputo Forense", "Informática Forense", "Computer Forensics", "Digital Forensics" "Marco de trabajo", "Framework" "Chain of Custody", "Confidence Level", "Best Practices" "Evidencia Digital", "Digital Evidence", "Traceability", "Standard", "Criminal Case", "Methodology"	Documentos sobre manejo de evidencia, que no tengan relación con la evidencia digital. Estudios sobre cómputo forense, pero aplicados a incidentes o herramientas específicas. Documentos de informática o computación forense que no ofrezcan una forma de evaluar el proceso de investigación forense.

Tabla 4: Criterio de inclusión y exclusión de estudios.

1.9.1.3.2 Definición de tipos de estudio

La siguiente tabla permite determinar los requerimientos usados para elegir los artículos de interés.

Pregunta de investigación	¿Quién?	¿Qué?	¿Cómo?	¿Dónde?
¿Qué documentos de referencia existen sobre la investigación de delitos informáticos que establezcan niveles de confianza, mejores prácticas, metodologías o que reflejen la legislación local?	Investigación de delitos informáticos y la evidencia digital.	Procedimientos utilizados en la investigación de delitos informáticos.	Determinar niveles de confianza en la admisibilidad de la evidencia digital. Establecer mejores prácticas para el manejo de evidencia digital en Costa Rica.	Instituciones Públicas, Organizaciones Privadas. Buscadores de Internet, bases de datos. Páginas Web.

Tabla 5: Tipos de estudio.

1.9.1.3.3 Procedimiento para la selección de los estudios

Para la selección de estudios relevantes se aplicó el siguiente proceso iterativo:

1. Se realizó una búsqueda aplicando las cadenas de búsqueda.
2. Si existían más de 50 resultados, se aplicaban filtros adicionales como rangos de fechas.
3. Se aplicaron los criterios de exclusión basándose en el abstract y keywords.

4. Se seleccionaron los resultados relevantes de las fuentes consultadas y se repite el proceso con cada fuente disponible.

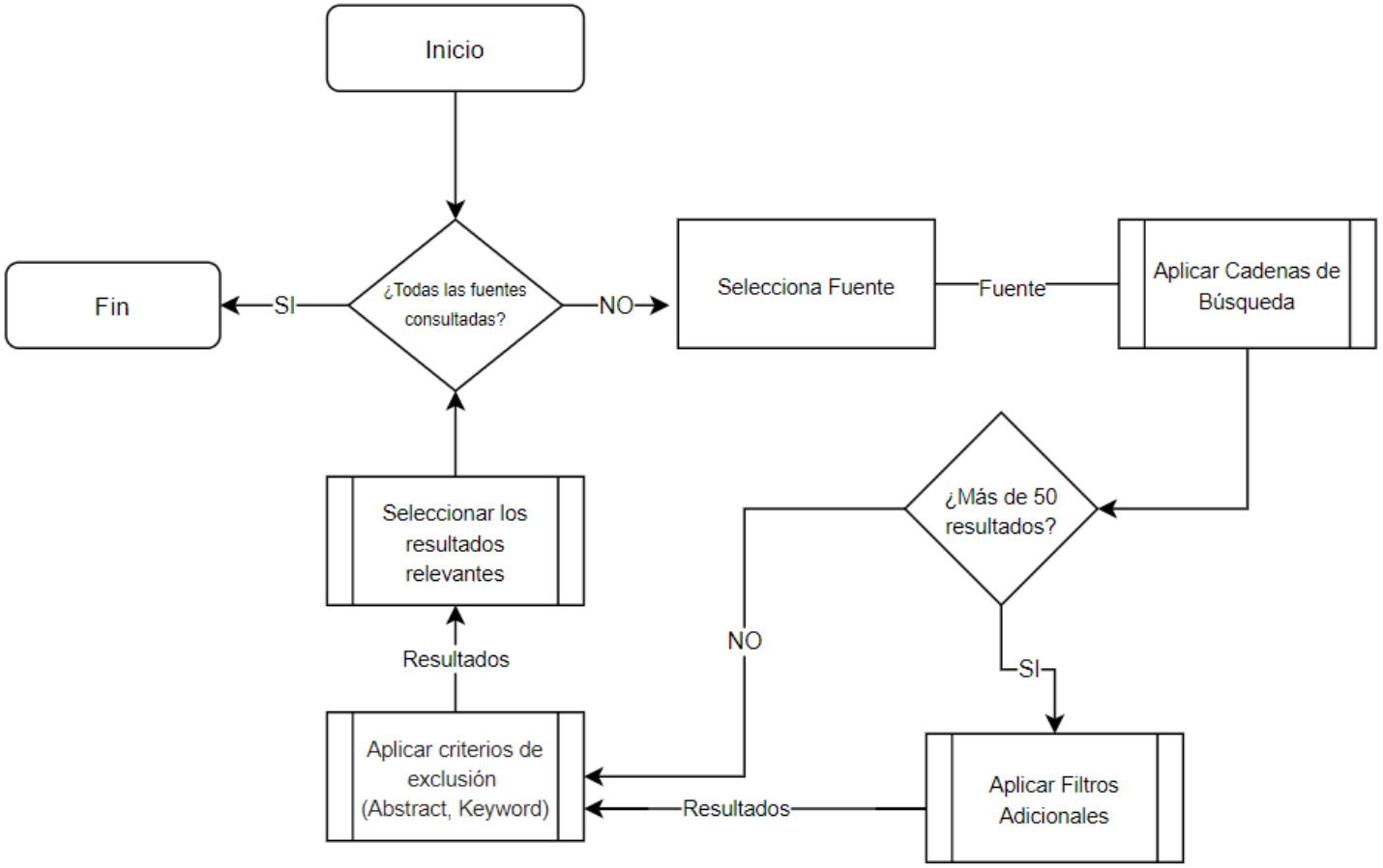


Figura 1: Procedimiento para la selección de los estudios. Fuente: elaboración propia.

1.9.2 Ejecución de la revisión.

En el Anexo A se muestra el proceso llevado a cabo para la revisión de las diferentes fuentes analizadas.

1.9.3 Resumen de los resultados

Durante todo el proceso de selección de estudios se lograron identificar 20 documentos que cumplían con los criterios de inclusión y exclusión. La siguiente tabla ofrece un resumen de los resultados.

Fuente	Relevantes	Primarios
IEEE	8	5
Scopus	12	8
Total	20	13

Tabla 6: Resumen de resultados.

1.9.4 Legislación sobre delitos informáticos en Costa Rica

El Código Penal es el principal instrumento legal utilizado para reprimir y sancionar los delitos informáticos en Costa Rica. Se le han hecho adiciones de varios artículos mediante la ley número 8148 con el fin fortalecer la ley a propósito de los delitos informáticos. Las modificaciones hechas se pueden encontrar en los siguientes tres artículos tomados de la ley 8148 del Código Penal Costarricense y su texto puede ser consultado en el Anexo B.

- Artículo 196 bis.- Violación de comunicaciones electrónicas.
- Artículo 217 bis.- Fraude informático.
- Artículo 229 bis.- Alteración de datos y sabotaje informático.

En dichos artículos de la ley se establecen las sanciones que se impondrán a aquellas personas que sean encontradas como culpables bajo uno o varios de los delitos citados. La pena va desde unos meses en prisión hasta de uno a diez años de cárcel como la pena más elevada. Además, la Sección de Delitos Informáticos se apoya en otras leyes especiales en donde se detallan artículos que castigan los delitos informáticos.

Principalmente se apoyan en las siguientes leyes y reglamentos:

1. Ley General de Aduanas, Capítulo II, Artículos 221 y 222.

2. Ley de la Administración Financiera de la República y sus Presupuestos.
3. Artículo 111: Ley de Derechos de Autor, Derechos Conexos.
4. Otros reglamentos y manuales que algunas instituciones públicas han creado con el fin de regular el buen uso de los sistemas informáticos.

En el año 2012, debido al avance de la tecnología y al incremento en la complejidad y cantidad de los delitos informáticos los legisladores costarricenses modificaron de nuevo el Código Penal mediante la ley 9048 y se reformó varios artículos que se listan a continuación:

- Artículo 167.- Corrupción.
- Artículo 196.- Violación de correspondencia o comunicaciones.
- Artículo 196 bis.- Violación de datos personales.
- Artículo 214.- Extorsión.
- Artículo 217 bis.- Estafa informática.
- Artículo 229 bis.- Daño informático.
- Artículo 288.- Espionaje.
- Artículo 229.- Daño agravado.
- Artículo 229 ter.- Sabotaje informático.
- Artículo 230.- Suplantación de identidad.
- Artículo 231.- Espionaje informático.
- Artículo 232.- Instalación o propagación de programas informáticos maliciosos.
- Artículo 233.- Suplantación de páginas electrónicas.
- Artículo 234.- Facilitación del delito informático.
- Artículo 235.- Narcotráfico y crimen organizado.
- Artículo 236.- Difusión de información falsa.

El texto de estos artículos puede ser consultado en el Anexo B.

1.10 Requerimientos legales

Esta sección tratará los requerimientos legales y la legislación vigente en Costa Rica. El propósito es facilitar el entendimiento mínimo necesario para ejecutar una investigación de delitos informáticos bajo el marco regulatorio costarricense para sumarle valor probatorio a la evidencia digital y que esta sea admisible durante un proceso penal en las cortes. Se incluyen, a continuación, los artículos del código penal costarricense que, directa o indirectamente, se relacionan con el cómputo forense. Además, se incluye la jurisprudencia relacionada a delitos informáticos.

Los cinco requerimientos legales principales para la admisibilidad de la evidencia digital abordados en la investigación son:

1. Autorización legal
2. Relevancia de la evidencia digital
3. Autenticidad de la evidencia digital
4. Integridad de la evidencia digital
5. Fiabilidad de la evidencia digital.

1.10.1 Autorización legal

El obtener la autorización legal otorga legitimidad judicial a la evidencia digital. Desde este punto de vista, podría ser el paso más importante en la recolección y manejo de la evidencia digital. Por ejemplo, una orden de registro es normalmente requerida para incautar dispositivos electrónicos y evidencias digitales. No conseguir una autorización legal puede descalificar a la mejor evidencia y poner en peligro todo el caso. Por otro lado, introducir evidencia digital que no haya sido recopilada con una autorización legal tiene consecuencias penales para las personas responsables involucradas (Antwi-Boasiako & Venter, 2017).

Es importante preguntarse si se cuenta o no con la autorización legal para recopilar la evidencia antes de iniciar con la fase de recolección. De lo contrario, no solo se podría desestimar la evidencia digital, sino que se podría infringir la Ley 7425 (Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones). Además, dependiendo del contexto, se podría incluso entrar en

conflicto con los artículos de Código Penal 196 bis (Violación de comunicaciones electrónicas) y 231 (Espionaje informático).

1.10.2 Relevancia de la evidencia digital

La relevancia es un criterio determinante para la admisibilidad de la evidencia digital. Para que la evidencia sea admisible, debe ser suficientemente relevante a los hechos en litigio. Para que una pieza de evidencia pueda considerarse relevante en un proceder legal, esta debe tender a probar o desaprobar un hecho sobre el caso. La evidencia que tiene valor probatorio debe probar que el hecho en cuestión es más (o menos) probable de lo que sería sin la evidencia.

En la jurisprudencia costarricense hay ejemplos donde la relevancia de la evidencia digital es objeto de discusión. Uno de los casos más conocidos es el de la UPAD. En él se investiga el supuesto acceso de datos confidenciales de los costarricenses por parte del gobierno que resulta en un abuso de poder por parte del Presidente Carlos Alvarado (Arrieta, 2021). Como parte de la investigación, el OIJ realizó un allanamiento a la Casa Presidencial y decomisó teléfonos celulares, computadoras y otros dispositivos.

Posteriormente, los abogados del mandatario presentaron gestiones ante la Sala de Casación Penal. Ellos argumentaron que la Fiscalía debió haber secuestrado y copiado la información relacionada con el caso y no toda la información en poder del Presidente. Se apoyaban en que esta acción suponía poner en peligro información sensible para la salud pública y la seguridad nacional.

En síntesis, con estas gestiones, la defensa pretendía que la Fiscalía se limitase a investigar únicamente lo relacionado al caso UPAD y que se definiera si el decomiso de los celulares del Presidente era realmente necesario (Muñoz, 2021).

A propósito de ello, la Sala de Casación Penal resolvió que los teléfonos celulares y la computadora del presidente Carlos Alvarado Quesada sí formaban parte de la investigación. En su resolución 2020-01404, los magistrados indicaron que:

"(...) esta Cámara no vislumbra ausencia de justificación, en cuanto a la necesidad y proporcionalidad respecto a la orden del decomiso de los dispositivos telefónicos y computadoras, ya que, claramente se consideraron los indicios y elementos probatorios que hasta ese momento se tenían en la investigación, lo necesario para justificar bajo los principios de proporcionalidad y racionalidad, la pertinencia de las actividades de investigación solicitadas a fin de obtener posibles elementos probatorios necesarios para determinar la verdad de los eventos indagados y, en particular, lo indispensable que resultaba la obtención de los celulares, computadoras entre otras evidencias, propiedad de los investigados, o bien, asignados a cada uno de los sospechosos, en razón de su función, como parte de los dispositivos en los cuales podría ubicarse información relevante".

"(...) alega el señor defensor que los teléfonos no resultaban indispensables en la investigación ahora en curso, que existían otros medios alternativos para localizar prueba idónea en el proceso, sin embargo, esas son apreciaciones puramente subjetivas y, hasta especulativas; pues sin saber si existen contenidos útiles para el proceso, sería imposible visualizar su hallazgo en otro lugar".

"Desde luego, conscientes de la seriedad del proceso, de los derechos y garantías que asisten a las personas que están siendo investigadas y, que además, por su fuero, como ocurre en el caso del señor Carlos Alvarado Quesada, actual Presidente de la República, desde luego que la apertura de los dispositivos electrónicos, como son por ejemplo los teléfonos celulares, deberán realizarse en estricto apego a los límites que conlleva la afectación a su derecho a la intimidad, en este caso, solo permitiendo el acceso a la prueba de interés y relevancia, para esta investigación".

Posteriormente, la defensa del presidente Carlos Alvarado Quesada presentó un recurso de apelación ante la Sala de Casación Penal con el objetivo de evitar que los datos extraídos de los teléfonos y la computadora se analizaran con el método forense propuesto por la Fiscalía. Ellos alegaban que se obtendría acceso a toda la información y no únicamente la relacionada con la UPAD. Como resultado, el procedimiento no sería el usual en este tipo de investigaciones.

El procedimiento usual consiste en que la información solo esté accesible para el órgano acusador y los defensores de los implicados únicamente en lo que a estos concierne. Una vez revisada, las dos partes determinarán qué documentos, conversaciones, correos, entre otros, se deben incluir en la pesquisa y cuáles no, por no estar relacionados. En caso de desacuerdo, el órgano jurisdiccional de garantías será el que establezca la procedencia o no del elemento.

El procedimiento propuesto por la fiscalía se diferenciaba respecto al utilizado regularmente para el acceso a información contenida en artefactos electrónicos. Normalmente, del total de archivos se hace una discriminación desde el criterio de interés en el caso a través de un software forense En este software las partes involucradas indican parámetros de búsqueda, siempre de forma privada y en presencia de un juez. De esa manera, se respeta la privacidad del acusado en todo aquello que no tenga que ver con el caso.

Sin embargo, la Sala de Casación Penal declaró inadmisibles los recursos presentados por la defensa porque el Código Procesal Penal no contempla expresamente este tipo de recursos en el procedimiento especial para juzgar a los miembros de los Supremos Poderes. Como resultado, la apelación no fue rechazada por el fondo o porque los argumentos no fueran pertinentes, sino por una limitación de procedimiento en el contexto de estos casos. La limitación reduce las posibilidades de defensa que sí otorga el procedimiento común a todas las personas investigadas.

Este caso en particular sirve para ilustrar cuáles son los procedimientos usuales a seguir para discriminar y admitir la evidencia digital en Costa Rica. También ilustra cómo la relevancia puede ser un punto de discusión. Mantener la privacidad y confidencialidad de las partes es de suma importancia al realizar una investigación de delitos informáticos. Un fallo puede llevar a conflictos con la Ley de

Protección de la Persona frente al Tratamiento de sus Datos Personales y la Ley de Delitos Informáticos.

1.10.3 Autenticidad de la evidencia digital

Una vez demostrada la relevancia de la evidencia digital, hay que determinar su autenticidad. Para que la evidencia digital sea admitida en la corte deben haber elementos probatorios que respalden y demuestren que la evidencia en cuestión es lo que se supone que es. De ahí que sea común encontrar en las cortes costarricenses apelaciones, reclamos e impugnaciones que ponen en duda la autenticidad de la evidencia digital. Un ejemplo de esto es la Resolución Nº 02308 - 2019 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José.

En esta resolución la sala responde a una impugnación que alegaba quebranto al debido proceso por discordancia en la rotulación de un disco que contenía evidencia digital en la forma de un videoreportaje. Ocurre que durante la etapa preparatoria, se incorporó como prueba un disco con la evidencia digital. Sin embargo, cuando inició el juicio, ese disco no apareció. Para subsanar, el tribunal utilizó otro disco identificado como “copia”.

En la impugnación se argumentó que el hecho de que no se trate del mismo objeto significa una vulneración seria. De esta forma, genera dudas fundadas sobre si lo que se incorporó al debate es el mismo elemento de prueba que fue autorizado por el juez penal. Como resultado, violentaba los principios que informan la cadena de custodia, en especial, el principio de identidad. La parte impugnante afirmó que no existía confiabilidad en el manejo del elemento, la rotulación no correspondía, ni el número de serie, por lo que no se podía garantizar su veracidad.

No obstante, el tribunal declaró sin lugar los motivos anteriores argumentando lo siguiente:

> *“[L]a Ley Orgánica del Poder Judicial reza “Artículo 6 bis.- Tendrán la validez y eficacia de un documento físico original, los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos o producidos por nuevas tecnologías, destinados a la*

tramitación judicial, ya sea que contengan actos o resoluciones judiciales. Lo anterior siempre que cumplan con los procedimientos establecidos para garantizar su ***autenticidad****, integridad y seguridad. Las alteraciones que afecten la autenticidad o integridad de dichos soportes los harán perder el valor jurídico que se les otorga en el párrafo anterior". Expuesto todo lo anterior, es importante definir que* ***ni el lacrado ni los controles por sí mismos*** *son la cadena de custodia, ni que el disco compacto se identifique con otra numeración a la consignada es una violación al debido proceso, que genera la ilegalidad de la prueba por falta de identidad e integridad. En el caso concreto, se percata esta cámara que el elemento probatorio ofrecido como tal no es el disco compacto per se, sino [...] un videoreportaje .Así las cosas, la probanza fue el video,* ***no el objeto en que se almacenó****".*

De este ejemplo, se comprende que no importa el medio donde se almacene la evidencia digital, siempre que se cumplan los procedimientos establecidos para garantizar su autenticidad, integridad y seguridad. En cuanto a qué procedimientos seguir para asegurar la autenticidad, el presente estándar propone un modelo de 6 fases para la investigación de delitos informáticos. Se listan prácticas como la identificación de fuentes originales, copias mediante funciones hash y la asociación del analista con la evidencia digital por medio de firma digital, sellado de tiempo, fotografías y biometría.

1.10.4 Integridad de la evidencia digital

Consiste en asegurarse que la evidencia se encuentre completa e inalterada. Un requerimiento primario para admitir la evidencia digital en un proceso judicial es hacer una correcta evaluación de la integridad de la evidencia. Esto permite a las partes involucradas determinar el peso o valor probatorio de la evidencia. La integridad de la evidencia digital no es una condición absoluta más bien es un estado de relaciones (Antwi-Boasiako & Venter, 2017). Al evaluar la integridad de la evidencia digital las cortes suelen considerar varios factores y relaciones.

Las cortes requieren que la integridad de la evidencia sea establecida y garantizada durante la investigación siguiendo los requerimientos técnicos para protegerla de alteraciones. En Sudáfrica, por ejemplo, la originalidad de la evidencia depende en su integridad como se señala en la sección 14(2) del acta ECA (Electronic communications and Transactions Act) del 2002.

Por otra parte, en Costa Rica existe un vacío sobre el tema pues no existe una sección similar en el Código Penal que haga referencia a la originalidad o integridad de la evidencia digital. Sin embargo, existe jurisprudencia al respecto. Por ejemplo, en la resolución 2021-1086 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José se señalan fallos en el proceso de extracción de la evidencia digital:

> "*Se detectó tenían algunos errores de formato y orden por lo que se consultó con la sección de Delitos Informáticos, quienes indicaron que debían ejecutar nuevamente la extracción de algunos casos ya que el software tenía (sic) varios días vencido. En torno a esto, asegura la impugnante que existió un daño de los archivos, lo que motivó otra sucesiva extracción. Aunado a que, dentro del interrogatorio, se logró establecer que la extracción de estos archivos no es exacta, que pueden alterarse el orden u omitir archivos en el proceso. Asevera que esta situación eventualmente podrá generar interpretaciones erróneas de los mensajes de texto, empero, esto ni siquiera fue considerado por el tribunal de juicio. Menciona que dentro del informe C.I. 1444-DRL-2017, hay una secuencia de mensajes que establecen una conversación fluida, pero que se saltan números".*

De este modo, según la apelante, se carece de la certeza de la forma en que dicha prueba fue manipulada desde el momento de su decomiso y hasta la extracción de la información. En este ejemplo, se da una apelación totalmente válida que introduce la duda sobre la integridad de la evidencia digital presentada. Esta tuvo que someterse a la repetición de la fase de extracción en varias ocasiones.

1.10.5 Fiabilidad de la evidencia digital

Para que la evidencia se considere confiable, “no debe haber nada que arroje dudas sobre cómo se recopilaron las pruebas y posteriormente se manejaron” (Leroux, 2004). En un caso judicial muy conocido en Estados Unidos, Daubert v. Merrell, se consolida la base para evaluar el nivel de confianza de la evidencia científica en los Estados Unidos. Este célebre caso especifica cinco criterios para evaluar el nivel de confianza (y por extensión, la admisibilidad) de la evidencia digital:

1. Si la técnica empleada ha sido probada.
2. Si la técnica ha sido sometida a revisión por pares.
3. Si existe una tasa de error conocida asociada con la técnica utilizada.
4. Si existen o si se mantuvieron las normas que controlan sus operaciones.
5. Si la técnica es generalmente aceptada por la comunidad científica.

En Costa Rica no existe un procedimiento oficial que se refiera al manejo estandarizado de la evidencia digital a diferencia de países como Sudáfrica o México. No obstante, en el país sí existe jurisprudencia al respecto. Por ejemplo, en la resolución Nº 2021-0686 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José se acusa del crimen de homicidio simple a una persona. El defensor del acusado aduce su inconformidad con la valoración de la prueba y la violación al principio de defensa. Indica que en el juicio se presentó una actividad procesal defectuosa de carácter absoluto en dos aspectos:

A. *“Todo elemento que se recoja puede ser presentada en un proceso judicial, teniendo como basamento internacional el Tratado 51/162 de 1996 siempre y cuando tenga una debida cadena de custodia, pero no solamente la cadena de custodia convencional, ya que es necesario también garantizar los aparatos que se utilizan a la hora que se realiza una extracción forense de los archivos digitales y hasta los operadores que manipulan los elementos de pruebas digitales, y cuya información electrónica que es extraída de un celular, computador o modem, vea a*

recaer inminentemente en ser una evidencia digital. Por lo anterior, el yerro procesal en el que se cayó, insuperablemente, es en el manejo de la evidencia digital, ya que como error se indicó por parte del suscrito, que no se estableció fidedignamente que, el dispositivo denominado 257 y 256, fuesen dispositivos de almacenamiento incólumes y pulcros, y que a su vez, una vez respaldada la información en dichos aparatos, NO SE ESTABLECIÓ EL CÓDIGO HASH (High Algorithm Secure Hash- calcula únicamente el contenido del archivo, no su nombre), siendo este código de publicación obligatoria en la cadena de custodia para verificar si el contenido de la evidencia es el mismo de cuando se realizó la imagen forense de los archivos digitales en el aparato de almacenamiento".

B. *"Ahora bien, hay que entender que como principio básico de la informática forense, es el proteger la evidencia digital extraída, teniendo un abanico de opciones no excluyentes entre sí como lo son el ya mencionado código hash, la imagen forense (bit a bit), la cadena de custodia (convencional), la bodega de evidencia (convencional), y el Wipping (que es el borrado adecuado de la prueba de una unidad de almacenamiento para así garantizar que cualquier respaldo informático en dicho objeto garantizará la identidad de la prueba que se respalda. Una vez respaldada la prueba en el objeto del cual se ha garantizado que era apto y limpio para guardar almacenamiento, es que se emite el código hash, que garantiza que el contenido es el mismo e invariable, así se realicen 10 copias de dicho respaldo, ya que el peso de la información se mantiene incólume. Este código hash garantiza la trazabilidad en la extracción de la información y se rige por el 27037 ISO, que establece el paso a paso que todo perito debe realizar cuando hace una recolección y análisis de un informe, la única manera de demostrar que la evidencia original no ha sido modificada es por la marca HASH, pero que esta garantía no la logramos tener de la evidencia utilizada en el juicio oral y público".*

La defensa del imputado estima que, por lo anterior, dicha prueba no podía utilizarse en el debate y, a la luz de la teoría del fruto del árbol envenenado, la extracción, información obtenida y peritajes derivados de aquella son en todos sus extremos espurios.

El veredicto final con respecto a este caso determinó que sí existía la cadena de custodia haciendo referencia a la orden y a el acta de allanamiento, el acta de secuestro y el acta de apertura de evidencia. Sin embargo, es importante resaltar la mención a la doctrina del fruto del árbol envenenado. Esta es una metáfora legal asociada con la valoración de la prueba en procesos penales, según la Revista Judicial Arburola (2021) que implica extender la invalidez probatoria a la prueba derivada de la ilegalidad inicial. En otras palabras, cuando los jueces advierten la necesidad de extender la invalidez de las pruebas derivadas de la ilegalidad inicial, surge el concepto de la doctrina del árbol venenoso.

Capítulo 2. Marco conceptual

Para iniciar, se preparó una nube con el fin de identificar los conceptos más relevantes que se mencionan en los documentos incluidos en el estado de la cuestión. Concretamente, para la siguiente figura, se utilizaron extractos y partes de los resúmenes creados en la parte del estado de la cuestión.

Figura 2: Nube de palabras. Fuente: elaboración propia usando el sitio https://tagcrowd.com/

2.1 Conceptos sobre contenido

Considerando las distintas bases de datos de las cuales se extrae la información, además de otras fuentes tales cómo entrevistas, videos, opiniones, etc. Se explican a continuación los conceptos utilizados para el desarrollo de la investigación.

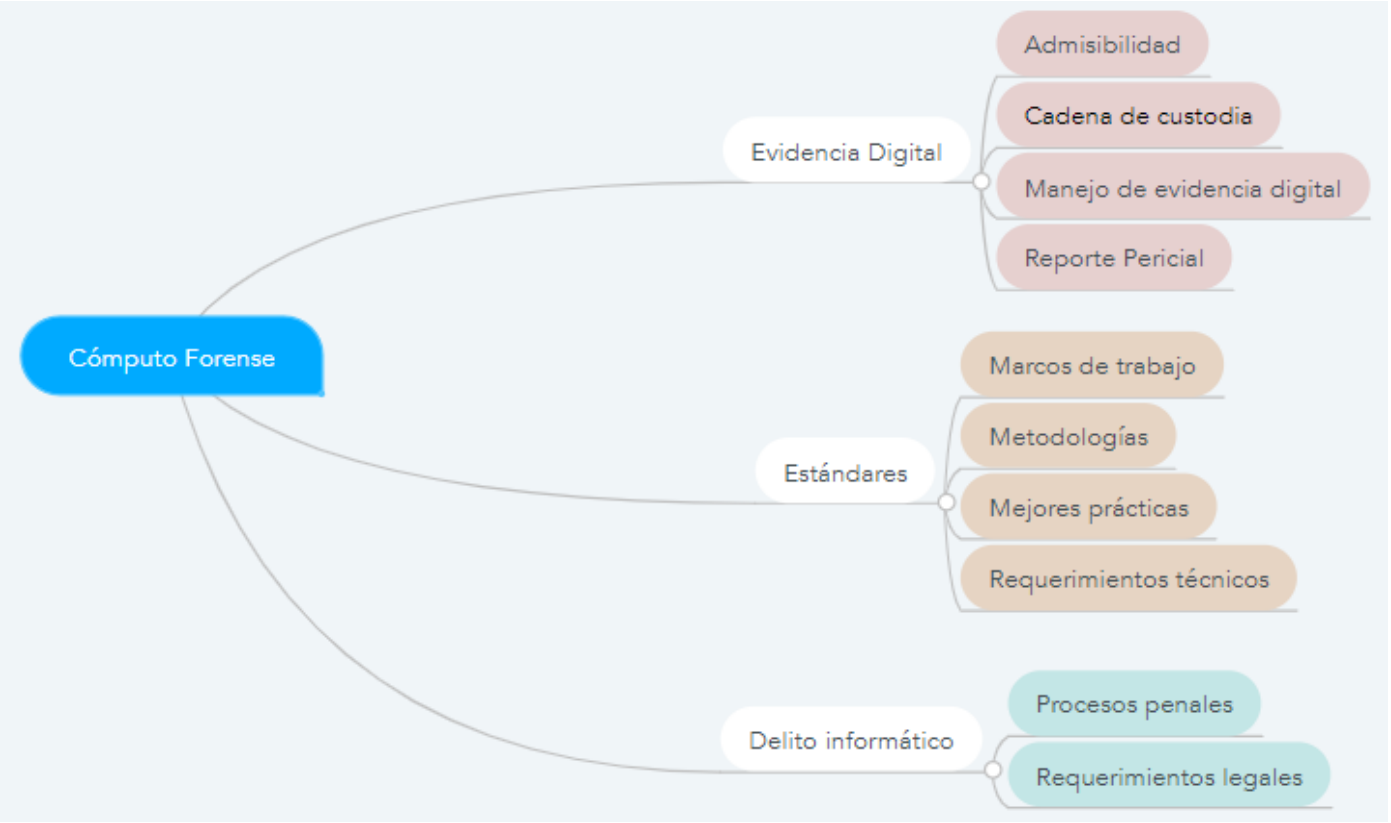


Figura 3: Mapa conceptual. Fuente: elaboración propia. https://www.mindmeister.com/

El alcance de esta investigación engloba la creación de un estándar que facilite determinar la admisibilidad de la evidencia digital en delitos informáticos. Además, profundiza en los requerimientos técnicos y legales identificados en la literatura consultada sobre el cómputo forense y en entrevistas realizadas a expertos del área en Costa Rica. A continuación, se procede a detallar los elementos clave para este trabajo:

- Cómputo forense
    - Evidencia digital
        - Reporte forense
        - Nivel de confianza
        - Admisibilidad

        - Trazabilidad
        - Manejo de la evidencia digital
        - Cadena de custodia
- Marco de Trabajo
- Estándar
    - Metodología
    - Buenas prácticas
- Caso Judicial
    - Procedimiento legal
    - Delito informático.

2.1.1 Cómputo forense

De acuerdo con Karie (2016), en el 2001 se entendía el concepto de cómputo forense como el uso de métodos probados y científicamente derivados para la recopilación, identificación y validación de artefactos que representan evidencia digital o pueden conducir a la reconstrucción de eventos en potencia considerados criminales.

El cómputo forense es una parte importante en la investigación de delitos informáticos. Sin embargo, debido a la rápida evolución de las tecnologías digitales, se está volviendo cada vez más sofisticado. Actualmente, es un reto para los investigadores, expertos en informática, organismos judiciales o cualquier parte interesada, el poder identificar, rastrear o incluso verificar la fuente y el historial de la evidencia digital capturada durante un proceso de investigación.

2.1.1.2 Evidencia digital

Según explican Stoykova y Franke (2020), la evidencia digital es el resultado de un procedimiento forense controlado. Este asegura la autenticidad e integridad de los datos. Así mismo, puede ser validado y en caso de que el método o herramienta utilizada para recopilar y analizar la evidencia digital por alguna circunstancia haya cambiado los datos originales, estos cambios son identificables, debido a que los procedimientos de validación utilizados aseguran que la técnica

forense digital se realice dentro del método científico. De esta forma, se producen resultados exactos, confiables y reproducibles.

Sin embargo, actualmente la ciencia forense digital carece de procedimientos formales de validación que puedan socavar su credibilidad científica. Como resultado, no puede hacer inadmisible la evidencia digital cambiada o que se considere poco probatoria en los tribunales de justicia.

Algunos autores como Carrier y Spafford (2004) mencionado por Siti et al. (2013) prefieren diferenciar la evidencia digital en potencia (EDP) de la evidencia digital relevante (EDR). Entonces, es necesario resaltar que todo objeto con características únicas, basadas en su funcionalidad y su creador debe considerarse como evidencia digital en potencia. Y por consiguiente, la evidencia digital relevante es un subconjunto de la evidencia digital en potencia pues esta última ha pasado a través de un análisis forense riguroso. Como resultado, le permite formar parte de un argumento legal. La EDR permite reconocer las fuentes originales e historia que la asocian con las causas del incidente.

Por último, Carrier y Spafford (2004) agregan que los datos en forma digital pueden tener una forma física y viceversa.

2.1.1.2.1 Reporte forense

De acuerdo con la guía publicada por NIST (Kent, 2016), el reporte forense consiste en informar los resultados del análisis forense inclusive la descripción de las acciones utilizadas. Se debe explicar cómo se seleccionaron las herramientas y procedimientos. También se debe indicar qué otras acciones hay que realizar de ser necesario. Por ejemplo, un análisis forense con fuentes de datos adicionales, aseguración de vulnerabilidades identificadas, mejorar los controles de seguridad existentes y proporcionar recomendaciones para mejorar políticas, procedimientos, herramientas y otros aspectos del proceso forense.

Muchos factores pueden afectar el proceso de generación del reporte forense:

1. Explicaciones alternativas: Cuando la información sobre un evento es incompleta, puede que no sea posible llegar a una explicación definitiva sobre los hechos. Cuando un evento tiene dos o más explicaciones posibles, cada

una debe ser dada en consideración dentro del proceso de generación del reporte. El analista debe utilizar un enfoque metódico para intentar probar o refutar cada posible explicación que se propone.

2. Consideración de la audiencia. Es importante saber a cuál audiencia se le mostrará los datos. Un incidente que requiera la participación de las fuerzas del orden requiere informes muy detallados de todo lo recopilado. También, puede requerir copias de todos los datos probatorios obtenidos. El administrador del sistema puede querer ver con detalle el tráfico de red y las estadísticas relacionadas. Las altas gerencias podrían querer una descripción general de alto nivel sobre el evento, una representación visual simplificada de cómo ocurrió el evento y hasta qué se debe hacer para prevenir incidentes similares.
3. Información procesable. Presentar un informe incluye la identificación de la información procesable obtenida a partir de datos que puedan permitir a un analista recopilar nuevas fuentes de información. Por ejemplo, una lista de contactos se puede desarrollar a partir de los datos que pueden conducir a información adicional sobre un incidente o crimen.

2.1.1.2.2 Nivel de confianza

Según menciona Rasjid et al. (2019), el concepto de Nivel de confianza refiere al momento en que la evidencia se encuentra bajo análisis forense digital. Este se ve afectado con la misma medida en que se dan cambios o alteraciones a la integridad de la evidencia digital. En su investigación, Rasjid et al. (2019) desarrollan un marco de trabajo para estimar el nivel de confianza de guía a los jueces antes de dar un veredicto final.

2.1.1.2.3 Admisibilidad

Para Rasjid et al. (2019) la admisibilidad es la medida del porcentaje de confianza otorgado a la evidencia. Cuando la integridad de la evidencia permanece intacta, entonces el nivel de confianza en la admisibilidad es de 100%. En el caso de que la evidencia puesta en investigación pase a través de varias fases de

investigación y el número de investigadores trabajando sobre la misma evidencia aumenta, esto puede reducir el nivel de confianza. Esto se debe a que en ese punto puede haberse aplicado varios cambios a la evidencia.

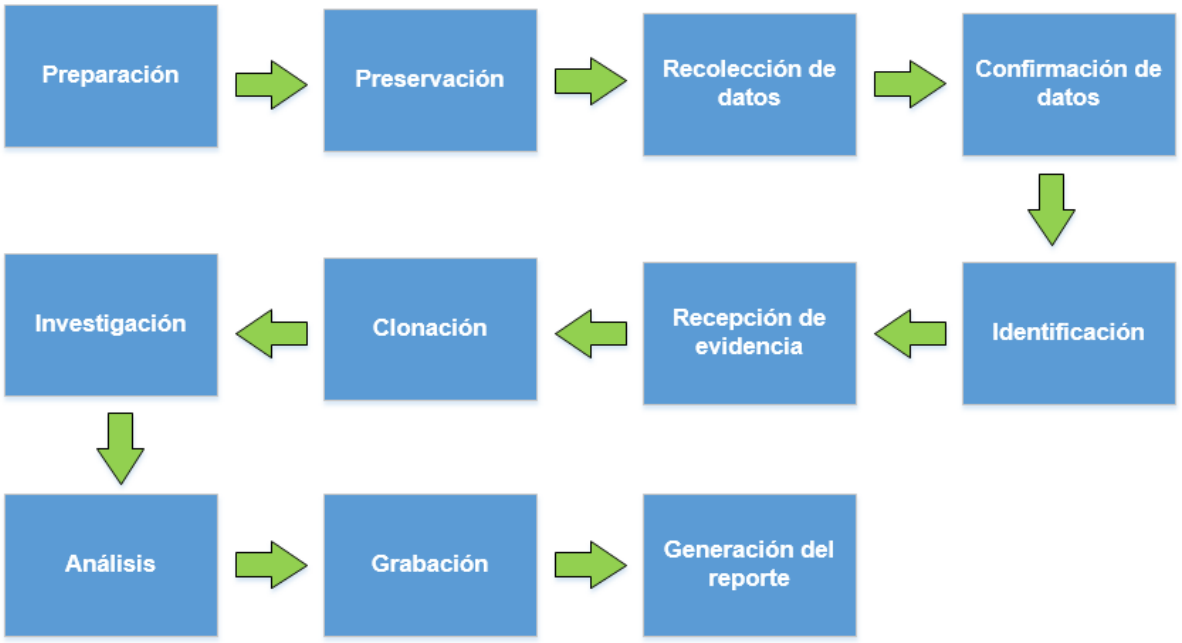


Figura 4. Brechas de seguridad durante las fases del manejo de evidencia digital. Construcción de imagen propia, toma como referencia la Figura 2 del trabajo de Rasjid et al. (2019).

2.1.1.2.4 Trazabilidad

De acuerdo con Karie (2016) que a su vez cita a Rupali y Tabassum (2012) junto con Siti (2013), trazabilidad es la capacidad de verificar la fuente, historial, ubicación o la aplicación de un artículo específico mediante la identificación documentada. La trazabilidad es un componente indispensable en muchas áreas de la vida y en el área de la ciencia forense digital ayuda a los investigadores a rastrear todos los aspectos de cualquier evidencia digital en función de su origen e historia. Dependiendo del origen del objeto o evidencia a analizar, la trazabilidad brinda la oportunidad de rastrear una cadena de eventos, así como de predecir los resultados sobre el proceso.

2.1.1.2.5 Manejo de la evidencia digital

De acuerdo con Rasjid et al. et al. (2019), el proceso para manejar la evidencia digital inicia con respecto a dos ubicaciones: la escena del crimen y el laboratorio forense. A continuación se muestra un diagrama de flujo con el procedimiento para manejar la evidencia digital en la escena del crimen.

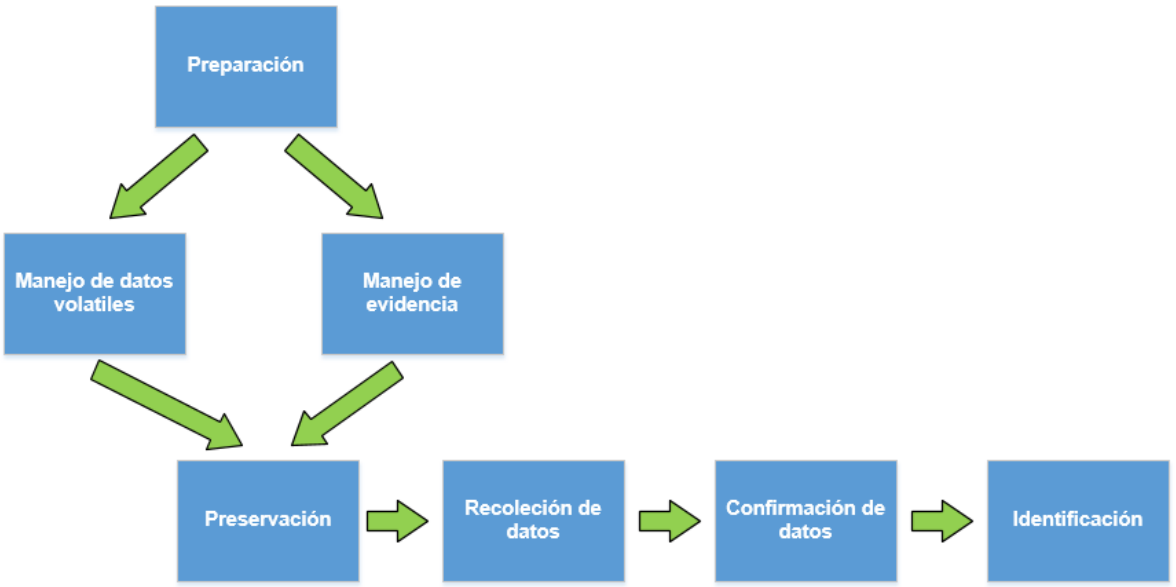


Figura 5. Manejando evidencia digital en la escena del crimen. Construcción de imagen propia, toma como referencia la Figura 1 del trabajo de Rasjid et al. (2019).

El primer paso es la preparación. Se debe prever todo tipo de evidencia pues los diferentes tipos de evidencia requieren un trato y equipo diferente. Por ejemplo, en el caso de una computadora tipo laptop que se encuentre encendida, existen datos volátiles que debe manejarse inmediatamente para evitar escenarios donde el computador se apague.

La evidencia obtenida en este paso deberá ser preservada y asegurada para que permanezca intacta. La evidencia debe ser identificada por un sello dado mediante una función criptográfica hash. Además, en la fase de recolección de

datos, toda la información disponible se recopila y finalmente se valida en la fase de confirmación.

En el laboratorio forense, después de recibir la evidencia, se vuelve a pasar por la función hash para asegurar que la integridad está intacta. Luego de esto, se debe crear un clon pues cualquier análisis se hará solamente en la versión clonada. Cabe señalar que toda la información encontrada se registrará.

En el posible caso de que trabajen más de un investigador en la fase de análisis, cuando la investigación esté terminada, todos los hallazgos deben ponerse en un reporte técnico basado en la investigación de la evidencia. Finalmente, los reportes de cada investigador deben presentarse unidos, es decir, en un solo reporte pericial que será presentado como un caso en la corte.

2.1.1.2.6 Cadena de custodia

Según explica Kent (2006), la cadena de custodia es un procedimiento para realizar documentación sobre la evidencia puesto en forma de eventos cronológicos. También agrega que la cadena de custodia es una parte importante del proceso de investigación pues garantizará que las pruebas puedan ser aceptadas en el sistema judicial. En estos términos, la cadena de custodia documentará los términos relacionados con el dónde, cuándo, por qué, quién, cómo y sobre el uso de evidencia digital, para todas y cada una de las etapas del proceso de investigación. Los problemas asociados a la cadena de custodia son determinantes en una investigación pues la autenticidad de la evidencia debe mantenerse acorde a la condición en la que se descubrió por primera vez y debe continuar así hasta que se presente en el tribunal.

El alcance de la cadena de custodia incluye a todas las personas involucradas en el proceso de adquisición, recopilación, análisis de evidencia, registros de tiempo. Se le suma la información contextual como es el etiquetado de casos, la unidad de trabajo y laboratorio que procesan la evidencia.

2.1.1.3 Marco de trabajo

En las Ciencias de la Computación se entiende el concepto de marco de trabajo (del inglés *framework*) como un conjunto estandarizado de conceptos,

prácticas y procesos para resolver un problema en particular. A su vez, funciona como referencia para resolver problemáticas similares en el futuro.

El concepto se extiende a diferentes ramas de la computación. Por eso es posible encontrar marcos de trabajo de arquitectura de sistemas, de desarrollo de software o incluso de inteligencia artificial. Por ejemplo, dentro del cómputo forense existen marcos de trabajo con el objetivo de resolver problemáticas particulares como la admisibilidad de la evidencia digital:

> *"Proponemos un marco para establecer el nivel de confianza de la admisibilidad de la evidencia. Con base en este marco, construimos un modelo que permite calcular el nivel de confianza de admisibilidad, a partir de la cual podemos producir un registro histórico para la trazabilidad de los documentos" (*Rasjid et al., 2019*).*

2.1.1.5 Estándar

En el ámbito de la tecnología, un estándar es una norma establecida para una tarea técnica repetible. Generalmente, toman la forma de un documento que incluye un conjunto de métodos, procesos y buenas prácticas. Los estándares son generalmente adoptados de manera voluntaria a menos que estos sean impuestos. Esto ocurre cuando hay contratos asumidos por organizaciones o por medio de la legislación gubernamental. Cuando un estándar se convierte en un estándar nacional, es debido a que los intereses del estándar se han integrado en los intereses nacionales (Xu, 2014).

2.1.1.5.1 Metodología

Dentro del contexto de Ciencias de la Computación, el concepto de metodología describe al conjunto de procedimientos racionales utilizados para alcanzar uno o varios objetivos. En este ámbito, existen al menos 5 tipos de metodologías (Elio, 2020):

1. Metodología formal: Utilizada para demostrar hechos sobre algoritmos y sistemas, tales como complejidad espacio-tiempo o la calidad de las soluciones generadas.
2. Metodología experimental: Empleada para evaluar nuevas soluciones a problemas. Suele ser dividida en una fase exploratoria donde se toman medidas para identificar las preguntas que deben formularse sobre el sistema evaluado y otra evaluativa donde se busca responder estas preguntas.
3. Metodología de construcción: Consiste en construir un artefacto con capacidades nuevas para demostrar que puede ser creado y que ningún artefacto previo cuenta con estas capacidades.
4. Metodología de proceso**:** Aplicada con el objetivo de entender los procesos necesarios para cumplir ciertas tareas en Ciencias de la Computación. Se utiliza en investigaciones sobre interacción humano-máquina o en el campo de la inteligencia artificial.
5. Metodología de Modelo: Define un modelo abstracto para un sistema real que a su vez es menos complejo, facilitando el entendimiento del sistema y la ejecución de experimentos o simulaciones.

2.1.1.5.2 Buenas prácticas

Cuando un método, técnica o procedimiento es aceptado como superior a otras alternativas se le considera como una buena práctica. El carácter de superior se le da debido a que produce consistentemente mejores resultados que otras alternativas. En el área de la tecnología, las buenas prácticas son aplicadas en campos como el diseño de software donde *“ayudan a capturar mejor las propiedades de calidad y a hacer que los problemas de calidad sean más tangibles”* (Brauer, 2017). En otros campos como el cómputo forense, las buenas prácticas son un elemento clave en el cumplimiento legal:

> *“Para respaldar el enjuiciamiento, las pruebas deben ser admisibles en el tribunal y poder resistir las impugnaciones en cuanto a su autenticidad, por lo tanto, los investigadores deben seguir instrucciones específicas y cumplir*

con ciertas regulaciones y requisitos que se conocen como buenas prácticas" (Ali, 2012).

La adopción de buenas prácticas por parte de organizaciones suele ser voluntaria. Es común encontrarlas dentro de estándares que a su vez pueden ser mandatorios para organizaciones que buscan certificarse en áreas específicas. Un ejemplo de esto es el estándar ISO 27001 que contiene buenas prácticas para la gestión de la seguridad de la información.

2.1.1.6 Proceso judicial

Se entiende el proceso judicial como una serie de actos jurídicos ejecutados por órganos jurisdiccionales de cualquier orden (civil, penal, comercial, entre otros) para aplicar la ley en la resolución de un caso. En los actos jurídicos participa el Estado, las partes interesadas y terceras personas no relacionadas con el caso en discusión.

En Costa Rica los procesos judiciales se rigen por varios códigos como el Código Procesal Civil, el Código Procesal Penal o el Código Procesal Contencioso-Administrativo. Estos códigos definen, entre otras cosas, cuales son los principios que deben guiar el proceso judicial. Por ejemplo, en el artículo 2 del Código Procesal Civil se definen los principios de igualdad procesal y buena fe procesal:

> ***"Igualdad procesal**. El tribunal deberá mantener la igualdad de las partes respetando el debido proceso e informando por igual a todas las partes de las actividades procesales de interés para no causar indefensión."* (Ley Nº 9342, 2016).

> ***"Buena fe procesal**. Las partes, sus representantes o asistentes y, en general, todos los partícipes del proceso, ajustarán su conducta a la buena fe, al respeto, a la lealtad y la probidad. El tribunal deberá tomar, a petición de parte o de oficio, todas las medidas necesarias que resulten de la ley o de sus poderes de dirección, para prevenir o sancionar cualquier acción u omisión contrarias al orden o a los principios del proceso, impidiendo el fraude*

procesal, la colusión y cualquier otra conducta ilícita o dilatoria." (Ley Nº 9342, 2016).

El proceso judicial no debe confundirse con el procedimiento judicial puesto que el primero contiene y es más amplio que el segundo. Además del procedimiento judicial, el proceso judicial incluye aspectos como las relaciones entre las partes o el objeto del proceso.

2.1.1.6.1 Procedimiento judicial

El procedimiento judicial es el conjunto de normas jurídicas generales que rigen la ejecución de un juicio. Estas normas regulan las resoluciones que los jueces y tribunales toman bajo su potestad jurisdiccional y son empleadas como medio para la terminación justa del proceso judicial. Nieto-Morales da la siguiente descripción del procedimiento judicial:

"Cuando el conflicto de intereses entre las partes se judicializa corresponderá resolverlo a los tribunales de Justicia, y se hará por medio de Jueces y Magistrados. Lógicamente estos deberán hacerlo siguiendo unos criterios fijados en las leyes, concretamente lo harán a través del procedimiento judicial" (Nieto-Morales, 2016).

Un punto a resaltar es que no existe un único procedimiento judicial. Existen varios de ellos y dependen de la naturaleza del conflicto:

"Aunque en términos genéricos hablemos de procedimiento judicial, en la realidad tenemos que saber que nuestra Administración de Justicia, según la naturaleza del conflicto a resolver. abarca distintos procedimientos judiciales. Por tanto, el procedimiento judicial que seguiremos dependerá de la naturaleza del conflicto, de aquí que si el problema se centra, sírvase de ejemplo, en el despido de un trabajador, el tema se resolverá en la jurisdicción social. Si es de una licencia para construir conocerá la jurisdicción contencioso-administrativa. Si estamos ante un divorcio deberá resolverse

ante la jurisdicción civil. Por último, si el problema es de delincuencia el campo propio será la jurisdicción penal" (Nieto-Morales, 2016).

2.1.1.6.2 Delito informático

El delito informático está tipificado en la legislación costarricense en el Código Penal, específicamente en la sección VIII, denominada "Delitos informáticos y conexos", del título VII. En esta sección se describen los siguientes delitos y sus penas:

- Suplantación de identidad
- Espionaje informático
- Instalación o propagación de programas informáticos maliciosos
- Suplantación de páginas electrónicas
- Facilitación del delito informático
- Narcotráfico y crimen organizado
- Difusión de información falsa.

Si bien se describen varios delitos informáticos, no hay una definición particular del delito informático. La carencia de una definición sólida del delito informático ya ha sido notada en Costa Rica desde el 2010:

"Para denominar este tipo de criminalidad existe actualmente una visible confusión, dándose infinidad de expresiones entre estas: abuso informático y de datos, delito corporativo, robo electrónico, intrusión en sistemas informáticos, delito de cuello blanco, criminalidad informática, delitos electrónicos, delitos informáticos, crímenes por computadora, delincuencia relacionada con el ordenador, cyber crímenes, delito relacionado con la computadora, delitos cibernéticos entre otros" (López & Torres, 2010).

"No existe una definición única del concepto del delito informático, reflejo de la complejidad que encierra para los juristas, entender una rama jurídica que va de la mano de la tecnología, la mejor definición debe incluir la

mezcla de ambas áreas, el sólo pensar jurídicamente deja un gran sesgo a una definición integral" (Lemaitre, 2010).

"Los actuales delitos informáticos del Código Penal Costarricense, son reflejo de una mala práctica legislativa, desconocimiento del tema y una respuesta apresurada de un problema emergente, el cual no recibió el proceso serio de creación jurídico-informático que se requería, los tipos penales presentan errores de forma, fondo y de desconocimiento de la terminologia informatica consignada en los artículos, lo cual agrava la protección real de este tipo de delitos" (Lemaitre, 2010).

A pesar de no existir una definición general del delito informático, se puede considerar, para efectos de esta investigación, el delito informático como todo aquel delito efectuado mediante un sistema o red informática o telemática contemplando también, los contenedores electrónicos, ópticos o magnéticos. Esta definición toma como base el artículo 234 del Código Penal de Costa Rica donde se tipifica el delito de facilitación del delito informático de la siguiente manera:

"Facilitación del delito informático: Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos" (Ley Nº 9048, 2012).

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

En este trabajo se empleó la investigación de tipo aplicada ya que se utilizan marcos de trabajo, metodologías y buenas prácticas en el ámbito de la investigación de delitos informáticos para proponer un estándar nacional que facilite determinar la admisibilidad de la evidencia digital en procesos judiciales.

3.2 Alcance investigativo

El alcance investigativo de este trabajo es de tipo descriptivo. Se basa en el perfil del investigador forense digital en Costa Rica y su predisposición a ejecutar el análisis de evidencia digital sin un estándar definido que permita, entre otras cosas, definir el nivel de admisibilidad de la evidencia digital.

El propósito de este trabajo es que cualquier investigador en cómputo forense pueda adherirse al estándar aquí propuesto y mejorar el proceso de investigación de delitos informáticos actual al utilizar las buenas prácticas y métodos que componen el estándar.

3.3 Enfoque

El enfoque que aborda esta investigación es el alternativo debido a que calza mejor el contexto del cómputo forense. Permite utilizar herramientas que se encuentran tanto en los enfoques cuantitativos como cualitativos.

Se puede agregar además que los enfoques cualitativos y cuantitativos no tienen por qué existir de manera separada y que no tiene sentido hablar de enfoques mixtos ya que estos intentan mezclar artificialmente cuestiones que nunca han estado separadas (Chavarría, 2011).

Seguidamente, se establecen las dimensiones epistemológica, ontológica y axiológica de la investigación, sin hacer referencias directas a un enfoque en particular.

3.3.1 Dimensión epistemológica

Esta investigación estudia los estándares, marcos de trabajo y metodologías existentes en cuanto al manejo de evidencia digital dentro del cómputo forense para producir un estándar nacional en Costa Rica. Por lo tanto, los investigadores tienen una posición de observadores al no estar cambiando el cómputo forense en sí (nuestro objeto de investigación), sino más bien estandarizando las prácticas en Costa Rica dentro de este campo.

Los investigadores por medio de entrevistas y la base de conocimiento adquirida, analizaron los procesos actuales de cómputo forense en cuanto a conceptos como trazabilidad, cadena de custodia, admisibilidad y reporte forense, esto con el objetivo de determinar cuáles son los requerimientos técnicos y legales necesarios en Costa Rica.

3.3.2 Dimensión Ontológica

El cómputo forense ha sido descrito y modelado desde principios de este siglo (Reith, 2003), y siendo que este campo se nutre de los conocimientos propios de la investigación forense general, se considera que el estudio propuesto cuenta con una representación concisa del conocimiento que se desea producir. La representación ontológica del cómputo forense se muestra a continuación.

Figura 6: Ontología del cómputo forense.

Fuente: Elaboración propia. https://www.mindmeister.com/

El estándar que este trabajo propone busca generar un mecanismo que permita establecer niveles de confianza en la admisibilidad de la evidencia digital.

3.3.3 Dimensión Axiológica

La dimensión axiológica se enfoca particularmente en el establecimiento de la admisibilidad de la evidencia digital en procesos judiciales. La evaluación se realiza desde el entendimiento y comprensión para determinar cuándo la evidencia digital presenta una admisibilidad apropiada, para lo mismo el esfuerzo de los investigadores se centra en proveer una serie de requerimientos técnicos y legales debidamente explicados en su contexto.

De esta manera cualquier parte interesada en una investigación de delitos informáticos puede, por medio del estándar propuesto, comprender mejor las implicaciones de haber cumplido o no con un requerimiento legal o técnico.

3.4 Diseño

El enfoque de este trabajo es cualitativo empleando un diseño conocido como “Design Science” en español Ciencia de Diseño, en el trabajo realizado por (Hevner & Chatterjee, 2010) ellos logran adaptar un marco de trabajo que utiliza las bases de la Ciencia de diseño, la cual por definición busca extender los límites de las capacidades organizacionales y humanas creando “artefactos” innovadores junto con la Ciencia del comportamiento, que busca desarrollar y verificar teorías que explican o predicen el comportamiento de las organizaciones y humanos. Fusionando ambos aspectos ellos presentan este marco de trabajo utilizado para la investigación en sistemas de información.

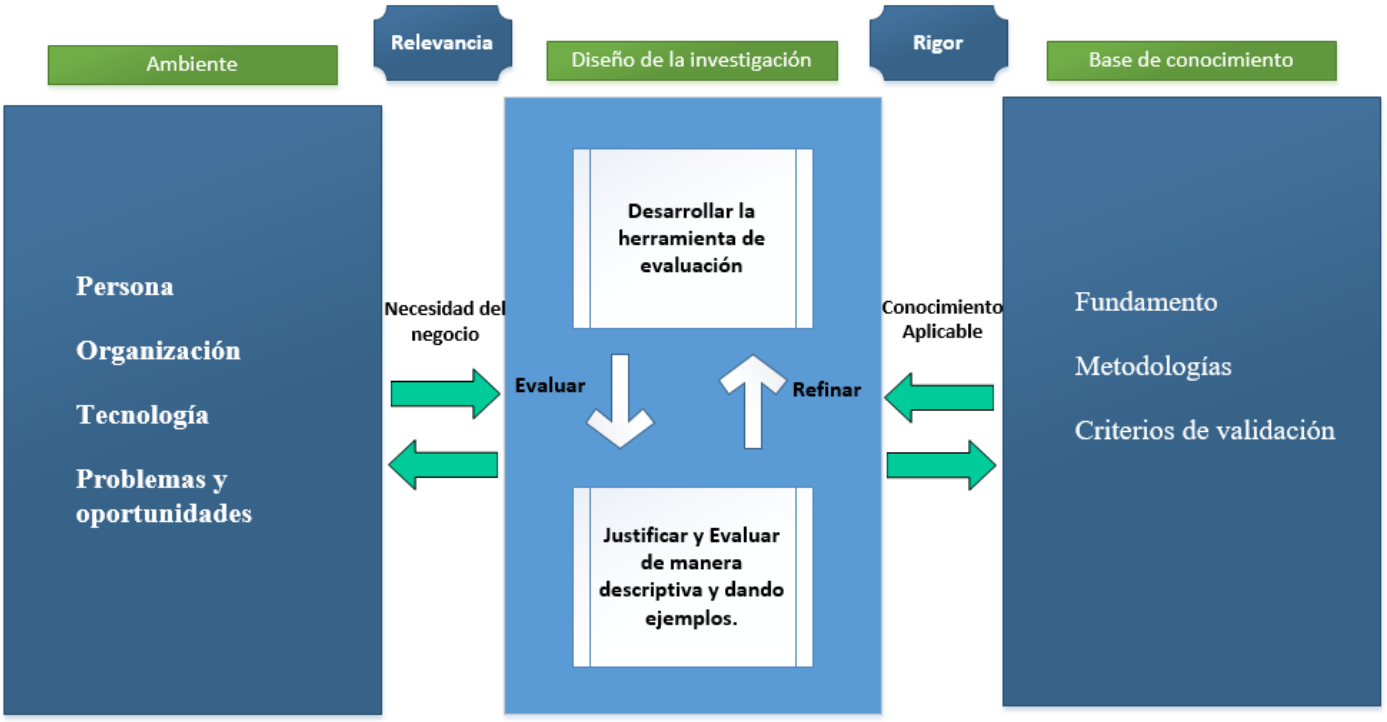


Figura 7: elaboración propia basada en la información de (Hevner & Chatterjee, 2010).

Dentro del ciclo de diseño de esta investigación, Ciencia de diseño ayuda en la elaboración de iteraciones, donde el artefacto (la propuesta de un estándar nacional que facilite determinar la admisibilidad de la evidencia digital en delitos informáticos en Costa Rica) se estará alimentando desde el rigor que da la academia en el marco teórico y de las necesidades existentes en el ambiente de la forense digital, el cual tiene necesidades, experiencias, organizaciones, personas que aportaran por medio de entrevistas enfocadas en encontrar puntos de mejora en el proceso de análisis forense.

El método de evaluación es el descriptivo. En términos de ciencia de diseño, este tipo de evaluación utiliza la base de conocimiento relevante, para construir un argumento convincente sobre la utilidad del artefacto. Además, se deberá construir los escenarios detallados sobre el artefacto, para demostrar su utilidad.

3.5 Población y Muestreo

Dado que esta investigación es aplicada y con un enfoque cualitativo se hizo uso del método de muestreo no probabilístico conocido como muestreo por conveniencia, el cual consiste en seleccionar unidades muestrales convenientes para el estudio, por lo que no existe control de la composición de la muestra (Fernández,2014). Este tipo de técnica es comúnmente utilizada en estudios que hagan uso de cuestionarios o entrevistas, herramientas que son parte de esta investigación.

3.6 Instrumentos de Recolección de Datos

Al ser este un trabajo de enfoque cualitativo la recolección de datos se realizó por medio de entrevistas donde al entrevistado se le hicieron una serie de preguntas sobre los procedimientos actuales de la investigación de delitos informáticos que se siguen en Costa Rica en los procesos judiciales. Esto con el objetivo de comprender los procesos que conforman la investigación de delitos informáticos en Costa Rica e identificar los puntos de mejora en los procedimientos del cómputo forense.

3.6.2 Cuestionario

El siguiente cuestionario tiene como fin recopilar información por parte de investigadores en cómputo forense digital costarricenses, con diferentes capacidades, características, experiencias y roles en la organización. Las personas involucradas fueron seleccionadas con el método de Fernández (2014), llamado muestreo por conveniencia. Las preguntas del siguiente cuestionario pretenden sacar información sobre la relevancia de la admisibilidad y la trazabilidad de la evidencia digital a lo largo del proceso de la investigación de delitos informáticos.

Preguntas	Resultado Esperado
¿Cuántos años tiene de experiencia trabajando en el cómputo forense?	Entrevistados cuentan con al menos 5 años de experiencia
¿Trabaja en el sector público/privado?	Los entrevistados cuentan con experiencia en ambos sectores.
¿Cuál es el estado actual del cómputo forense en Costa Rica?	Una descripción amplia sobre el estado del cómputo forense en Costa Rica.
¿Qué buenas prácticas sigue usted al realizar una investigación de delitos informáticos?	Un conjunto de buenas prácticas para realizar la investigación de delitos informáticos.
¿Cómo garantiza usted la calidad en la investigación de delitos informáticos?	Lineamientos para garantizar la calidad en la investigación de delitos informáticos.
Ejemplos de malas prácticas	Una serie de ejemplos de malas prácticas que sirvan como muestra de lo que se debe evitar
¿Conoce legislación o procedimientos que guíen a las cortes en la evaluación de la evidencia digital?	Evidencia de la carencia de procedimientos que guíen a las partes no técnicas involucradas en la evaluación de la prueba (evidencia digital) en un juicio.
¿Existe un faltante de experticia sobre el cómputo forense en CR?	Entrevistados encuentran un faltante de profesionales calificados en cómputo forense actualmente
¿Existe mercado para el cómputo forense?	Entrevistados describen un mercado pequeño e incipiente
¿Áreas de mejora/recomendaciones para la investigación de delitos informáticos en CR?	Entrevistados brindan un listado de mejoras en la práctica de la investigación de delitos informáticos en CR

¿Conoce estándares o documentos que guían al profesional en la investigación de delitos informáticos?	Obtener un listado de estándares y documentos que sirvan de insumo para la investigación

Tabla 7: Cuestionario a aplicar orientado a expertos en forense digital.

3.7 Técnicas de Análisis de Información

El siguiente diagrama de flujo muestra el proceso general para la generación de una fuente de información con ejemplos de procesos judiciales en Costa Rica, la parte de entrevistas ha sido enfocada en identificar oportunidades de mejora sacadas de ejemplos reales de experiencias obtenidas por expertos. Por cada ejemplo específico los expertos proveerán detalle sobre cada proceso llevado a cabo durante las diferentes fases de la investigación de delitos informáticos, el criterio experto obtenido mostrará formas de mantener la calidad durante el manejo de la evidencia digital.

Al concluir las entrevistas, se inicia con un proceso de análisis por cada caso, para proponer un método en el que se puedan incorporar indicadores tales como la trazabilidad y el porcentaje de admisibilidad de la evidencia digital para dar una medida general sobre la confianza en el proceso del cómputo forense. Este proceso se evaluará de manera descriptiva según menciona (Hevner & Chatterjee, 2010) en su marco de trabajo para la investigación en sistemas de información, por lo que entrará en un ciclo de retroalimentación donde se incorporan los aspectos de Ambiente (Las personas del negocio entrevistadas) y la fuente de conocimiento (Teorías, métodos, estándares internacionales, marcos de referencia) con el fin de agregar rigor y relevancia al diseño del método en mención.

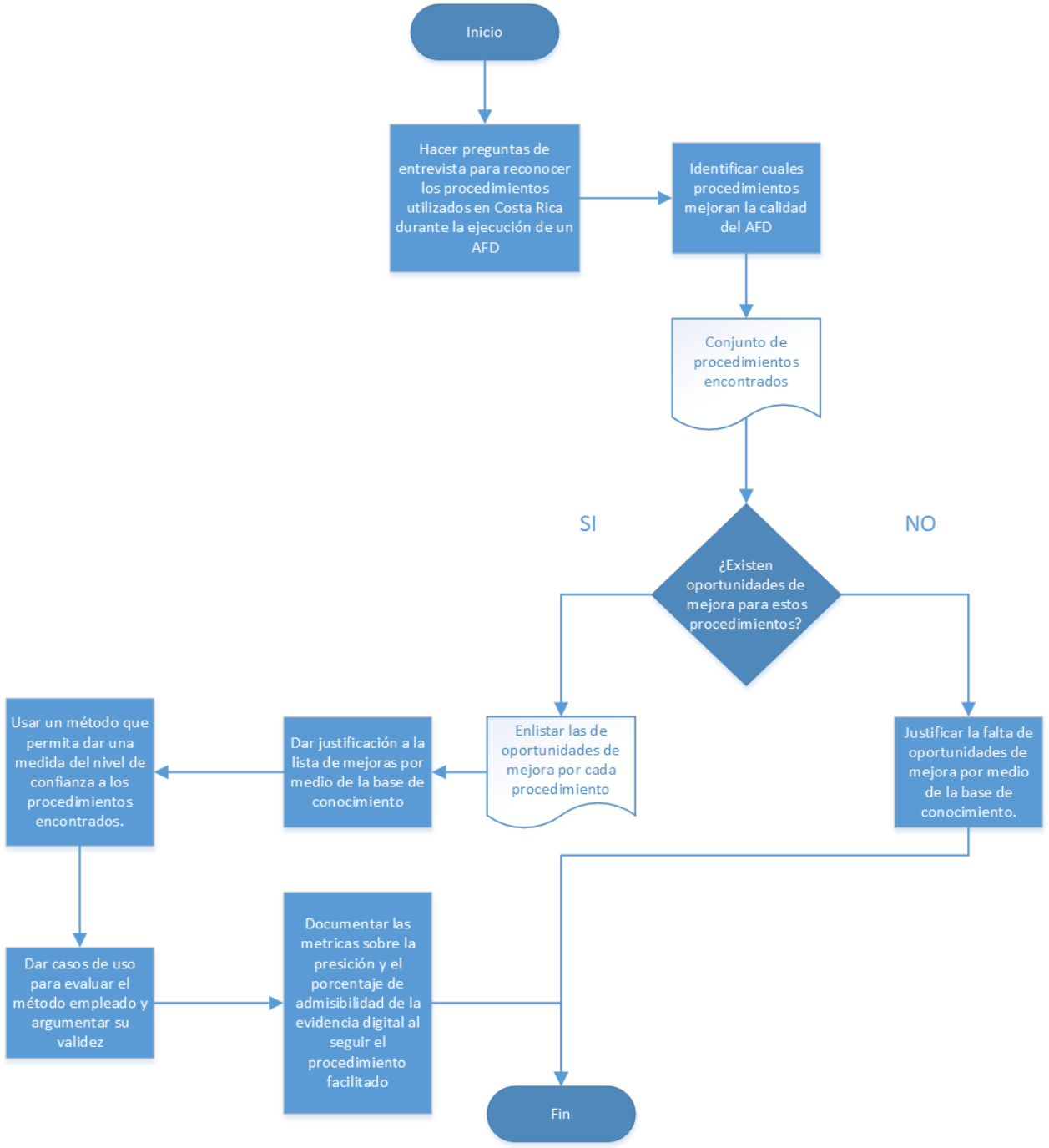


Figura 8: Diagrama de flujo de Técnicas de Análisis de Información. Fuente: Elaboración propia.

Capítulo 4. Análisis del diagnóstico

4.1 Aplicación de cuestionarios a expertos

Tomando como base del conocimiento la información recolectada en el Capítulo 1 y 2, se procedió a aplicar entrevistas como un instrumento de recolección para distinguir los procedimientos y buenas prácticas que consideran los expertos al ejecutar una investigación de delitos informáticos en Costa Rica. Se obtuvieron los resultados a continuación:

4.1.1 Agrupación de la muestra de entrevistados

Los expertos fueron segmentados en profesionales del sector público, privado y ambos. Son elegidos debido a su experiencia probada en el ámbito del análisis forense digital. Estos son los resultados:

Segmentación de la población entrevistada	Resultado obtenido
¿Cuántos años tiene de experiencia trabajando en cómputo forense?	Los entrevistados elegidos rondan entre 5 y 15 años de experiencia.
¿Trabaja en el sector público/ privado?	Entre los entrevistados 2 de ellos tienen experiencia solamente en el privado, 3 solamente en el público y 2 en ambos a la vez.
Roles en los que ejercen los entrevistados	● Fiscalizador en Contraloría General de la República. ● Coordinador CSIRT de Costa Rica ● CISO (Sector privado) ● Auditor de Ciberseguridad del Banco Nacional ● Gerente de Prácticas de Ciberseguridad (Sector privado) ● Fiscalizador en la Contraloría General de la República ● Analista de Ciberseguridad CSIRT-ICE

Tabla 8: Compilación de las respuestas de diferentes expertos.

4.2 Respuestas de las entrevistas

A continuación, se muestra un resumen de las respuestas obtenidas en las entrevistas:

4.2.1 ¿Cuál es el estado actual del cómputo forense en Costa Rica?

Se denotan cuatro aspectos relacionados al estado actual del cómputo forense en Costa Rica. Se describen a continuación:

1. **La legislación nacional:**

   Sobre la legislación nacional se menciona que la tipificación del delito informático es deficiente, aparte no existe marco local que tabule leyes que defiendan al ciudadano ante delitos informáticos.

2. **Los procedimientos y su forma:**

   Sobre la forma en que se lleva a cabo el cómputo forense y sus procedimientos, se menciona que la labor del OIJ está centralizada en la gran área metropolitana (GAM) y es la única unidad de delitos informáticos del país. Hay faltante de estadísticas e información que muestre el estado actual sobre la cantidad de delitos informáticos o procesos penales donde la evidencia digital esté asociada. Estas estadísticas ayudarían a dar perspectiva y ayudar en la toma de decisiones para la mejora continua.

   Además, hay poca inversión por parte del Estado en equipo y compensación salarial, lo que provoca sobrecarga de trabajo y fuga de talento. Aparte de esto, no existe una política o procedimiento formal a nivel del OIJ que establezca la forma a realizar una investigación de delitos informáticos.

3. **Aspecto cultural:**

   Se menciona que los ciudadanos realizan pocos reportes y aparte de esto, solo unos pocos de los incidentes reportados son perseguidos. En

ambos sectores (público/privado) existe carencia de un proceso de respuesta a incidentes.

4. **Aspecto profesional:**

   En el ámbito profesional, las empresas privadas e independientes ofrecen servicios de cómputo forense y sus profesionales se encuentran mejor preparados, pero son pocas empresas. Por otra parte, en el sector público, el perfil del especialista en ciberseguridad no está bien definido por el Servicio Civil. En su lugar, se contrata simplemente a personas con conocimientos generales de informática y no a aquellos especializados en ciberseguridad y cómputo forense. Como resultado, ocurre selección de personal no calificado para el puesto.

   Ha habido esfuerzos para capacitar a profesionales de otras áreas no técnicas, tales como profesionales en derecho y fiscales de la república. Sin embargo, aún hay una gran falta de experiencia. En el sector público, se observa una mejora en los últimos años, gracias al trabajo de la sección de delitos informáticos, y como resultado se observa más presencia de casos de ciberdelitos detectados o detenidos en los medios de comunicación.

4.2.2 ¿Qué buenas prácticas sigue usted al realizar una investigación de delitos informáticos?

Algunos entrevistados mencionan el Protocolo de Cadena de Custodia del OIJ como el único documento nacional de referencia para saber cómo levantar una cadena de custodia. Solo un entrevistado en particular, que se ha dedicado al cómputo forense en el sector público y privado, utiliza una metodología propia desarrollada en su tesis.

En general, los entrevistados recomiendan utilizar y seguir alguno de los estándares internacionales reconocidos tales como las normas ISO, la NIST (800-86). En particular, reconocen la guía para la integración de técnicas forenses en respuesta a incidentes, las normas SANS, la metodología TARA, la Metodología CFREDS. A su vez, es importante tener en cuenta las buenas prácticas recomendadas por los fabricantes de las soluciones tecnológicas.

Algunas buenas prácticas para preservar la cadena de custodia que fueron recomendadas en las entrevistas son los siguientes:

- Evitar la alteración de la prueba o, en su defecto, contaminar la escena.
- Utilizar guantes al manipular la evidencia.
- Usar kits de evidencia que incluyan bolsas, sellado y embalado.
- No apagar el equipo cuando hay un incidente; si el equipo está encendido no apagarlo, si está apagado no encenderlo para evitar alterar la evidencia digital.
- Aislar el equipo, contenerlo en la red.
- Tener conocimientos previos de sistemas operativos.
- Tomar la imagen forense desde un dispositivo en modo solo lectura. Los demás equipos en el laboratorio también deben estar en modo lectura.
- Después de extraer la copia forense, sacar duplicados de las copias y hashes.
- Sacar una línea de tiempo de cada proceso observado.
- Revisar logs y documentar hallazgos.
- Revisar dispositivos de red.
- Realizar la recuperación de archivos.
- Hacer análisis del disco.
- Revisión de malware.
- Utilizar herramientas de visualización.
- Mantener puntos de chequeo para garantizar que la información es la original.

Sumado a lo anterior, algunos entrevistados hicieron especial énfasis en tener buena documentación del proceso. En otras palabras, es mejor documentar en exceso a que haga falta documentación del proceso. También, se debe levantar un acta sobre la escena y documentar el proceso paso a paso, tomar números de serie, marcas, estado del dispositivo, sacar fotografías o grabación audiovisual, de cerca y lejos en la escena y el lugar. Debe existir buena redacción y pensar con anticipación que todo esto llegará a ser leído por jueces, fiscales, abogados. Por eso, debe ser claro y consistente.

4.2.3 ¿Cómo garantiza usted la calidad en la investigación de delitos informáticos?

De acuerdo con los entrevistados, la calidad en la investigación de delitos informáticos se puede lograr desde las siguientes contramedidas. Son pensadas para evitar reproducir los errores comunes más conocidos. Por ejemplo, cómo se debe llevar la documentación a través de la investigación de delitos informáticos. Entonces, es así cómo los expertos coinciden en los siguientes puntos:

- La redacción del documento debe realizarse considerando que va a presentarse ante un tribunal o ser auditado.
- La documentación debe permitir que el proceso sea repetible y, siendo así, que se obtengan los mismos resultados. Solo así se elimina la subjetividad.
- Se recomienda tomar *screenshots*, tomar la hora y fecha, tomar cualquier registro multimedia, tomar números de serie, marcas y estado de los dispositivos encontrados en la escena; tomar fotos de la evidencia (de cerca y largo), fotos del lugar, llevar una lista de los hashes que se obtienen al realizar las copias forenses.
- Desde el momento en que se hace la extracción de la evidencia digital inclusive en el análisis a realizar en el laboratorio, se debe contar con un documento que muestre el inventario del software o herramientas utilizadas que sirvieron durante la investigación.
- Utilizar plantillas para la recolección de indicadores de compromiso (IOCs, por sus siglas en inglés).
- Utilizar plantillas para la recolección de indicadores clave de rendimiento (KPIs por sus siglas en inglés).
- Utilizar plantillas para cada procedimiento.
- Clasificar el tipo de caso que se va a atender. La clasificación de casos facilita identificar cuáles herramientas de software son las recomendadas pues facilita la labor del analista forense digital.
- Dar fe pública con un notario, fiscal, juez o auditor, para certificar que las plantillas utilizadas y el documento final cumplen o no con los pasos estipulados.
- Justificar cómo se llegaron a las conclusiones.
- Basar el trabajo en una norma internacional aceptada.
- Estar al tanto del tiempo que toma la investigación.

- Estar previamente preparado. Por ejemplo, realizar prácticas en laboratorios.
- Usar varias herramientas aunque hagan lo mismo para comparar resultados.
- El embalaje debe incluir etiqueta legible sin tachones. Estas deben indicar qué es lo que se está llevando, por qué se está llevando, donde se recolectó, quien lo recolectó, qué fiscal o juez estuvo presente y firmar todo.
- Tener documentación de apoyo de los proveedores de cada tecnología para poder demostrar que hay o no un comportamiento anómalo de un sistema.
- Trabajar con copias de la evidencia y no sobre la original.
- Implementar un proceso de mejora continua.

4.2.4 ¿Ejemplos de malas prácticas?

Los expertos coinciden que se debería evitar la repetición de las prácticas mencionadas a continuación:

Mal embalaje:

- Mal cerradas las bolsas o realizadas en un medio o lugar inadecuado (agua, golpes).
- Hashes que no corresponden por contaminación de la prueba.
- No etiquetar evidencia.

Mala documentación del proceso:

- Incompleta o inexistente documentación del procedimiento.
- Actas de recolección de indicios mal levantadas o escuetas.
- Omitir información en la documentación.
- Dar una opinión sesgada (personal) sobre la investigación.

Alterar la evidencia:

- Alterar el estado en el que se encontró el equipo (encendido / apagado).
- Fuga de información que pueda alertar a las partes investigadas.
- No activar los logs.

Falta de experticia:

- No asegurar que la tipificación del delito sea correcta.
- No tener, o no saber cuáles herramientas utilizar. Esto hace perder el tiempo que es muy valioso en los casos.
- Depender de una única herramienta *(software / hardware)*.
- Desconocimiento sobre las herramientas y sobre cómo recoger la evidencia.
- Perder la evidencia.
- Recabar pruebas no relacionadas con el caso en cuestión.
- No tener un control cruzado entre los investigadores.

4.2.5 ¿Conoce legislación o procedimientos que guíen a las cortes en la evaluación de la evidencia digital?

Para todos los entrevistados es claro que existe un faltante de procedimientos que establezcan consideraciones necesarias para evaluar la evidencia digital en Costa Rica. Expresaron que en las cortes muchas veces la evaluación de la evidencia por parte del juez depende del convencimiento y comunicación del perito. Resaltaron la importancia de “traducir” el lenguaje técnico en términos más comprensibles para un público no técnico.

Otros entrevistados apuntaron a que existen estándares y marcos de trabajo internacionales de organizaciones como NIST o SANS pero que estos no están amoldados al contexto de Costa Rica. Debido a ello, no son utilizados.

Otro grupo indicó que sí existen métodos pero que estos son a nivel institucional. Además, tienen algún nivel de eficacia, sin embargo, están alineados al contexto institucional, con lo cual se vuelven sesgados e inflexibles.

4.2.6 ¿Existe un faltante de experticia sobre cómputo forense en CR?

Se obtuvieron respuestas variadas a esta pregunta. Sin embargo, la mayoría concuerda en que si existe un faltante y listan las siguientes razones:

- En el sector público las contrataciones son reguladas por el Servicio Civil. Ellos clasifican las diferentes profesiones. El Servicio Civil no establece el perfil de informático forense. Su sistema solo cuenta con un perfil genérico de informático. Esto hace que gente sin experiencia sea asignada en cargos de

cómputo forense que a su vez no son compensados acorde a lo que el perfil de informático forense requiere.

- El perfil de informático forense no cuenta con una formación específica en las universidades. Existen universidades como CENFOTEC que cuentan con perfiles en Ciberseguridad pero estos no están especializados en cómputo forense.
- En el sector privado, hay escasez de profesionales que cuenten con la experiencia y certificaciones necesarias. Esto obliga al sector privado a buscar en el extranjero.
- Los profesionales en derecho (abogados, fiscales y juristas) no se han capacitado lo suficiente en temas de cómputo forense.

Otros entrevistados han indicado que si existe experticia en el área, pero la cantidad de profesionales es limitada. Mencionan los siguientes casos donde sí hay experticia:

- Unidad de Delitos Informáticos del OIJ.
- Empresas que ofrecen servicios de Red Teaming en el extrajero.
- Cluster de Ciberseguridad de la CAMTIC.
- El Centro de Respuesta de Incidentes de Seguridad Informática de Costa Rica (CSIRT-CR), perteneciente al Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT).
- Equipo de Respuesta a Incidentes de Seguridad (CSIRT) del Instituto Costarricense de Electricidad (ICE).
- Comisión de seguridad informática (Castro, *2018*).

4.2.7 ¿Existe mercado para el cómputo forense?

El consenso entre los entrevistados es que sí existe un mercado para el cómputo forense pero este es muy incipiente. Estos son algunos de los comentarios de los entrevistados:

- Es poco probable que una empresa sea rentable en Costa Rica haciendo sólo cómputo forense.
- Si en Costa Rica se implementaran ciberseguros, eso generaría un incremento en la demanda de especialistas en cómputo forense.

- Hoy en día, la práctica del cómputo forense en Costa Rica se centra más en investigaciones judiciales o procesos administrativos.
- Hace falta crear perfiles para informáticos forenses en las universidades.

4.2.8 ¿Áreas de mejora/recomendaciones para la investigación de delitos informáticos en Costa Rica?

Los entrevistados identificaron múltiples oportunidades de mejora en ámbitos profesionales, culturales e inclusive, en la legislación nacional. A continuación, se hará una lista de ello:

- Mejoras profesionales:
    - Los profesionales en el área deben contar con certificaciones reconocidas internacionalmente (SANS, EC-COUNCIL).
    - Crear procesos donde se compruebe la capacidad técnica de quien quiera ejercer.
    - Desarrollar especialidades en universidades pues el cómputo forense debería ser una materia obligatoria o al menos optativa en los planes de estudio (Escuelas de Ingeniería y Derecho).
    - El perfil de un informático forense debe ir más allá de lo técnico e incluir habilidades sociológicas y psicológicas.
- Mejoras culturales a nivel país:
    - Denunciar más los delitos.
    - Dar un contexto país de cómo se percibe el cómputo forense en el marco legal.
    - Una guía que establezca las previsiones necesarias para realizar una investigación de delitos informáticos.
    - Las Instituciones deben contar con un CSIRT.
    - Contar con el apoyo del Colegio de Informáticos.
    - Que se propicie la entrada al país de organizaciones que puedan proveer de ciberseguros. Esto formalizaría el siniestro cibernético y generaría más oportunidad laboral para los profesionales en cómputo forense. Por consiguiente, aumentaría el mercado.
- Mejoras en la legislación nacional:

- Mejorar la tipificación de los delitos informáticos.
- Legislación política, o una ley, para que se pueda evidenciar cuándo se ha sido víctima de un delito complejo y el requerir servicios de peritos informáticos en la demostración.
- Orientar artículos del Código Penal para que se mencione el cómputo forense.

4.2.9 ¿Conoce estándares o documentos que guían al profesional en la investigación de delitos informáticos?

Todos los entrevistados brindaron ejemplos de documentos u organizaciones especializadas en el cómputo forense. La mayoría provienen de organizaciones internacionales pero también hay ejemplos de documentos de entidades costarricenses:

- NIST 800-86
- SANS
- Protocolo cadena de custodia OIJ
- Guia de recoleccion de indicios OIJ
- ISO 27037
- ISACA-COBIT
- Deloitte
- EC-COUNCIL.

4.3 Estándares y buenas prácticas internacionales aplicables a la investigación de delitos informáticos

La evidencia digital ha estado presente en las investigaciones criminales desde los noventas cuando era considerada como simple “evidencia”. Desde entonces, los especialistas en el campo del cómputo forense se han encargado de desarrollar diversos modelos y metodologías para el manejo de la evidencia. Esta investigación ha analizado sistemáticamente los trabajos más recientes en este campo con el objetivo de proponer un estándar nacional que facilite determinar la admisibilidad de la evidencia digital en delitos informáticos.

Se realizó un escrutinio de los estándares y buenas prácticas internacionales aplicables a la investigación de delitos informáticos. Se encontraron marcos de trabajo que describen en varias fases como llevar a cabo el cómputo forense manteniendo la integridad de la evidencia por medio de la documentación de cada acción realizada durante la investigación.

Algunos de estos marcos de trabajo están enfocados a situaciones específicas como ataques de red o legislaciones que aplican a solo un país. Sin embargo, la mayoría son lo suficientemente generales como para ser útiles en esta investigación. En la siguiente tabla, se listan algunos de los marcos de trabajo consultados y su número de fases:

Nombre	Fases
Computer Forensic Investigative Process	4
DFRWS Investigative Model	6
Abstract Digital Forensics Model	9
Integrated Digital Investigation Process	5
Enhanced Digital Investigation Process Model	5
Computer Forensics Field Triage Process Model	6
Digital Forensic Model based on Malaysian Investigation Process	7
Scientific Crime Scene Investigation Model	4
End to End Digital Investigation	6
Extended Model of Cybercrime Investigation	13
A Hierarchical, Objective-Based Framework for the Digital Investigations Process	6
Framework for a Digital Forensic Investigation	3

Common Process Model for Incident and Computer Forensics	3
Dual Data Analysis Process	4
Network Forensic Generic Process Model	9
Generic Computer Forensic Investigation Model	5
Harmonised Digital Forensic Process Model	12
Framework For Establishing Confidence Level of Digital Evidence Admissibility	5

Tabla tomada de Dimpe y Kogeda, 2018.

De la misma manera, se revisó la literatura mencionada en el apartado 1.9.3 de esta investigación. En el Anexo A se listan los documentos consultados.

4.4 Procedimientos que conforman la investigación de delitos informáticos en Costa Rica

Para poder comprender los procedimientos que conforman la investigación de delitos informáticos en Costa Rica, se realizaron entrevistas a expertos en el cómputo forense que operan en el país.

La prueba digital debe ser admisible en un tribunal costarricense y poder resistir las impugnaciones en cuanto a su autenticidad. Por eso, los investigadores deben seguir instrucciones específicas y cumplir con ciertas regulaciones y requisitos que se conocen como buenas prácticas.

Dicho esto, las preguntas de las entrevistas fueron hechas con el objetivo de capturar los intereses nacionales sobre las buenas prácticas aplicadas en Costa Rica en la investigación de delitos informáticos. A continuación, la lista de preguntas:

- ¿Qué buenas prácticas sigue usted al realizar una investigación de delitos informáticos?
- ¿Cómo garantiza usted la calidad en la investigación de delitos informáticos?
- ¿Áreas de mejora/recomendaciones para la investigación de delitos informáticos en CR?

- ¿Ejemplos de malas prácticas?
- ¿Conoce estándares o documentos que guían al profesional en la investigación de delitos informáticos?

Basándose en la literatura consultada en esta investigación y comparándola con la información obtenida en las entrevistas, se identificó un conjunto (no exhaustivo) de buenas prácticas en el cómputo forense empleadas en Costa Rica. Estas prácticas han sido categorizadas dentro de las 5 fases descritas por Proaño (2017):

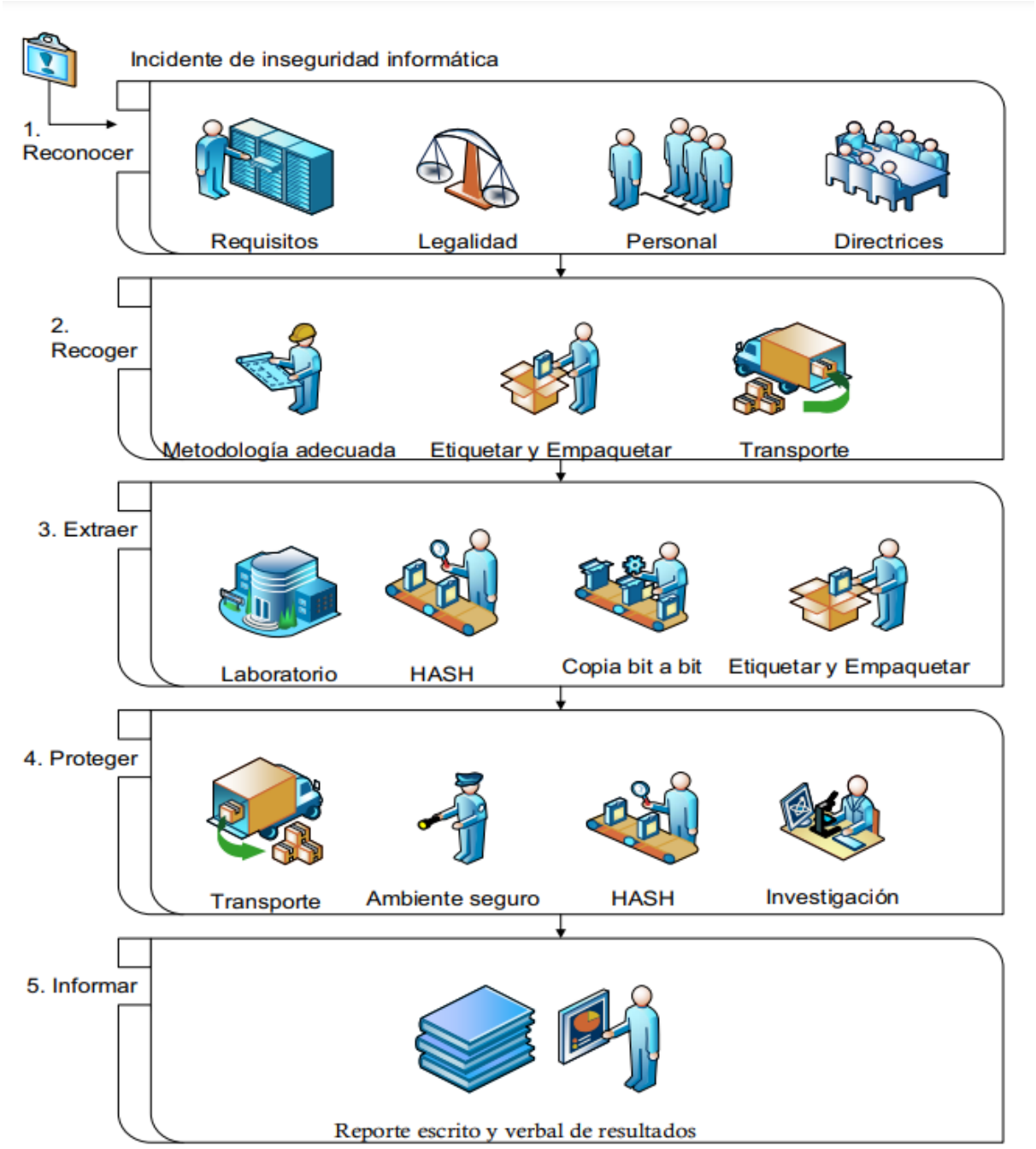


Imagen tomada de Proaño (2017)

1. Reconocer: Se identifican y documentan los dispositivos que contengan datos asociados al incidente.
    - La evidencia puede ser tangible, intangible, visible o no visible. Es por eso que es necesario clasificar y priorizar con base a su volatilidad y criticidad.
    - Utilizar estándares ISO\IEC 27041 y NIST 800-86 para identificar si se requiere un análisis en “vivo” o “muerto”. Además, se debe consultar ISO\IEC 27042 para las herramientas utilizadas en el análisis en vivo.
    - Tomar números de serie, marcas y estado de los dispositivos.
    - Tomar fotos (de cerca y largo) de la evidencia y el lugar.
    - Documentar el proceso asumiendo que el documento va a presentarse ante un tribunal o ser auditado.
    - Asegurar que la tipificación del delito que se persigue sea correcta.

2. Recoger: Retirar la evidencia desde su lugar de origen hacia un ambiente controlado para su posterior extracción y análisis.
    - Se debe mantener el equipo en el estado en que se encontró (Encendido / Apagado).
    - Revisar dispositivos de red.
    - Utilizar guantes al manipular la evidencia.
    - Dar fe pública con un notario/fiscal/auditor que certifique la documentación del proceso.
    - Usar kits de evidencia (bolsas, sellado, embalado).
    - El embalaje debe incluir etiquetas legibles sin tachones que indiquen qué se está llevando, por qué se está llevando, dónde se recolectó, quien lo recolectó, qué fiscal o juez estuvo presente y firmar todo.
    - Cerrar bien las bolsas de embalaje y almacenarlas apropiadamente (evite agua, golpes, entre otros).

3. Extraer: Consiste en la extracción de la evidencia digital sin alterarla, documentando todo el proceso.

- La documentación debe permitir que el proceso sea repetible y además, arrojar los mismos resultados para eliminar la subjetividad.
- Sacar duplicados y hashes, 2 copias.
- Evite depender de una única herramienta (Software / Hardware).
- Etiquetar evidencia.
- Tomar la imagen desde un dispositivo en modo solo lectura.

4. Proteger: Se protege la integridad de la evidencia digital y se realiza la investigación de la información recabada.
    - Es necesario evitar fugas de información que pueda alertar a las partes investigadas.
    - Sacar una línea de tiempo de cada proceso observado.
    - Aislar el equipo, contenerlo en la red.
    - Contar con un documento de inventario del software utilizado.
    - Trabajar con copias de la evidencia y no sobre la original.
    - Usar varias herramientas aunque hagan lo mismo para comparar resultados.

5. Informar: Consiste en la presentación de la evidencia digital y las conclusiones que derivan de ella, argumentando los resultados obtenidos y justificando el proceso que llevó a la obtención de esos resultados.
    - Utilizar herramientas de visualización.
    - Tener documentación de apoyo de los vendedores de cada tecnología para poder demostrar que hay un comportamiento anómalo de un sistema.
    - Justificar cómo se llegaron a las conclusiones.

4.5 Puntos de mejora en la investigación de delitos informáticos en Costa Rica

Utilizando la base de conocimientos obtenidos en la revisión de la literatura y las respuestas de los entrevistados, se identificó varios puntos de mejora en la investigación de delitos informáticos en Costa Rica. Algunos de estos puntos de

mejora no son tareas puntuales a la hora de ejecutar una investigación, sino más bien temas de fondo que involucran cambios culturales, organizacionales, legales y hasta académicos.

Así por ejemplo, algunos entrevistados apuntan a que los profesionales en cómputo forense deben contar con certificaciones reconocidas internacionalmente por organizaciones como SANS o EC-COUNCIL. También mencionan que el sector público debe crear procesos donde se compruebe la capacidad técnica. Se menciona también la necesidad de desarrollar especialidades en cómputo forense en las universidades o incluir el tema como una materia optativa en los planes de estudio tanto en ingeniería como en derecho. Esto con la intención de formar más perfiles profesionales en cómputo forense en diferentes ámbitos profesionales, yendo estos perfiles más allá de lo técnico, incluyendo habilidades sociológicas y psicológicas.

Los entrevistados mencionaron también la necesidad de mejorar la tipificación de los delitos informáticos pues la actual conlleva a que casi todo delito pueda ser considerado un delito informático y esto causa saturación de casos en el OIJ.

Como resultado, esta saturación provoca que pocos casos sean investigados y, aún menos, resueltos. Sumado a ello, la población no denuncia y quedan delitos impunes. Además, apuntaron a la posible modificación del código penal para que se aborde el cómputo forense y la creación de algún instrumento legal que ampare a las víctimas en casos complejos donde se requiera de peritos informáticos

Se habló también de la necesidad de crear una guía bajo el contexto del marco legal costarricense que defina las consideraciones previas y los pasos a seguir para abordar una investigación de delitos informáticos. Un documento que le sirva a entidades públicas y privadas como un checklist sobre qué hacer en casos donde se necesite una investigación de delitos informáticos. Un documento que cuente además con un anexo que liste las posibles herramientas a utilizar, y en qué casos utilizarlas.

Sin embargo, uno de los temas más recurrentes, tanto en las entrevistas como en la literatura, es el aseguramiento de la cadena de custodia. En este tema, los entrevistados indicaron que en Costa Rica se dan casos de mal embalaje donde las bolsas que transportan la evidencia quedan mal cerradas, se encuentran hashes

que no corresponden debido a contaminación de la prueba o evidencia sin etiquetar. También se encuentra documentación del procedimiento incompleta o inexistente, fuga de información que puede alertar a las partes investigadas, actas de recolección de indicios mal levantadas o escuetas, o peritos que dan una opinión sesgada desde lo personal sobre la investigación.

Muchas de estas deficiencias pueden ser mejoradas implementando los marcos de trabajo, estándares y buenas prácticas descritas en los apartados 4.3 y 4.4 Los beneficios de implementar este tipo de instrumentos en la investigación de delitos informáticos son muchos y su efectividad ha sido puesta a prueba. Por ejemplo, en una investigación en Ecuador se obtuvieron los siguientes resultados:

> *La guía metodológica aplicada, garantizó que la evidencia digital seleccionada sea auténtica e íntegra, incluso que la muestra obtenida pueda ser utilizada en cualquier jurisdicción. Se obtuvo pruebas digitales previo inventario detallado de los elementos de convicción (...) Se manipuló la prueba digital sin comprometerla, evitando un mal manejo de la evidencia digital (...) Se usó estándares, buenas prácticas y documentación de procedimientos, los cuales aseguraron integridad y confiabilidad del peritaje informático a través de las fases propuestas que son: reconocer, recoger, extraer, proteger e informar pruebas suficientes y relevantes, obteniendo resultados detectables, ubicables y trazables* (Proaño, 2017).

4.6 Determinar la admisibilidad de la evidencia digital.

En el modelo propuesto por Antwi-Boasiako & Venter (2017) se explica que la admisibilidad de la evidencia digital en procesos judiciales se sustenta de dos requerimientos: los técnicos y los legales. La relación entre estos fundamentos técnico-legales permite a las partes interesadas determinar el nivel de confianza en la admisibilidad de la evidencia digital.

4.6.1 Requerimientos técnicos

Son extraídos de estándares, investigación académica, precedentes legales o jurisprudencia, opiniones de expertos, entre otras fuentes. Cada requerimiento técnico ayuda a determinar el peso de una evidencia en particular.

El trabajo presentado por Antwi-Boasiako & Venter (2017) analiza los siguientes ocho requerimientos técnicos. Se debe hacer la salvedad de que no son los únicos ni los mejores, simplemente son, en la experiencia, los que aplican de forma genérica a la mayoría de casos.

4.6.1.1 Modelos usados en el cómputo forense

El procedimiento para extraer evidencia digital de un teléfono móvil es diferente al de un disco duro. Tomando en cuenta que esto aplica para múltiples escenarios y tecnologías, cuando la corte evalúa la admisibilidad de la evidencia, esta debe considerar los procedimientos forenses específicos que fueron usados para extraer y procesar la evidencia en cuestión. Los modelos en el cómputo forense agrupan un número de lineamientos para asegurar que los procedimientos forenses apropiados sean utilizados cuando se conduce la investigación. Un ejemplo de estos procedimientos son los desarrollados por la organización ISO o la NIST.

4.6.1.2 Herramientas para la investigación de delitos informáticos

Los practicantes del cómputo forense tienen acceso a un amplio catálogo de herramientas de código abierto y propietarias para tener asistencia en la recolección, análisis y preservación de la evidencia digital. A pesar de esto, no existen reglas generales que gobiernen el uso de las herramientas para la investigación de delitos informáticos. Eso sí, hay un consenso general en la comunidad científica de que las herramientas forenses deben ser probadas o validadas y su tasa de errores debe estar bien documentadas. La validación de dichas herramientas cuenta como criterio para determinar la admisibilidad de la evidencia digital. Organizaciones como la NIST y la ISO han desarrollado marcos de trabajo y métodos para probar las herramientas en forense digital (ISO, 2012).

4.6.1.3 Cadena de custodia

Consiste en una serie de procedimientos para preservar la integridad y dar trazabilidad al manejo de la evidencia digital. De acuerdo con Antwi-Boasiako y Venter (2017), la cadena de custodia es un proceso usado para mantener y documentar de manera secuencial el historial de la evidencia. A su vez, las terceras partes independientes deberían ser capaces de rastrear el movimiento de la evidencia desde la escena del crimen, paso por paso, en la cadena de custodia hasta llegar a la corte. Se afirma que la evidencia digital debería ser aceptada como válida en la corte sólo si puede establecerse su cadena de custodia.

4.6.1.4 Analista / experto en cómputo forense

Las calificaciones profesionales de un analista forense digital son también un requerimiento y criterio de evaluación importante relacionado con la admisibilidad de la evidencia digital. El cómputo forense es una ciencia multidisciplinaria que se compone de tecnologías de la información, habilidades de investigación y leyes, entre otras cosas.

4.6.1.5 Laboratorio de cómputo forense

Un laboratorio de forense digital bien organizado que cuenta con los procedimientos operativos estándar (SOPs) y sistemas de aseguramiento de la calidad impacta positivamente el proceso investigativo. Consecuentemente, impacta también la calidad de la evidencia producida. La asociación conocida como Chief Police Officers Good Practice Guide (Williams QPM, 2012) enlista un conjunto de lineamientos para establecer y operar un laboratorio forense digital.

Es importante resaltar que un fallo en adoptar los procedimientos operacionales establecidos podría alterar el estado original y el estado de la data almacenada en un dispositivo. Por ejemplo, utilizar instalaciones en pésimas condiciones o procedimientos de almacenamiento inapropiados podría resultar en que la evidencia sea tratada como inadmisible en un proceso penal.

4.6.1.6 Verificación de la integridad técnica

El mantenimiento y la verificación de la integridad de cada pieza de evidencia digital son consideraciones técnicas importantes que pueden impactar la admisibilidad. Los analistas en forense digital han adoptado una variedad de métodos para mantener y demostrar la integridad de la evidencia digital. Por ejemplo el uso de los dispositivos *Write Blockers* que, como su nombre indica, bloquean la escritura. Estos son un requerimiento forense estandarizado para mantener la integridad del dispositivo. Las firmas digitales, encriptación y algoritmos hash son empleados para mantener, validar y demostrar la integridad de la evidencia digital (Antwi-Boasiako & Venter, 2017).

4.6.1.7 Testigo experto en cómputo forense

Los testigos expertos en cómputo forense son individuos con experiencia relevante. Sus conocimientos y habilidades son comúnmente requeridos para servir como testigos expertos en procesos judiciales, de acuerdo con la U.S. Federal Rules of Evidence. Un testigo experto debe estar calificado en las bases de conocimiento, experticia, experiencia, educación o entrenamiento. El conocimiento científico, técnico y cualquier otro conocimiento especializado que posea un testigo experto permite al individuo testificar a los hechos en cuestión (Antwi-Boasiako & Venter, 2017).

4.6.1.8 Reporte de la investigación de delitos informáticos

El reporte producido por una investigación de delitos informáticos es una consideración técnica importante que soporta la admisibilidad de la evidencia digital. Según Garrie (2014), un reporte forense digital debe tener conclusiones que sean reproducibles por terceras partes. Así mismo, afirman que las conclusiones que no sean reproducibles no deben tener credibilidad en procesos legales. Un ejemplo de esto es el caso Republic vs. Alexander Tweneboah (Ghana Suit No. TB 15/13/15 of 2016) donde la corte se dirigió en contra de un reporte forense emitido por un testigo experto que trabajaba con la compañía e-Crime Bureau. En este caso, el juez

consideró que el reporte no incluía y no representaba toda la evidencia contenida en un CD que era parte del caso.

4.6.2 Requerimientos legales

La mayoría de jurisdicciones tienen requerimientos legales que proveen los cimientos para la admisibilidad de la evidencia digital en los procederes legales (Antwi-Boasiako & Venter, 2017). Esta sección discute los problemas legales pertenecientes a la admisibilidad de la evidencia digital.

4.6.2.1 Autorización legal

Evaluar la evidencia digital a menudo requiere de una autorización legal. Los derechos humanos, la protección y privacidad de los datos tiene un impacto en víctimas y acusados, por consiguiente debe ser tomado como un asunto primordial.

Dicho esto, pueden existir excepciones. La ley generalmente provee de controles para la protección de los derechos individuales. Obtener la autorización legal otorga legitimidad judicial a la evidencia en cuestión. De hecho, este podría ser el paso más importante en la recolección y manejo de la evidencia digital (Antwi-Boasiako & Venter, 2017).

Por ejemplo, una orden de registro es normalmente requerida para incautar dispositivos electrónicos y evidencias digitales. Fallar en conseguir una autorización legal puede descalificar la evidencia y poner en peligro todo el caso. Admitir evidencia que no fue soportada por la autorización legal podría resultar en que los fiscales y las fuerzas del orden involucradas estén atropellando las libertades civiles.

4.6.2.2 Relevancia de la evidencia digital

La relevancia es un criterio determinante para la admisibilidad de la evidencia digital. De acuerdo con Antwi-Boasiako y Venter (2017) para que la evidencia sea admisible, debe ser suficientemente relevante a los hechos en litigio. La evidencia no puede ser admisible si no se considera relevante. Para que una pieza de evidencia pueda considerarse relevante en un proceder legal, esta debe tender a probar o desaprobar un hecho sobre el caso. La evidencia que tiene valor probatorio

debe probar que el hecho en cuestión es más (o menos) probable de lo que sería sin la evidencia.

4.6.2.3 Autenticidad de la evidencia digital

La autenticidad impacta la confianza en la evidencia. De acuerdo con Antwi-Boasiako y Venter (2017) para que la evidencia digital sea admitida en la corte debe haber evidencia aducida que respalde y demuestre que la evidencia en cuestión es lo que se supone que es. En el caso de “The American Express Travel Related Services Company Inc. vs. Vee Vinhneem” la corte dio el fallo en contra de American Express por no justificar la autenticidad de los registros utilizados. American Express apeló, pero el tribunal de apelaciones reafirmó la decisión de la corte.

De esta manera, para que un registro digital pueda ser admisible, la corte deberá ser convencida de que el registro en cuestión fue de hecho generado por el individuo del cual se supone que le pertenece la autoría.

4.6.2.4 Integridad de la evidencia digital

La integridad se refiere a la solidez de la evidencia digital. La integridad implica que la evidencia se encuentra completa e inalterada. Una evaluación de la integridad de la evidencia es un requerimiento primario para la admisibilidad de la evidencia digital y sirve de base para determinar el peso de la evidencia.

Antwi-Boasiako y Venter (2017) sostienen que la integridad de la evidencia digital no es una condición absoluta más bien es un estado de relaciones. Al evaluar la integridad de la evidencia digital, las cortes pueden considerar varios factores y relaciones.

Las cortes requieren que la integridad de la evidencia sea establecida y garantizada durante la investigación. Por eso, la evidencia deberá ser preservada ante modificaciones durante todo el ciclo de vida de la investigación de delitos informáticos. En Sudáfrica por ejemplo, la originalidad de la evidencia depende de su integridad como se señala en la sección 14(2) del acta de comunicación y transacciones de 2002.

4.6.2.5 Fiabilidad de la evidencia digital

Para que la evidencia se considere confiable, “no debe haber nada que arroje dudas sobre cómo se recopilaron las pruebas y posteriormente se manejaron” (Leroux, 2004). En un caso judicial muy conocido en Estados Unidos, “Daubert v. Merrell”, se consolida la base para evaluar el nivel de confianza de la evidencia científica en los Estados Unidos De América. Este célebre caso especifica cinco criterios para evaluar el nivel de confianza (y por extensión, la admisibilidad) de la evidencia digital:

1. Si la técnica ha sido probada.
2. Si la técnica ha sido sometida a revisión por pares.
3. Si existe una tasa de error conocida asociada con la técnica.
4. Si existen y se mantuvieron las normas que controlan sus operaciones.
5. Si la técnica es generalmente aceptada por la comunidad científica.

Capítulo 5. Propuesta de solución

5.1 Introducción

Esta es la primera versión de un estándar que permite determinar la admisibilidad de la evidencia digital en delitos informáticos. A continuación, se presentan una serie de requerimientos base segregados en un modelo de 6 fases las cuales son: Reconocimiento, Recolección, Extracción, Protección, Análisis e Informe.

Estos requerimientos están inspirados en la jurisprudencia y el Código Legal Costarricense. Se suma a esto, el punto de vista experto de costarricenses que se dedican al cómputo forense así como los estándares reconocidos internacionalmente tales como el ISO 27037, la NIST (800-86), en particular, la guía para la integración de técnicas forenses en respuesta a incidentes. El documento reúne los lineamientos mínimos considerados por los profesionales que ejecutan el cómputo forense. También está dirigido a cualquier interesado en saber cómo determinar la admisibilidad de la evidencia digital.

Este estándar funciona como una herramienta que facilita el entendimiento de los pasos en una investigación de delitos informáticos. Está destinado tanto a personas que no tienen relación con el cómputo forense, como a personas familiarizadas con la informática y desean comprender de manera detallada los procedimientos científicos para dar trazabilidad y resguardar la integridad de la evidencia digital.

5.2 Fases

El estándar está inspirado en las fases del cómputo forense descritas por Proaño (2017) más la inclusión de una fase de análisis a criterio de los investigadores. Cada fase cuenta con una serie de requerimientos mínimos que se deben seguir a la hora de realizar una investigación de delitos informáticos.

5.2.1 Reconocimiento

En esta fase se identifican y documentan los dispositivos que contengan datos asociados al incidente. Se toma en cuenta la autorización legal, el levantamiento de la cadena de custodia y las medidas para garantizar la autenticidad e integridad de los indicios. Los siguientes requerimientos deben ser considerados para garantizar la admisibilidad de la evidencia digital.

El analista debe contar con las calificaciones requeridas para completar una investigación de delitos informáticos.

Es importante tomar en cuenta las calificaciones profesionales del analista forense digital encargado de la investigación. Esto formará parte de los criterios de evaluación al determinar la admisibilidad de la evidencia digital. Se recomienda que el perfil del analista forense digital incluya certificaciones emitidas por organizaciones reconocidas internacionalmente (SANS, EC COUNCIL, ISO, NIST, entre otros).

El perfil de un informático forense además, debe ir más allá de lo técnico e incluir habilidades sociológicas y psicológicas. Es recomendable que además tenga conocimiento de la legislación costarricense, específicamente en materia de delitos informáticos.

Algunas organizaciones requieren que todos los miembros de sus equipos forenses aprueben exámenes anuales sobre sus competencias. La revisión periódica de políticas, pautas y procedimientos también ayuda a asegurarse de que la organización se mantendrá al día con las tendencias en tecnología y los cambios en la ley (Stine, 2008).

Se debe levantar la cadena de custodia utilizando los formatos oficiales del Ministerio de Seguridad Pública o los recomendados por estándares internacionales.

La cadena de custodia está respaldada por diversos documentos jurídicos. Estos resaltan su necesidad y relevancia para el proceso investigativo. Entre las

resoluciones jurisprudenciales dictadas por la Sala Constitucional y fortalecedoras de nuestra disciplina, cabe citar el voto número 1739-92 de julio de 1992. En dicho voto se indica que representa: “(...) un fallo histórico porque contiene una serie de apreciaciones jurídicas de gran valor para la institucionalidad del país y para el mantenimiento de nuestra democracia (…)” De esa resolución deriva un concepto esencial: el Debido Proceso.

Del voto antes señalado, también se extrae el principio de inmediación de la prueba. Este es necesario para que todos los sujetos procesales reciban la prueba de una manera directa, inmediata y simultánea, para que llegue a conocimiento de la persona juzgadora sin alteración alguna, en estricto apego a las exigencias del principio general de legalidad, que se extreman en el campo del proceso penal (OIJ, 2020).

Por lo tanto, se indica que la custodia inicia desde el hallazgo del indicio. Sin embargo, la cadena de custodia iniciará a partir de la recolección del indicio, por los mecanismos establecidos de identificación, bajo un estricto control, que garantice en las diferentes etapas del proceso, su identidad y seguridad jurídica. En el Anexo C se puede encontrar un ejemplo sobre cómo elaborar una boleta única de cadena de custodia de indicios.

<u>El analista deberá contar con las herramientas mínimas necesarias.</u>

Los analistas deben contar con un conjunto de herramientas forenses para la recopilación, el examen y el análisis de datos. Eso debe contener varias herramientas que brinden la capacidad de recopilar y examinar datos volátiles y no volátiles. Además, debe permitir realizar revisiones rápidas de datos, así como análisis en profundidad. En fin, el conjunto de herramientas debe permitir que sus aplicaciones se ejecuten de manera rápida y eficiente desde medios extraíbles (por ejemplo, disquete, CD) o en un laboratorio forense. En el Anexo H se provee una lista de recursos forenses.

<u>La escena del incidente debe ser documentada de manera visual.</u>

El analista al llegar a la escena del incidente debe inmediatamente documentar visualmente su estado por medio de fotografías, videos o dibujos. Se deberá también documentar cualquier elemento dentro de la escena que pueda resultar relevante: notas de escritorio, libretas, apuntes, diarios, documentos impresos, facturas, entre otras.

De acuerdo con el Protocolo de Cadena de Custodia del OIJ, debe utilizarse un disco maestro para el almacenamiento de todas las fotografías digitales y videos tomados durante la atención del sitio de suceso. El disco debe ser embalado en un sobre registrado bajo la orden de trabajo N° ot.48130, como se observa en la siguiente imagen:


PODER JUDICIAL
República de Costa Rica

OIJ

OFICINA: _____

Número único: _____

Asunto: _____

Fecha(s) de toma: _____

Nombre de quien fotografía: _____

Fecha de almacenamiento: _____

Nombre de quien almacena: _____

☐ CD-R: ☐ DVD+R: ☐ DVD-R: ☐ Otro: _____

Marca: _____ Espacio utilizado: _____

Código de puntos: _____

Disco Maestro

_____ - _____ - M_____

Imagen tomada del Protocolo de Cadena de Custodia del OIJ.

<u>Identificar los dispositivos digitales que necesitan ser recogidos.</u>

El analista deberá identificar y documentar todos los dispositivos que necesiten ser recolectados posteriormente: mainframes, servidores, computadoras de escritorio, puntos de acceso, conmutadores, concentradores, enrutadores,

dispositivos móviles, PDA, PED, dispositivos Bluetooth, sistemas de CCTV y muchos más. Deberá indicar detalles como el tipo de dispositivo, su marca, número de serie, IMEI y modelo. En el caso de los dispositivos móviles se deberá tomar en cuenta las tarjetas de memoria, tarjetas SIM, número IMEI, cargadores, código PIN y código PUK.

El estado de los dispositivos debe mantenerse tal y como se encuentra.

En la fase de identificación, el estado de los dispositivos y sus periféricos no debe alterarse. Esto significa que si se encuentra apagado no debe encenderse y si se encuentra encendido no debe apagarse. No debe tampoco desconectarse ninguno de los periféricos conectados al dispositivo.

Incumplir con estas recomendaciones puede llevar a la generación de pruebas contaminadas o espurias. Si el dispositivo está encendido el analista deberá tomar una fotografía de lo que se esté mostrando en pantalla o documentarlo de manera escrita incluyendo una descripción de lo que se muestra en pantalla (títulos, textos, contenidos, imágenes, posiciones de ventanas y otros).

Identificar sistemas de videovigilancia.

El analista deberá identificar la existencia de sistemas de circuito cerrado (CCTV). Se debe anotar el número de cámaras conectadas al sistema así como el detalle de cuales estaban operando y cuáles no. El analista deberá documentar detalles como la marca, el modelo y la configuración del sistema, la configuración de visualización, la configuración de grabación y la ubicación de almacenamiento. De modo que si se deben realizar cambios en el proceso de extracción sea posible devolver el sistema a su estado original.

Identificar los servicios prestados por los dispositivos de red.

El analista debería identificar los dispositivos de red en la escena y comprender qué servicios están ofreciendo. Esto es importante para entender su

criticidad y sus dependencias antes de proceder a remover el dispositivo de la red. Algunos de estos dispositivos pueden estar cumpliendo funciones críticas que no toleren tiempos de inactividad. Sin embargo, si el analista concluye que el dispositivo es parte de un ataque malicioso activo deberá desconectarlo para proteger la integridad de la evidencia digital.

Identificar posibles cargadores de batería y cables de los dispositivos.

Los dispositivos que se encuentren encendidos podrían llegar a descargarse generando así pérdida de información. El analista deberá, desde un inicio, identificar cualquier cargador o cable que sirva de suministro de energía a los dispositivos.

Utilizar un detector de señales inalámbricas.

Con el objetivo de identificar posibles señales inalámbricas emitidas desde dispositivos ocultos, el analista deberá utilizar un detector de señales inalámbricas. Si por razones de costo u otras limitaciones no se puede utilizar un detector de señales inalámbricas entonces el analista deberá documentarlo incluyendo una justificación.

Identificar a las personas responsables de las instalaciones/dispositivos en el lugar de los hechos.

Es posible que las personas que se encuentren en la escena cuenten con información adicional y documentación que ayude a la investigación. Por ejemplo, las contraseñas de los dispositivos, configuraciones del sistema y credenciales de administrador. El analista deberá, por ejemplo, entablar una conversación, cuando sea posible, con el administrador del sistema, el dueño del dispositivo, usuarios de computadoras y periféricos. Se debe documentar el nombre de la persona, su rol y la información que facilitó.

El proceso de identificación de la evidencia digital debe ser documentado.

La documentación del procedimiento inicia desde el momento en que se reportó el incidente. Esto será clave y servirá para construir la cadena de custodia. Se debe generar la mayor cantidad de documentación posible. Incluir cada paso del procedimiento que identifique de manera única cada dispositivo. Esto puede ser considerado evidencia digital.

Además, hay que describir el estado en el que se encuentra la evidencia, material audiovisual (fotos de los 4 lados, de cerca y de largo, grabaciones y videos). Todo debe estar señalado con números de serie, marcas y estado de los dispositivos que incluya señas identificativas como golpes o daños específicos.

Se debe documentar el proceso asumiendo que el documento va a presentarse ante un tribunal o ser auditado. Desde ese punto, debe ser posible identificar la cronología del manejo de la evidencia.

Algunas preguntas que pueden ayudar a la identificación de la cronología y deberán adjuntarse a la boleta única de cadena de custodia son:

- ¿Quién accedió a la evidencia?
    - ¿Dónde y cuándo?
- ¿Quién revisó la evidencia ?
    - ¿Cuándo?
- ¿Por qué la evidencia se revisó?
    - ¿Quién lo autorizó?
- Si hubo modificaciones inevitables a la evidencia digital,
    - ¿Quién fue el responsable?
    - ¿Cuál es su justificación?

La evidencia digital debe ser clasificada en base a su volatilidad.

A la hora de buscar elementos que puedan contener evidencia digital en potencia, el analista deberá priorizar la recolección basándose en la volatilidad. La evidencia digital puede ser tangible, intangible, oculta o visible. Por ello, para obtener la mejor evidencia se debe identificar la volatilidad de los datos. De esta

forma, se asegurará el correcto orden del proceso de recolección y minimizando el daño infringido en la evidencia en potencia. La volatilidad según (Castilla Guerra, 2013) puede ser clasificada en tres categorías:

- Altamente volátil.
    - CPU (Registros Cache) y Memoria de Video. Usualmente la información en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de memoria del sistema (Castilla Guerra, 2013).
- Medianamente volátil.
    - RAM. Incluye información sobre los procesos en ejecución, el hecho de capturarla hace que cambie. Requiere conocimiento especializado para poder reconstruirla, pero no se requiere mucho conocimiento para hacer una búsqueda de palabras clave (Castilla Guerra, 2013).
- Poco volátil.
    - Medios fijos (Discos Duros). Incluye área de SWAP, colas, directorios temporales, directorios de registro – logs y otros directorios. La información recolectada en el área de SWAP y las colas permite analizar los procesos y la información de los mismos en un punto del tiempo particular. Los directorios permiten reconstruir eventos (Castilla Guerra, 2013).
    - Medio removible (Cintas, CD-ROM). Usualmente son los dispositivos para el almacenamiento de contenidos históricos del sistema. Si existen previamente a un incidente pueden ser usadas para acortar el periodo de tiempo en el cual sucedió (Castilla Guerra, 2013).
    - Medio impreso (Papel). Difíciles de analizar cuando son muchos. Ya que no se pueden realizar búsquedas automáticas sobre ellos (Castilla Guerra, 2013).

Utilizar algún documento de referencia reconocido para la identificación de la evidencia digital.

Es ampliamente recomendado por expertos en cómputo forense utilizar estándares reconocidos como referencia para la fase de reconocimiento. Algunos ejemplos de estos estándares son ISO\IEC 27037, ISO\IEC 27041, NIST 800-86 o el protocolo de cadena de custodia del Organismo de Investigación Judicial de Costa Rica.

5.2.2 Recolección

Una vez identificados todos los dispositivos con evidencia digital potencial se procede a retirar la evidencia desde su lugar de origen hacia un ambiente controlado para su posterior extracción y análisis. Los dispositivos que contienen la evidencia pueden estar encendidos o apagados; las herramientas y procedimientos a seguir dependen del estado del dispositivo.

La evidencia física debe ser recolectada.

Durante el proceso de recolección de evidencia se debe recoger evidencia física que pueda ser relevante. Algunos ejemplos pueden ser: documentos impresos, cargadores de los dispositivos, cables, baterías externas, UPS y notas que contengan direcciones web, nombres de usuario o claves.

Realizar un análisis de rastros biológicos previo a la manipulación de los dispositivos electrónicos.

Los dispositivos electrónicos pueden contener evidencia biológica latente. Por esta razón, se recomienda utilizar guantes al manipular los dispositivos que puedan contener posible evidencia digital. En algunos casos es recomendable esperar a que se realice cualquier análisis asociado al seguimiento de rastros biológicos para después manipular los dispositivos electrónicos de almacenamiento.

Se recomienda seguir el manual de evidencia digital de la OEA el cual indica que “(...) no se debe tomar los objetos sin guantes de hule, podría alterar, encubrir o hacer desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático” (Acurio Del Pino, 2004).

Documentar el proceso de etiquetado y empaquetado de la evidencia digital.

Se debe etiquetar la evidencia de manera legible, sin tachones y documentar qué es lo que se está recogiendo, por qué se está recogiendo, dónde se recolectó, quien lo recolectó, y de ser posible, qué fiscal o juez estuvo presente al momento de la recolección.

Además, se debe contar con la firma de un juez o fiscal para obtener fe pública que certifique la documentación del proceso principalmente en investigaciones penales. Todos los cables que se recogen deben ser etiquetados junto con una descripción del puerto al que estaban conectados. Así se podrá reconstruir el estado del sistema posteriormente.

Igualmente, se debe revisar y documentar el contenido de las bandejas de CD/DVD, puertos USB, la unidad de disco flexible. Hay que incluir el estado en el que se encuentran los interruptores de los dispositivos recolectados ya que si estos cambian pueden alterar la integridad de la evidencia digital.

De acuerdo con el Ministerio Público y el Protocolo de Cadena de Custodia del OIJ, este es un proceso esencial al momento de la recolección de un indicio. Esto se debe a que guarda, protege, preserva y asegura el elemento de interés recolectado. Para ello, se requiere de la aplicación de pasos básicos como el sellado, lacrado y etiquetado (completamente confeccionado) del soporte que contiene el indicio. Cabe destacar que el uso de los sellos, lacrados y etiquetados es obligatorio y se aplican con la finalidad de proteger el indicio o la evidencia, y así garantizar su identidad.

Justificar la exclusión de dispositivos digitales en el proceso de recolección.

Si algún dispositivo digital no fue recogido debe existir una justificación para ello. Además, se debe documentar los detalles del dispositivo. Esto es necesario para no generar dudas sobre la omisión de evidencia.

Crear una copia de los datos volátiles y del estado actual de los dispositivos antes de apagarlos.

Al apagar un dispositivo se puede perder información potencialmente valiosa como llaves de cifrado, datos corporativos, contenido del portapapeles, puertos y conexiones de red abiertas, aplicaciones y procesos en ejecución, archivos temporales y de caché, unidades de red conectadas y otros datos cruciales que se alojan en la memoria activa o en la memoria inactiva que aún no se ha borrado. Para evitar esa pérdida de información, se deben realizar copias de los datos volátiles y del estado actual del dispositivo antes de apagarlo. Para realizar las copias se deben utilizar herramientas confiables y validadas previamente.

Remover la batería en vez de presionar el botón de apagado en el caso de las laptops.

Presionar el botón de apagado puede disparar la ejecución de algún código malicioso que altere o elimine información importante antes de apagar el dispositivo. Esta acción puede también alertar a sistemas conectados para que destruyan evidencia digital aún no identificada. Por estas razones, lo mejor es remover la batería después de recolectar la información volátil. Se debe también revisar si hay un cargador conectado, el cual debe ser removido después de quitar la batería.

Apagar los dispositivos desconectando directamente la fuente eléctrica.

Dependiendo de las configuraciones del dispositivo, el analista deberá determinar si el dispositivo a recoger debe apagarse y de qué forma este debe ser apagado. En caso de que sea necesario desconectarlo directamente de la fuente eléctrica, el analista debe quitar el cable de suministro de energía quitando primero

el extremo conectado al dispositivo digital y no el extremo conectado al enchufe. Tener en cuenta que los datos pueden sufrir alteraciones si se quita el cable de alimentación del enchufe y no del dispositivo.

Recoger los dispositivos encendidos sin interrumpir el suministro de electricidad.

En casos donde se dan ataques con técnicas de cifrado (ransomware por ejemplo) puede volverse necesario mantener el dispositivo encendido para lograr extraer la llave de cifrado alojada en memoria. Existen herramientas de hardware que permiten desconectar el dispositivo de la red eléctrica y transferirlo a un banco de energía portátil sin interrumpir la alimentación del dispositivo. Sin embargo, cuando se recoge un dispositivo de esta forma se deben tener en cuenta cuestiones como el enfriamiento, protección contra golpes, duración de la carga, entre otras.

Tomar las precauciones necesarias para evitar que la electricidad estática genere daños al retirar un disco duro.

Si es necesario retirar el disco duro, entonces el analista debe tener cuidado con la energía electrostática del ambiente y de su propio cuerpo. Esta puede dañar el disco duro. Para ello puede utilizar una pulsera antiestática o tocar una superficie metálica antes de manipular el disco. De lo contrario, el disco duro no se debe retirar. En este caso, se debe etiquetar como disco duro sospechoso y documentar todos sus detalles, entre ellos la marca, el nombre del modelo, el número de serie y el tamaño del disco duro.

Los dispositivos de la red deben ser aislados.

En algunos casos puede ser necesario mantener ciertos dispositivos conectados a la red para que el analista pueda monitorear su comportamiento. Por otro lado, si existe certeza que ninguna información relevante va a ser alterada, entonces el analista deberá aislar el dispositivo de la red desconectando el cable de red o removiendo la conexión Wi-Fi.

Antes de aislar el dispositivo, el analista deberá documentar todas las conexiones existentes y sus puertos para una futura reconstrucción de la red. Además, debe asegurarse que no haya ningún otro método de comunicación activo, como lo puede ser bluetooth, infrarrojo o tarjetas telefónicas. El objetivo de todas estas medidas es proteger la destrucción de posible evidencia digital.

Se deben revisar los sistemas de videovigilancia.

El analista deberá revisar los sistemas CCTV y determinar si son relevantes para la investigación. Posteriormente, deberá determinar si el sistema documentó la secuencia de video de interés, encontrar el rango de tiempo de las secuencias de video requeridas y comparar el tiempo del sistema con el tiempo correcto y documentar cualquier diferencia.

El analista también debe determinar qué cámaras se requieren y si se pueden tomar por separado. Se debe anotar la marca y el modelo del sistema. Esta información puede ser necesaria para obtener el software de reproducción correcto.

5.2.3 Extracción

En esta fase se realiza la extracción de la evidencia digital. Se deben producir copias de discos duros, particiones, archivos, memoria, y otros. Todo esto se documenta registrando todos los métodos empleados y actividades realizadas a lo largo del proceso de extracción. El analista se encontrará con tres escenarios: dispositivos encendidos, dispositivos apagados y dispositivos encendidos que no pueden ser apagados. Por eso, se debe adaptar el método de extracción acorde a la situación, el costo y el tiempo disponible. Las decisiones deben justificarse.

La documentación del proceso de extracción debe ser reproducible y verificable por terceros.

Cualquier analista calificado debe ser capaz de reproducir el proceso desde cero basándose en la documentación y llegar a los mismos resultados sin necesidad de interpretación u orientación alguna. En casos donde algún paso no sea

reproducible, el analista debe asegurar la correcta y detallada documentación del proceso de extracción, incluyendo controles de calidad.

Un ejemplo de estos casos es cuando se ha copiado un disco duro original y se ha vuelto a utilizar o dispositivos con memoria volátil. Es de suma importancia que el proceso de extracción sea reproducible y verificable para asegurar la admisibilidad de la evidencia digital.

Tanto las fuentes originales como las copias realizadas deben ser verificadas utilizando una función de verificación comprobada.

El proceso de extracción debe producir copias de la posible evidencia digital. Tanto las versiones originales como las copias deben pasar por una función de verificación (función hash) que sea reconocida como confiable (por ejemplo SHA-256 o SHA-512) en el momento y producir los mismos resultados posteriormente. Esto es necesario para asegurar la integridad de la evidencia digital.

En casos donde no se pueda realizar el proceso de verificación, el analista debe emplear el mejor método disponible e incluir en la documentación una justificación de su decisión.

De ser necesario, deben ser realizadas extracciones parciales.

Existen situaciones en las que no es posible realizar una extracción completa de la posible evidencia digital. Esto puede pasar por razones como el tamaño del conjunto de datos, sistemas críticos que no pueden ser apagados, limitaciones legales o cuando solo una parte de los datos en el sistema son relevantes. En estos casos, el analista deberá realizar una extracción lógica de solo ciertos tipos de datos, directorios o localizaciones a nivel de archivos y particiones. Se deberá documentar cuáles datos se extrajeron y por qué, además de justificar por qué se realizó una extracción parcial.

Crear copias maestras y copias de trabajo.

El analista debería crear copias de la posible evidencia digital: una copia maestra y al menos dos copias de trabajo. Todas las copias deberán ser verificadas por medio de una función hash confiable. La copia maestra no deberá ser utilizada a menos que sea necesario para verificar el contenido de las copias de trabajo o para producir otra copia de trabajo que reemplace una que haya sido dañada.

Los datos volátiles deben ser extraídos.

Si el dispositivo se encuentra encendido, una de las primeras actividades en el proceso de extracción debe ser generar copias de los datos volátiles como llaves de cifrado, configuraciones de zona horaria, contenido del portapapeles, puertos y conexiones de red abiertas, aplicaciones y procesos en ejecución, archivos temporales y de caché, unidades de red conectadas y otros datos cruciales que se alojan en la memoria RAM. Para realizar las copias se debe utilizar herramientas confiables y validadas previamente.

Utilizar un contenedor lógico para almacenar los datos volátiles.

Al extraer datos volátiles es recomendable utilizar un contenedor lógico y documentar su valor hash una vez extraídos los datos. De no contar con un contenedor, puede utilizarse un archivo ZIP que contenga todos los datos volátiles y documentar su valor hash.

En cuanto al contenedor o archivo ZIP, debe guardarse en un medio de almacenamiento digital dedicado solo a la evidencia digital. Es recomendable que el medio de almacenamiento digital sea nuevo pero uno que haya sido sanitizado es suficiente. Para esta tarea se pueden utilizar dispositivos como USB o discos de estado sólido (SSD).

Se debe aplicar la función hash a los dispositivos de almacenamiento originales y sus copias para garantizar su autenticidad.

Existen funciones de verificación por hash como SHA-256 y la familia de algoritmos SHA-512. Estas funciones son consideradas seguras debido a su mecanismo, el cual consiste en pasar un mensaje (puede ser cualquier tipo de archivo o documento digital) a través del algoritmo, el cual retorna una cadena de caracteres aleatorios conocida como firma hash.

Todas las firmas hash obtenidas deben registrarse en el documento de cadena de custodia. La posibilidad de que otro mensaje diferente al original pueda generar la misma secuencia de caracteres aleatorios es computacionalmente inviable. En otras palabras, si algo altera el mensaje, archivo o documento digital original este generará un hash distinto. Por lo cual, si este es el caso, significa que se rompió la cadena custodia quitando cualquier valor probatorio sobre la evidencia digital. El hash es la clave para garantizar que la evidencia digital no ha sido alterada.

Utilizar la firma digital sobre la posible evidencia digital extraída.

Opcionalmente, para garantizar la autenticidad del emisor, el no repudio y la integridad del contenido extraído, así como su marca de tiempo, se recomienda usar la firma digital en las copias forenses extraídas. Esto aplica también, por ejemplo, para la extracción de correos electrónicos donde el analista debe extraer el correo en su forma original. Esto debe hacerse preferiblemente frente a un notario pero, en los casos donde no cuenten con uno, la firma digital garantizará la autenticidad del experto en forense digital encargado de extraerlos.

El procedimiento consiste en extraer el correo electrónico, anotar cuáles fueron las normas y la metodología empleada en la extracción como parte de la cadena de custodia. Aparte de esto, hay que aplicar la firma digital para luego ponerla en una memoria USB con los originales de los correos electrónicos. Esto permitirá mantener la trazabilidad (Laguna, 2022).

Extraer información de los sistemas de videovigilancia.

El analista debe extraer todas las videograbaciones relevantes durante el tiempo de interés para preservar cualquier información adicional. Se debe determinar el tamaño de almacenamiento del sistema de CCTV y en qué momento el sistema está programado para sobrescribir los videos. Esta información le permitirá al analista saber cuánto tiempo se retendrá la secuencia de video en el sistema antes de que se pierda. Algunas opciones para la extracción de videos son:

- Extracción en un CD/DVD/disco Blu-ray. Puede resultar poco práctico si el archivo de video es demasiado grande.
- Extracción escribiéndolos en un medio de almacenamiento externo.
- Extracción a través de una conexión de red. Esto puede estar disponible si el sistema de CCTV está equipado con un puerto de red.
- Exportación de los videos en formato MPEG o AVI desde el sistema CCTV. Esto solo debe usarse como último recurso, ya que la recompresión altera los datos originales y siempre elimina los detalles de la imagen.

Utilizar herramientas confiables en el proceso de extracción.

El analista nunca debe confiar en los programas instalados en los dispositivos ya que estos pueden haber sido alterados. Por eso el analista debe utilizar sus propias herramientas previamente validadas y estar consciente de los efectos que estas pueden tener en el dispositivo. Por ejemplo, puede alterarse el contenido de la memoria al cargar la herramienta.

Deben documentarse todas las acciones que estas herramientas realizan y los cambios que producen en la evidencia digital. Si los cambios no pueden ser determinados con exactitud, esto también debe ser documentado.

Asociar al analista con la posible evidencia digital extraída.

Es recomendable relacionar la evidencia digital con la persona encargada de su extracción por medio de firma digital, sellado de tiempo, fotografías y biometría. Esto es necesario para dar un sentido de trazabilidad en la cadena de custodia.

Revisar que los dispositivos en apariencia apagados estén realmente apagados.

Algunos dispositivos pueden parecer apagados pero en realidad están en modo hibernación o conectados a fuentes de energía portátiles. El analista deberá asegurarse de que el dispositivo esté totalmente apagado y así evitar la pérdida de datos volátiles.

Utilizar buenas prácticas provenientes de algún documento de referencia reconocido para extracción en medios de almacenamiento.

Es recomendable que el analista se apoye en documentos de referencia y reconocidos que den más robustez al proceso de extracción como lo son el ISO 27037 y la norma NIST 800-86. Algunos ejemplos de buenas prácticas son:

- Se debe decidir entre recolectar el medio de almacenamiento o extraer la información en el lugar. Para ello el analista deberá basarse en la naturaleza del incidente y los recursos disponibles.
- Si se decide recolectar el medio de almacenamiento, este debe envolverse, etiquetarse y almacenarse en lugar apropiado.
- Etiquetar todos los medios de almacenamiento encontrados incluyendo sus partes asociadas. Las etiquetas no deben colocarse directamente en las partes mecánicas ni deben cubrir información importante como el número de serie, el número de modelo y el número de parte.
- La evidencia debe ser sellada a prueba de manipulaciones y el analista junto con el personal a cargo de la investigación forense deben firmar la etiqueta con fecha y hora.

- El analista deberá tomar en cuenta las políticas de retención de datos especificadas en la legislación para no sobrepasar el tiempo máximo de retención y generar prueba espuria.
- Tomar la imagen desde un dispositivo en modo solo lectura.
- Evite depender de una única herramienta (software / hardware).

5.2.4 Protección

La protección tiene como fin proteger y prevenir pérdidas, daños y alteraciones, así como permitir la auditabilidad sobre la evidencia digital y los dispositivos que la contienen. Por eso es importante que el experto responsable de la integridad de la evidencia conozca los procedimientos adecuados para manipular, empaquetar, transportar y almacenar la evidencia digital. Esto asegura la integridad según las características o naturaleza de los dispositivos electrónicos que la contienen.

Utilizar un estándar o documento de referencia reconocido para seguir las prácticas adecuadas sobre la manipulación segura de la evidencia digital.

Se debe utilizar algún documento de referencia reconocido tal como la norma ISO 27037, la NIST (800-86), en particular, la Guía para la Integración de Técnicas Forenses en Respuesta a Incidentes, el Manual de Evidencia Digital de la OEA, las normas SANS, la metodología TARA, la Metodología CFREDS o, para apegarse a la legislación nacional, se puede seguir como guía el Protocolo de Cadena de Custodia del OIJ. Así los investigadores se apegarán a los procedimientos adecuados para la protección de la evidencia digital y el mantenimiento de la cadena de custodia (Stine, 2008).

Durante el empaquetado se debe proteger cada dispositivo electrónico según sus características y naturaleza.

Durante el empaquetado y el transporte, el experto en forense digital responsable debe ser consciente de la posible presencia de descargas

electrostáticas, golpes, vibraciones, cambios de altitud, calor y exposición a radiofrecuencias que puedan dañar el valor probatorio de posibles pruebas digitales.

Por eso, se deberá empaquetar el dispositivo en un contenedor adecuado para evitar estas amenazas potenciales. Por ejemplo, si el dispositivo es un ordenador portátil este deberá transportarse con bolsas antiestáticas especiales, los dispositivos móviles requieren de bolsas de faraday o bolsas que protejan de radiofrecuencias.

Además, si se trata de un dispositivo móvil y se encuentra encendido, el experto debe asegurar que este se mantenga de esta forma. Se recomienda considerar transportarlo con una fuente de poder auxiliar dentro de la bolsa. Su estado debe monitorearse constantemente para evitar que su batería se descargue. Para casos donde no se cuente con recursos especializados, se recomienda al menos utilizar kits de evidencia que incluyan bolsas de sellado y embalado.

La evidencia digital debe contar con un documento de transporte.

La ISO 27037 recomienda adjuntar un documento de transporte que permita verificar la integridad del paquete durante su transporte. Estos documentos deben incluir hora y fechas de entrega y recibido, la firma de los responsables de la entrega y de la recepción, fotografías de la evidencia una vez empaquetada y previo al transporte. El formato recomendado por los autores se puede encontrar en el Anexo D de esta investigación (ISO, 2012).

Para procesos penales, según indica el Protocolo de Cadena de Custodia del OIJ, toda entrega y recibido debe consignarse en la boleta única de cadena de custodia (ver Anexo C) así como en los demás registros. Por ejemplo, en el libro de control de evidencia y bienes decomisados y los sistemas de registros utilizados por el Ministerio Público. Esto con el objetivo de respaldar la trazabilidad del indicio o evidencia. Ello significa: verificar que en los apartados establecidos se consigne toda la información requerida, tales como hora, fecha, persona que entrega el bien, persona que recibe la evidencia y todos los demás datos de individualización, para garantizar con ello la trazabilidad del indicio.

De acuerdo con el Ministerio Público, el personal a cargo del transporte está en la obligación de ejecutar las acciones necesarias para que el trato sea el idóneo para preservar la integridad de los indicios. Se recomienda que cualquier movimiento de la posible evidencia digital sea documentado.

Imagen tomada de Chacón, 2015.

Los encargados de la recepción de la evidencia digital deben contar con las calificaciones requeridas para garantizar su integridad y seguridad jurídica.

Para evitar un inadecuado manejo, así como su eventual rechazo de la evidencia digital en otras instancias, se deberá designar una persona encargada de la recepción, registro, custodia y disposición del indicio o evidencia. Además, se deberá contar con un espacio apropiado para la recepción de la evidencia, en un lugar de acceso restringido al público. En caso de procesos penales, la recepción de la evidencia digital se da por parte de la fiscalía del Ministerio Público quienes deberán seguir los lineamientos del Protocolo de Cadena de Custodia del OIJ.

La persona que entrega la evidencia digital debe ser la misma que se registra en el último eslabón de entrega.

La persona que entrega el indicio o evidencia digital debe ser la misma que se registra en el último eslabón de entrega. En otras palabras, ser la última persona en la boleta única de cadena de custodia o en la etiqueta adherida al empaque que contiene la evidencia de cadena de custodia. Es decir, la persona encargada de la evidencia deberá solicitar a quien hace entrega que consigne su firma y datos personales en el documento de control de evidencia correspondiente.

La bodega para custodia de evidencia debe cumplir con requerimientos.

Los requerimientos de la bodega son los siguientes:

- Seguridad en el ingreso. La bodega debe contar con un portón o puerta de seguridad que tenga acceso mediante combinación, llave o clave. Se recomienda un acceso biométrico y la utilización de cámaras de seguridad.
- Acceso restringido. El acceso a esta bodega se encontrará limitado a dos o máximo tres personas. Estas deberán registrar su ingreso en una bitácora. El ingreso de una segunda o tercera persona se justificará únicamente ante la necesidad de colaborarle a la persona encargada de la bodega cuando por el peso o la cantidad de evidencia esta no pueda ser trasladada por una sola persona.

Todo lo anterior, en concordancia con el Protocolo de Cadena de Custodia del OIJ.

El personal involucrado en la labor forense digital no deberá verse involucrado en fuga de información o en dar interpretaciones subjetivas que puedan tomarse como difusión de información falsa

La evidencia digital deberá manipularse con discreción y proteger su confidencialidad con el fin de evitar fugas de información que puedan alertar a las partes investigadas. Se debe evitar que alguna de las partes pueda intervenir y

tomar medidas para hacer más complicada la labor forense digital y del proceso judicial. Aparte de entorpecer el proceso, esto podría traer consigo incluso causas penales. Por ejemplo, los artículos 231 y 236 del Código Penal costarricense incluyen penas de cárcel por revelar información capaz de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios. Así mismo se refiere a cualquier información que tenga valor para el tráfico económico de la industria y el comercio.

5.2.5 Análisis

En esta fase, el analista debe estudiar y analizar los datos disponibles. Se busca llegar a una conclusión o determinar que aún no se puede sacar ninguna conclusión.

El análisis debe incluir la identificación de personas, lugares, artículos y eventos, determinando cómo se relacionan estos elementos para que se pueda llegar a una conclusión.

A menudo, este esfuerzo incluirá la correlación de datos entre múltiples fuentes. Por ejemplo, un registro del sistema de detección de intrusos en la red (IDS) puede vincular un evento a un host, los registros de auditoría del host pueden vincular el evento a una cuenta de usuario específica y el registro del IDS del host puede indicar qué acciones realizó ese usuario.

Herramientas como el registro centralizado y el software de gestión de eventos de seguridad pueden facilitar este proceso al recopilar y correlacionar automáticamente los datos. La comparación de las características del sistema con las líneas base conocidas puede identificar varios tipos de cambios realizados en el sistema.

Comprobar que los hashes de la copia de trabajo coinciden con los de la copia maestra.

Tal y como se mencionó en la fase de extracción, el analista debe contar con copias maestras y copias de trabajo. Antes de iniciar el análisis de la evidencia digital, el analista debe comprobar que los hashes de su copia de trabajo coinciden con los de la copia maestra. De esta forma, se corrobora que no han sido alteradas.

En caso de que no coincidan los hashes, esto se deberá documentar y la copia alterada deberá ser desechada y reemplazada por una copia de trabajo nueva creada a partir de la copia maestra.

El analista debe examinar las copias de trabajo, no las copias maestras.

Se debe trabajar con la copia de trabajo de los archivos sin afectar los archivos originales o la copia maestra. Esto es importante para preservar la integridad de la evidencia digital. En caso de que una copia de trabajo se dañe, una nueva copia de trabajo deberá ser creada a partir de la copia maestra. El acceso a la copia maestra debe ser respaldado por una autoridad competente y mantener un registro de quiénes acceden y cuándo a ella.

Se deben revisar los encabezados de los archivos para determinar su contenido.

El analista debe revisar los encabezados de los archivos y no las extensiones. Esto con el fin de determinar su tipo de contenido y tomando en cuenta que los usuarios pueden asignar cualquier extensión a los archivos. Los analistas no deben asumir que las extensiones de archivo son precisas.

Los analistas pueden identificar el tipo de datos almacenados en muchos archivos mirando sus encabezados de archivo. Aunque las personas pueden alterar los encabezados de los archivos para ocultar los tipos de archivos reales, esto es mucho menos común que alterar las extensiones de los archivos.

El analista debe tener un conjunto de herramientas forenses para el examen y análisis de datos.

El conjunto de herramientas debe contener varias herramientas que brinden la capacidad de realizar revisiones rápidas de datos, visualizaciones y análisis en profundidad (Laguna, 2022). El conjunto de herramientas debe permitir que sus aplicaciones se ejecuten de manera rápida y eficiente desde medios extraíbles (USB, CD, disco duro externo, etc) o una estación de trabajo forense. En el apartado de anexos se pueden encontrar un listado de recursos forenses.

El analista debe reconstruir el orden cronológico de los eventos.

El analista debe ser consciente del valor de utilizar las horas del sistema y las horas de los archivos. Debe saber cuándo ocurrió un incidente; cuándo se creó o modificó un archivo o se envió un correo electrónico. Saberlo es fundamental para el análisis forense.

Por ejemplo, la información se puede utilizar para reconstruir una línea de tiempo de actividades. Aunque esto puede parecer una tarea sencilla, a menudo se complica debido a las discrepancias intencionales o no intencionales en la configuración de tiempo entre los sistemas. Por eso, conocer la configuración de hora, fecha y zona horaria de una computadora cuyos datos se analizarán puede ser de gran ayuda para un analista.

No alterar los tiempos MAC durante el análisis.

El analista debe comprender cómo cada herramienta trabaja los tiempos de modificación, acceso y creación (MAC) de archivos. Por ejemplo, cuando un sistema de archivos es montado en un sistema operativo con permisos de escritura, algunas herramientas pueden modificar la última hora de acceso a un archivo o directorio. Debido a estos problemas, los analistas deben tener cuidado al elegir un método de visualización MAC y documentar los detalles de ese método. Se recomienda usar

bloqueadores de escritura para evitar que estas herramientas modifiquen los tiempos MAC.

El analista debe reunir datos de varias fuentes.

El analista debe revisar los resultados del proceso recolección y extracción de evidencia digital, como archivos, sistemas operativos, sistemas CCTV, correos electrónicos, dispositivos de almacenamiento, tráfico de red y otros. El fin de esto es determinar cómo estas diferentes fuentes de información se relacionan entre sí a la hora de reconstruir los eventos.

Incluir cualquier información que desprenda una acción como parte del documento único de cadena de custodia.

En algunos casos, los hallazgos en el análisis forense llevan consigo la necesidad de tomar acciones. Por ejemplo, de los datos hallados se puede desprender una lista de contactos que podrían conducir a información adicional sobre un incidente o crimen. Los casos donde se obtiene información que podría prevenir incidentes futuros, como una puerta trasera o *backdoor* en un sistema que podría continuar abierta y usarse para futuros ataques, un crimen que se está planeando, un gusano (*worm*) programado para comenzar a propagarse en un momento determinado, o una vulnerabilidad que podría ser explotada.

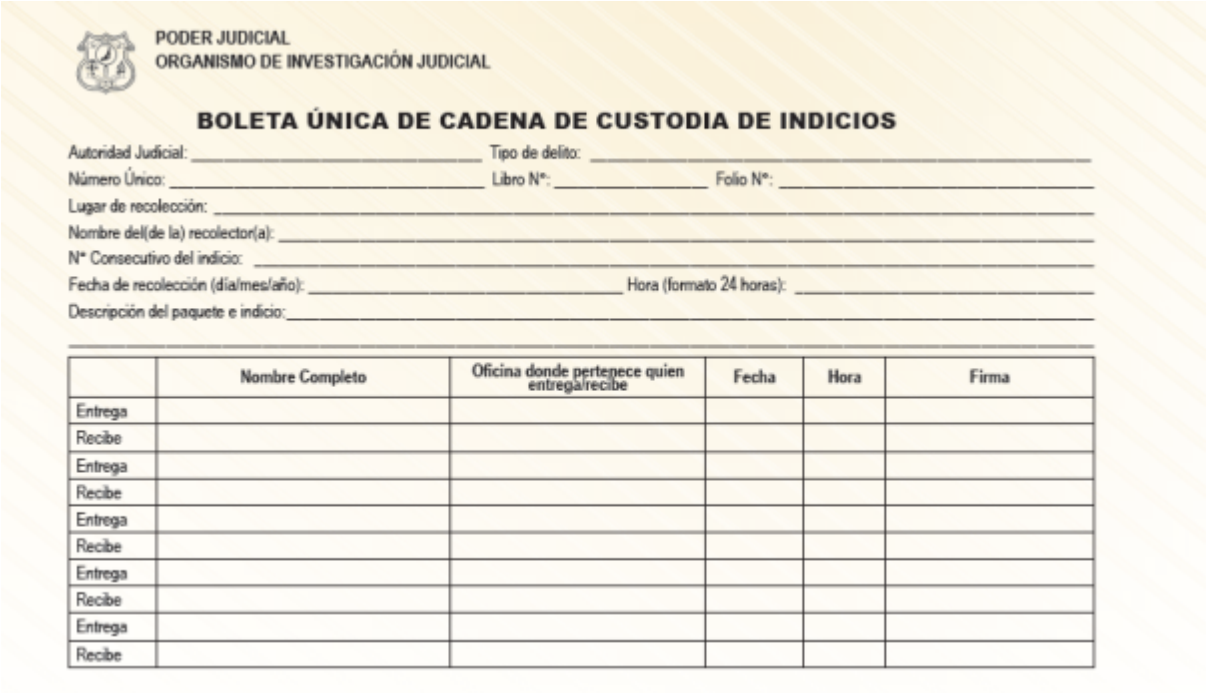
5.2.6 Informe

Consiste en preparar y presentar la información considerada relevante que fue extraída y analizada previamente. De acuerdo con la norma NIST 800-86 (Guía para la Integración de Técnicas Forenses en Respuesta a Incidentes) se deben incluir la descripción de cualquier acción realizada, explicar cómo las herramientas (software y hardware) fueron elegidas y además, determinar qué otras acciones necesitaron ser ejecutadas. Por ejemplo, si se necesitó examinar fuentes de datos

adicionales, asegurar vulnerabilidades encontradas en el camino o mejorar los controles de seguridad existentes.

Este reporte facilitará la toma de decisiones, para mejorar las políticas de seguridad, procedimientos, herramientas, entre otros.

Se debe confeccionar la Boleta Única de Cadena de Custodia



PODER JUDICIAL
ORGANISMO DE INVESTIGACIÓN JUDICIAL

BOLETA ÚNICA DE CADENA DE CUSTODIA DE INDICIOS

Autoridad Judicial: _____ Tipo de delito: _____
Número Único: _____ Libro N°: _____ Folio N°: _____
Lugar de recolección: _____
Nombre del(de la) recolector(a): _____
N° Consecutivo del indicio: _____
Fecha de recolección (día/mes/año): _____ Hora (formato 24 horas): _____
Descripción del paquete e indicio: _____

	Nombre Completo	Oficina donde pertenece quien entrega/recibe	Fecha	Hora	Firma
Entrega					
Recibe					
Entrega					
Recibe					
Entrega					
Recibe					
Entrega					
Recibe					
Entrega					
Recibe					

Imagen tomada del Protocolo de Cadena de Custodia del OIJ.

De acuerdo con el Protocolo de Cadena de Custodia del OIJ, esta boleta es una herramienta que permite identificar el indicio y se coloca posterior a su embalaje en el sitio. Una vez finalizado el embalaje del indicio respectivo en el lugar, se debe confeccionar de una vez la boleta única de cadena de custodia con toda la información del caso, a saber:

- autoridad judicial
- tipo de delito
- número único

- número de libro y de folio, número consecutivo de indicio (el cual se obtiene al registrar la información de los indicios recolectados, una vez que se llegue a la oficina, mediante registros establecidos detallados en la fase 4, Protección)
- lugar de recolección
- nombre de la persona recolectora
- fecha y hora de la recolección
- la descripción en el espacio correspondiente del paquete de indicio, haciendo referencia al tipo de soporte y lo que contiene (por ejemplo, una caja de cartón debidamente embalada, que contiene documentación varia)
- respecto a la del transporte (entrega y recibido) se hará constar a puño y letra cuando se configure la inmediatez y la unidad del acto, con quien lo vaya a recibir.

En el Anexo C se puede encontrar un ejemplo de cómo confeccionar una boleta única de cadena de custodia.

Se debe adjuntar la boleta de control de indicios a la boleta única de cadena de custodia.

La boleta de control de indicios, así como el uso de los sellos, lacrados y etiquetados deben ser parte de los adjuntos obligatorios. Estos son incluidos en el informe desde la fase de recolección. Son medidas para proteger el indicio o la evidencia y así garantizar su identidad. En el Anexo E se puede encontrar un ejemplo de boleta de control de indicios.

A continuación se adjunta el formato de identificación de indicios de carácter obligatorio empleado por el OIJ.

¡CUIDADO!
INDICIO POLICIAL
OIJ
Pla.Rev. (06-16) Depto. de Artes Gráficas. OT. 45154, F. 734

Artículo:	INDICIO ORGANISMO DE INVESTIGACIÓN JUDICIAL
N° único:	
Persona ofendida:	
Persona imputada:	
Donde se recolectó:	
Fecha y hora:	
Recolectado por:	

Pla.Rev. (06-16) Depto. de Artes Gráficas, OT. 45154, F. 735

OIJ

CONTROL DE INDICIO

N° único: _____

Persona ofendida: _____

Persona imputada: _____

Recolectado por: _____

Fecha: _____ Hora: _____

Dirección: _____

Descripción del indicio: _____

_____

_____

Donde se localizó?: _____

Pla.Rev. (06-16) Depto. de Artes Gráficas, OT. 51041, F. 736

Imagen tomada del Protocolo de Cadena de Custodia del OIJ

Se debe adjuntar a la boleta única de cadena de custodia todos los documentos relevantes para garantizar su trazabilidad.

El analista deberá adjuntar a la boleta única de cadena de custodia, todos los documentos relevantes. Por ejemplo, debe incluir el documento de transporte y el control de indicios. Para procesos penales, el OIJ en su protocolo de cadena de custodia recomienda adjuntos los siguientes documentos:

- actas de inspección ocular y recolección de indicios
- actas de secuestro
- actas de recibido
- actas de hallazgo
- control de indicios.

El documento de cadena de custodia debe incluir un dictamen pericial sobre la evidencia digital obtenida del análisis.

Este documento será leído por los jueces, fiscales, abogados y partes interesadas en la resolución de un proceso judicial. Deberá ser escrito haciendo énfasis en las conclusiones. Puede incluir una representación visual simplificada de cómo ocurrió el ataque, con el orden cronológico de los eventos.

En otras palabras, no les interesa conocer los valores hash ni si se utilizó herramientas de código libre. Se busca que en pocas páginas se aporte la información concreta, relevante y suficiente en cuanto sea determinante y facilite la toma de decisiones.

Solo en algunos casos se puede dar referencias a elementos técnicos si son de relevancia para que el juez tenga un panorama más amplio. En la mayoría de los casos, se recomienda que si son elementos técnicos que el juez podría no estar capacitado para entender, agregarse como parte de los anexos en un reporte técnico. Así, el juez tiene un documento más ligero pero que si quisiera podría revisar los anexos para entender cómo se llegó a las conclusiones que se plantean.

También puede ser acompañado por un glosario de términos para que todas esas palabras que un profesional en sistemas de información da por hecho, el juez pueda comprender gracias a su respectiva explicación (Laguna, 2022).

Una plantilla para construir el dictamen pericial se adjunta en el Anexo F de esta investigación.

El adjunto sobre el dictamen pericial también aporta la siguiente información:

- Datos del analista forense digital. Se recomienda adjuntar el documento con la protesta de cargo donde se da constancia de que el perito cuenta con la experiencia y perfil para ejercer el cargo. Una plantilla de esto se puede encontrar en los anexos.
- Cuerpo del dictamen.
- Cuestionario. Este último será realizado por el perito informático de manera que se muestre la información en cuanto sea determinante, según el objetivo.

<u>El documento de cadena de custodia debe incluir un reporte técnico sobre la evidencia digital obtenida del análisis.</u>

Es necesario adjuntar un reporte técnico para que acompañe al dictamen pericial. Hacerlo le permitirá a las partes involucradas, así como a los administradores de sistemas o peritos en cómputo forense, revisar, por ejemplo, la coincidencia de las firmas hash, el inventario de software o hardware utilizado, en el tráfico de la red, las estadísticas relacionadas con gran detalle. Este informe facilitará la toma de decisiones e incluso permitirá aplicar nuevos controles o implementar nuevas políticas de seguridad para prevenir incidentes similares.

Entre los anexos que de manera general pueden ser relevantes para incluir al documento único de cadena de custodia están los siguientes:

- Listado del equipo (hardware) para investigación requerido para llevar al lugar del incidente.
- Listado del inventario del software utilizado.
- Línea de tiempo de cada proceso observado.
- Descripción del área bajo investigación, tipo de escenario, nombre de la organización, dirección y mapa de la ubicación (si está disponible).

- Detalles sobre la autorización legal de la investigación.
- Detalles de las órdenes de allanamiento y cualquier otra autoridad que sea aplicable a la investigación, incluyendo los límites del allanamiento y la incautación.
- Aspectos e implicaciones legales.
- Información logística o planificación del cómputo forense.
- Anotar cualquier potencial conflicto de intereses.
- Documentos del transporte (entrega y recepción).
- Dictamen pericial donde se justifica cómo se llegaron a las conclusiones.
- Cualquier documentación de apoyo de los vendedores de cada tecnología si se precisa demostrar que existió un comportamiento anómalo de un sistema.

También es importante que el analista incluya una declaración jurada en el informe pericial, donde certifique sus atestados técnicos y se comprometa a cumplir con una serie de requisitos mínimos. En el Anexo G se puede encontrar un ejemplo sobre cómo elaborar una declaración jurada.

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

Existe una amplia cantidad de estándares internacionales, marcos de trabajo y modelos relacionados al cómputo forense. En esta investigación se analizaron más de 20 documentos. Entre los documentos principales están las normas ISO 27037 y la Guía para la Integración de Técnicas Forenses en Respuesta a Incidentes de la NIST 800-86.

Se analizó también lineamientos recomendados por legislaciones internacionales en países como Sudáfrica y México. Ellas ofrecen una perspectiva más amplia sobre los requerimientos legales del cómputo forense en delitos informáticos.

En cuanto a los requerimientos legales dentro del marco jurídico de Costa Rica, el Código Penal es el documento de referencia sobre el tema de los delitos informáticos. Si bien durante su creación no se contemplaron los delitos informáticos (en el año 2001), con la promulgación de la ley 8148 se empezaron a establecer disposiciones legales para combatir la ciberdelincuencia mediante la adición de los artículos 196 BIS (Violación de comunicaciones electrónicas), 217 BIS (Fraude informático) y 229 BIS (Alteración de datos y sabotaje informático).

Posteriormente, en el año 2012 debido al avance de la tecnología y al incremento en la complejidad y cantidad de los delitos informáticos los legisladores costarricenses modificaron de nuevo el Código Penal mediante la ley 9048 reformando los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288. Esta nueva ley menciona conceptos como el espionaje informático, la suplantación de identidad y los programas informáticos maliciosos. También introdujo nuevas penas, siendo estas especialmente fuertes cuando el infractor tiene conocimientos informáticos.

Por lo tanto, el Código Penal y los artículos mencionados anteriormente son las herramientas legales dentro del marco jurídico costarricense relacionadas a los delitos informáticos. Sin embargo, ya ha pasado más de una década desde el último esfuerzo legislativo en esta materia y el país necesita una legislación moderna sobre delitos informáticos que sea equilibrada técnica y jurídicamente. Se necesita una

legislación que proteja a los usuarios y a su información de la ciberdelincuencia. Cabe resaltar también que no hay mención alguna en la legislación actual sobre cuál debe ser el manejo de la evidencia digital ni sobre cómo debe realizarse la investigación pericial.

Tanto la investigación de los delitos informáticos como el manejo de la evidencia digital en Costa Rica recae principalmente en el OIJ. Es este ente el encargado de realizar las investigaciones en los procesos penales y para ello cuenta con una unidad especializada de delitos informáticos. Parte de los procedimientos que sigue el OIJ al investigar los delitos informáticos están definidos en su Protocolo de Cadena de Custodia y en su Guía de Recolección de Indicios.

La labor del OIJ está centralizada en la Gran Área Metropolitana y existe un faltante de estadísticas que contabilicen los delitos informáticos. Estas estadísticas ayudarían a dar perspectiva de la problemática y facilitar la toma de decisiones para la mejora continua.

Además, hay poca inversión por parte del Estado en equipo o en compensación salarial. Esto provoca sobrecarga de trabajo y fuga de talento. En cuanto al sector privado, existen empresas y trabajadores independientes que ofrecen servicios de cómputo forense con profesionales mejor preparados pero estas son pocas y operan en un mercado nacional incipiente.

En general, los profesionales en cómputo forense en Costa Rica siguen los procedimientos definidos en estándares internacionales reconocidos como las normas ISO 27037, NIST 800-86, SANS, la metodología TARA, la metodología CFREDS o hasta metodologías propias.

En cuanto a los puntos de mejora, en la investigación de delitos informáticos existen tres áreas: profesional, cultural y regulatoria. El ámbito profesional incluye todas las mejoras relacionadas a la definición de un perfil técnico profesional que pueda ejercer el cómputo forense en Costa Rica apropiadamente así como la necesidad de desarrollar especialidades en cómputo forense en las universidades o incluir el tema como una materia optativa en los planes de estudio tanto en ingeniería como en derecho.

En el aspecto cultural se denota la necesidad de cambios en la ciudadanía así como colaboración del sector público y privado. En este sentido, la ciudadanía debe

denunciar más los delitos informáticos. También, el OIJ debería descentralizar la investigación de delitos informáticos y distribuir la carga para evitar la saturación debido a la gran cantidad de casos. Las compañías aseguradoras podrían dar un aporte importante al incrementar la demanda de peritos en cómputo forense, incorporando en el país los ciberseguros.

En el aspecto regulatorio se debe modificar el Código Penal para definir una mejor tipificación de los delitos informáticos y promulgar leyes que permitan a las víctimas de un delito informático disponer de los servicios de peritos en cómputo forense.

En base a todo lo anteriormente expuesto, se desarrolló un estándar compuesto de 6 fases para determinar la admisibilidad y la trazabilidad de la evidencia digital. Se definieron las reglas mínimas con criterios técnicos y legales para evaluar la admisibilidad de la evidencia digital y en cada una de las fases desarrolladas se aborda el tema de la trazabilidad mediante la preservación de la cadena de custodia, desde la jurisprudencia y el Código Penal costarricense pero también desde la investigación realizada.

Producto de esto, el estándar desarrollado facilita a las personas no técnicas el identificar los criterios que los jueces o partes responsables de la toma de decisiones puedan considerar antes de emitir un veredicto. El estándar también sirve como guía para que los peritos en cómputo forense del país den un manejo adecuado a la evidencia digital y conozcan los criterios de evaluación técnicos y legales que se toman en cuenta para admitir la evidencia digital en procesos penales.

Sumado a ello, se facilita a los peritos el transmitir de manera asertiva las conclusiones del dictamen pericial y los procedimientos seguidos para llegar a este. A pesar de ser un estándar enfocado en procesos penales, a su vez es extrapolable para que se utilice en otro tipo de investigaciones. Por ejemplo, en los procesos de carácter administrativo que puedan ocurrir en ambientes laborales.

En cuanto a las buenas prácticas a seguir durante una investigación de delitos informáticos estas pueden derivarse de los estándares internacionales y marcos de trabajo. En ellas se describe en varias fases como llevar a cabo el cómputo forense manteniendo la integridad de la evidencia por medio de la

documentación de cada acción realizada durante la investigación. Se definieron una serie de estas buenas prácticas y en qué caso utilizarlas en la sección 4.4 de esta investigación.

Finalmente, basados en la base de conocimientos de la investigación y en las entrevistas realizadas a expertos en cómputo forense de Costa Rica, se concluyó que existe la necesidad de crear una guía bajo el contexto del marco legal costarricense que defina las consideraciones previas y los pasos a seguir para abordar una investigación de delitos informáticos. Se necesita un documento que le sirva a entidades públicas y privadas como una lista de chequeo sobre qué procedimientos de cómputo forense seguir.

Producto de ello, se observó que en las cortes la evaluación de la evidencia digital depende mucho de la habilidad de convencimiento y comunicación del abogado apoyándose en el dictamen pericial. Por eso, resulta de gran importancia la capacidad de “traducir” el lenguaje técnico en términos más comprensibles para un público no técnico. Es con el objetivo de subsanar estas necesidades que se realizó la propuesta de un estándar nacional que facilite determinar la admisibilidad de la evidencia digital en delitos informáticos.

6.2 Recomendaciones

Se presentan a continuación, algunas recomendaciones de la experiencia obtenida al realizar el trabajo, tanto desde el punto de vista investigativo, como a nivel de la administración de recursos:

- Se recomienda para futuros trabajos sobre delitos informáticos consultar la jurisprudencia nacional mediante la página web “Nexus” del Poder Judicial. Este es un recurso valioso para poder comprender cómo los jueces de la república abordan el tema de los delitos informáticos. Complementariamente, para facilitar el entendimiento de los criterios legales que utilizan los jueces al determinar el valor probatorio de la evidencia digital, revisar el documento publicado en Revista Judicial, Costa Rica, Nº 102, Diciembre 2011 titulado “La prueba ilícita o espúrea en materia penal”.

- El presente trabajo fue realizado por dos masterandos, lo cual conlleva la necesidad de utilizar herramientas colaborativas. Se recomienda utilizar herramientas gratuitas como Google Drive ya que facilita el control de versiones y permite crear diferentes recursos como hojas de cálculo, presentaciones visuales y documentos escritos. Además sirve como repositorio de videos para las entrevistas realizadas. Se recomienda también utilizar plataformas de comunicación gratuitas como Microsoft Teams para la realización de las entrevistas o sesiones colaborativas sin un límite de tiempo.
- Similar a la dinámica incluida en este trabajo, se recomienda que para la realización de trabajos relacionados al cómputo forense también se realicen entrevistas con expertos costarricenses en el área. Sin embargo, se recomienda incluir también abogados, fiscales y personas con conocimientos en derecho costarricense.
- Basados en las áreas de mejora descritas por los entrevistados, se recomienda a las universidades públicas y privadas, pero especialmente a la Universidad Cenfotec, desarrollar especialidades en cómputo forense y no solo crear materias optativas en los planes de estudio. Además, agregaría mucho valor al título obtenido la capacidad de poder graduarse teniendo ya una certificación internacional.
- En el sector público, el perfil del especialista en cómputo forense no está bien definido por el Servicio Civil. En su lugar, se contrata simplemente a personas con conocimientos generales de informática y no a aquellos especializados en ciberseguridad y cómputo forense. Como consecuencia, surgen casos de selección de personal no calificado para el puesto. Se recomienda al Estado definir el perfil de especialista en cómputo forense para evitar estos problemas.

Glosario

ACCCF: El *American Council For Cybersecurity And Computer Forensic* (ACCCF) es una organización formada para proporcionar educación y colaboración sobre la prevención e investigación de crímenes informáticos

Base de datos: Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios. (Acurio Del Pino, 2004)

CAMTIC: La Cámara de Tecnología de Información y Comunicación (CAMTIC) nació en 1998 y actualmente está integrada por cerca de 200 empresas. Juntas, conforman un bloque estratégico que busca fortalecer y apoyar al sector de las tecnologías digitales en Costa Rica

CFREDS: *Computer Forensic Reference Data Sets* es un proyecto de la NIST donde se proporciona a los investigadores conjuntos documentados de evidencia digital simulada para su examen.

CSIRT: Los equipos de respuesta a incidentes de seguridad (del inglés *Computer Security Incident Response Team*) buscan restituir las actividades normales con el impacto mínimo aceptable para las organizaciones ante un incidente.

CSIRT-CR: Centro de Respuesta de incidentes de Seguridad Informática de Costa Rica.

Firma Digital: El equivalente digital de una firma auténtica escrita a mano. Es un dato añadido a un fichero electrónico, diciendo que el dueño de esa firma suscribió o autorizó el archivo. (Acurio Del Pino, 2004)

GAM: La Gran Área Metropolitana (abreviado GAM) es la principal aglomeración urbana de Costa Rica, que incluye las conurbaciones de las cuatro ciudades más grandes de ese país (San José, Alajuela, Cartago y Heredia) todas localizadas en la Meseta Central

ICE: Instituto Costarricense de Electricidad

IOCs: Un indicador de compromiso o IOC, del inglés *Indicator of Compromise*, es toda aquella información relevante que describe cualquier incidente de ciberseguridad, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento.

ISO: Organización Internacional de Estandarización, es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de normalización.

KPIs: Los indicadores clave de rendimiento (del inglés *Key Performance Indicators*) se refieren a un conjunto de medidas cuantificables utilizadas para medir el rendimiento general a largo plazo de una empresa.

MICITT: El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica (MICITT) es el ministerio del gobierno de Costa Rica encargado de dictar la política pública de ciencia, tecnología y telecomunicaciones del país.

MTTS: Ministerio de Trabajo y Seguridad Social de Costa Rica.

Modem: Un aparato que cambia datos del computador a formatos que se puedan transmitir más fácilmente por línea telefónica o por otro tipo de medio. (Acurio Del Pino, 2004)

NIST: El Instituto Nacional de Estándares y Tecnología (del inglés *National Institute of Standards and Technology*), es una agencia de la Administración de Tecnología

del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica.

OIJ: El Organismo de Investigación Judicial es una dependencia de la Corte Suprema de Justicia de Costa Rica creada en 1973 como un órgano auxiliar de los tribunales penales del Ministerio Público en el descubrimiento y verificación científica de los delitos y sus presuntos responsables.

SANS: El Instituto SANS (del inglés *SysAdmin Audit, Networking and Security Institute*) es una institución con ánimo de lucro fundada en 1989, con sede en Bethesda (Maryland, Estados Unidos) que agrupa a 165.000 profesionales de la seguridad informática (consultores, administradores de sistemas, universitarios, agencias gubernamentales, etcétera).

TARA: Evaluación de amenazas y análisis de remediación (del inglés *Threat Assessment and Remediation Analysis*) es una metodología de ingeniería utilizada para identificar y evaluar vulnerabilidades cibernéticas y seleccionar contramedidas efectivas para mitigar esas vulnerabilidades.

Bibliografía

Acurio Del Pino, S. (2004). *Manual de Manejo de Evidencias Digitales y Entornos Informáticos*. Versión 2.0. Recuperado en Enero 25, 2022, de: https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Ahmad, T. (2020). *CoronaVirus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity*. SSRN Electronic Journal. doi:10.2139/ssrn.3568830

Ali, K. M. (2012). *Digital Forensics Best Practices and Managerial Implications. 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks*. doi:10.1109/cicsyn.2012.44

Antwi-Boasiako, A. (2018). *A model for digital evidence admissibility assessment. In 13th IFIP International Conference on Digital Forensics* (pp. 23-38). Orlando, FL.

Arburola, A. (2021). *La prueba ilícita o espúrea en materia penal*. Revista Judicial, Costa Rica, Nº 102. Recuperado en Enero 23, 2022, de https://escuelajudicialpj.poder-judicial.go.cr/Archivos/documentos/revs_juds/revista102/pdf/011_pruebaili.pdf

Arrieta, E. (2021). *Todo lo que debe saber de la UPAD y la comparecencia de Carlos Alvarado*. La República. Recuperado en Diciembre 10, 2021, de https://www.larepublica.net/noticia/todo-lo-que-debe-saber-de-la-upad-antes-de-que-carlos-alvarado-comparezca-hoy-ante-los-diputados

Bertolín, J. A. (2008). *Seguridad de la información: Redes, informática y sistemas de información*. Madrid: Paraninfo Cengage Learning.

Blanco, C., Lasheras, J., Valencia-García, R., Fernández-Medina, E., Toval, A., & Piattini, M. (2007). Ontologías de seguridad: revisión sistemática y comparativa. Recuperado en Enero 11 del 2021 de :

https://www.researchgate.net/publication/229083904_Ontologias_de_seguridad_revision_sistematica_y_comparativa

Brauer, J., Plosch, R., Saft, M., & Korner, C. (2017). *A Survey on the Importance of Object-Oriented Design Best Practices. 2017 43rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. doi:10.1109/seaa.2017.14

Castilla Guerra, J. E. (2013). *Importancia de la recolección de datos volátiles dentro de una investigación forense* [Tesis de postgrado, Universidad Piloto de Colombia]. Repositorio institucional de la Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/3088

Castro, J. (27 de Julio de 2018). *Costa Rica crea Alta Comisión de Seguridad Informática*. Recuperado en Enero 23 del 2022 de https://www.larepublica.net/noticia/costa-rica-crea-alta-comision-de-seguridad-informatica

Cavacini, A. (2014). *What is the best database for computer science journal articles?* Scientometrics, 102(3), 2059-2071. doi:10.1007/s11192-014-1506-1.

Chacón, K. (2015). *Detienen a universitario buscado por el FBI por delitos informáticos*. Recuperado el 8 de Diciembre del 2019 de https://www.nacion.com/sucesos/judiciales/detienen-a-universitario-buscado-por-el-fbi-por-delitos-informaticos/LWMPCOXTJZG5XD2NJHCX7EPOZ4/story/

Chinchilla, S. (17 de abril de 2020). *Abogados de Carlos Alvarado: Fiscalía extrajo datos sobre seguridad nacional de Casa Presidencial*. La Nación, Costa Rica. Recuperado en Julio 6, 2020, de https://www.nacion.com/el-pais/politica/abogados-de-carlos-alvarado-fiscalia-extrajo/SVRTXA6SA5BSJOTDOADMUSIQ7M/story/

Código Procesal Civil (Ley Nº 9342, 2016). Costa Rica. Recuperado el 11 de agosto del 2020 de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=81360

Daniel B. Garrie and J. David Morrissy, *Digital Forensic Evidence in the Courtroom: Understanding Content and Quality*, 12 Nw. J. Tech. & Intell. Prop. 121 (2014).https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss2/5

Nelson, José. (2020). *About Computing Science Research Methodology*

Fernández Nogales, A. (2014). *Investigación y técnicas de mercado*. España: ESIC Editorial.

Hevner, A., & Chatterjee, S. (2010). *Design Science Research in Information Systems. Integrated Series in Information Systems Design Research in Information Systems*, 9-22. doi:10.1007/978-1-4419-5653-8_2

Karie, Nickson, Victor Kebande, and Hein Venter. *A Generic Framework for Digital Evidence Traceability*. European Conference on Cyber Warfare and Security. Academic Conferences International Limited, 2016.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response*. doi:10.6028/nist.sp.800-86

Laguna, J. (2022). *Fundamentos de la informática forense*. México. Recuperado en Enero 21, 2022, de: https://durivau.lpages.co/fif/?fbclid=IwAR1GtvRoEtbDIe87dFKhnQqY99hTLsMjxvBQgDmw41CVJ-X5gXsEY78V_Ps

Lemaitre, R. (2010). *La impunidad de los delitos informáticos en la Ciber-Sociedad costarricense en el ámbito del Derecho Penal* (Universidad de Costa Rica, 2010) (pp. 210-211). San José: Facultad de Derecho.

Leroux, O. (2004). *Legal admissibility of electronic evidence*. International Review of Law, Computers & Technology, 18(2), 193-220. doi:10.1080/1360086042000223508

Loarte, Byron. (2019). *Marco de trabajo estandarizado para el análisis forense de la evidencia digital en el Ecuador*.

Lopez, J., & Torres, M. (2010). *Problemática del Delito Informático: Hacia una necesaria regulación internacional (Tesis de maestría inédita).* Universidad de Costa Rica.

M. C. Chavarría-González, *La dicotomía cuantitativo/cualitativo: falsos dilemas en investigación social.* Actualidades en psicología, vol. 25, no. 112, pp. 1-35, 2011

Muñoz, F. (17 de abril de 2021). *Abogados de Carlos Alvarado acusan a Fiscalía de secuestrar más información de la autorizada en caso UPAD.* Monumental. Recuperado en Enero 23 del 2022 de https://www.monumental.co.cr/2020/04/17/abogados-de-carlos-alvarado-acusan-a-fiscalia-de-secuestrar-mas-informacion-de-la-autorizada-en-caso-upad/

Nieto-Morales, C. (2016). *Análisis y valoración de la prueba pericial: Social, educativa, psicológica y médica*: El perito judicial (p. 15). Madrid: Dykinson.

Ministerio Público, Organismo de Investigación Judicial (2020). *Protocolo de cadena de custodia*. Recuperado en Enero 23, 2022, de https://ministeriopublico.poder-judicial.go.cr/images/phocadownload/CircularesAdministrativas/2020/Anexos2020/protocoloCadenaCustodia.pdf

Organización Internacional de Normalización. (2012). *Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO 27037)*. https://www.iso.org/standard/44381.html

P. M. Dimpe and O. P. Kogeda, *Generic Digital Forensic Requirements, 2018 Open Innovations Conference* (OI), 2018, pp. 240-245, doi: 10.1109/OI.2018.8535924.

Pabilonia, S. W., & Vernon, V. (2020). *Telework and Time Use in the United States*. SSRN Electronic Journal, 1-1. doi:10.2139/ssrn.3601959

Parlamento de República de Sudáfrica. Gaceta 23809 (30 de Agosto de 2002). *Electronic Communications and transactions act. Cape Town, Western Cape: Government Gazette.* Recuperado en Febrero 1 del 2022 de https://www.gov.za/documents/electronic-communications-and-transactions-act

Prayudi, Y., & Sn, A. (2015). *Digital Chain of Custody: State of The Art. International Journal of Computer Applications*, 114(5), 1-9. doi:10.5120/19971-1856

Rasjid, Z. E., Soewito, B., Witjaksono, G., & Abdurahman, E. (2019). *Framework for establishing confidence level of digital evidence admissibility.* ICIC Express Letters, 13(8), 663-672. doi:10.24507/icicel.13.08.663

Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos (Ley Nº 8148, 2001). Costa Rica. Recuperado el 11 de agosto de 2021 de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=47430&nValor3=50318&strTipM=TC

Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal (Ley Nº 9048, 2012). Costa Rica. Recuperado el 11 de agosto de 2021 de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=73583

Reith, Mark & Carr, Clint & Gunsch, Gregg. (2003). *An Examination of Digital Forensic Models*.

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

Stine, K. (2008). *Guide for Mapping Types of Information and Information Systems to Security Categories*. NIST STANDARD. doi:https://doi.org/10.6028/NIST.SP.800-60v1r1

Stoykova, R., & Franke, K. (2020). *Standard Representation for Digital Forensic Processing. 2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*. doi:10.1109/sadfe51007.2020.00014

Williams QPM, J., DAC. (n.d.). *ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence*. Recuperado en Enero 23 del 2022 de https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Xu, C., Fan, W., Wang, C., & Xin, Z. (2014). *Risk and intellectual property in technical standard competition: A game theory perspective*. China Communications, 11(5), 136-143. doi:10.1109/cc.2014.6880469

Anexos

Anexo A: Ejecución de la revisión de literatura

Ejecución de la revisión

A continuación se muestra el proceso llevado a cabo para las diferentes fuentes.

Ejecución de la selección en la fuente IEEE

Se aplican cada una de las cadenas de búsqueda especificadas en la sección 1.9.1.2.3 de esta investigación, por ejemplo la cadena:

- "digital forensics" AND ("standard" OR “methodology”)

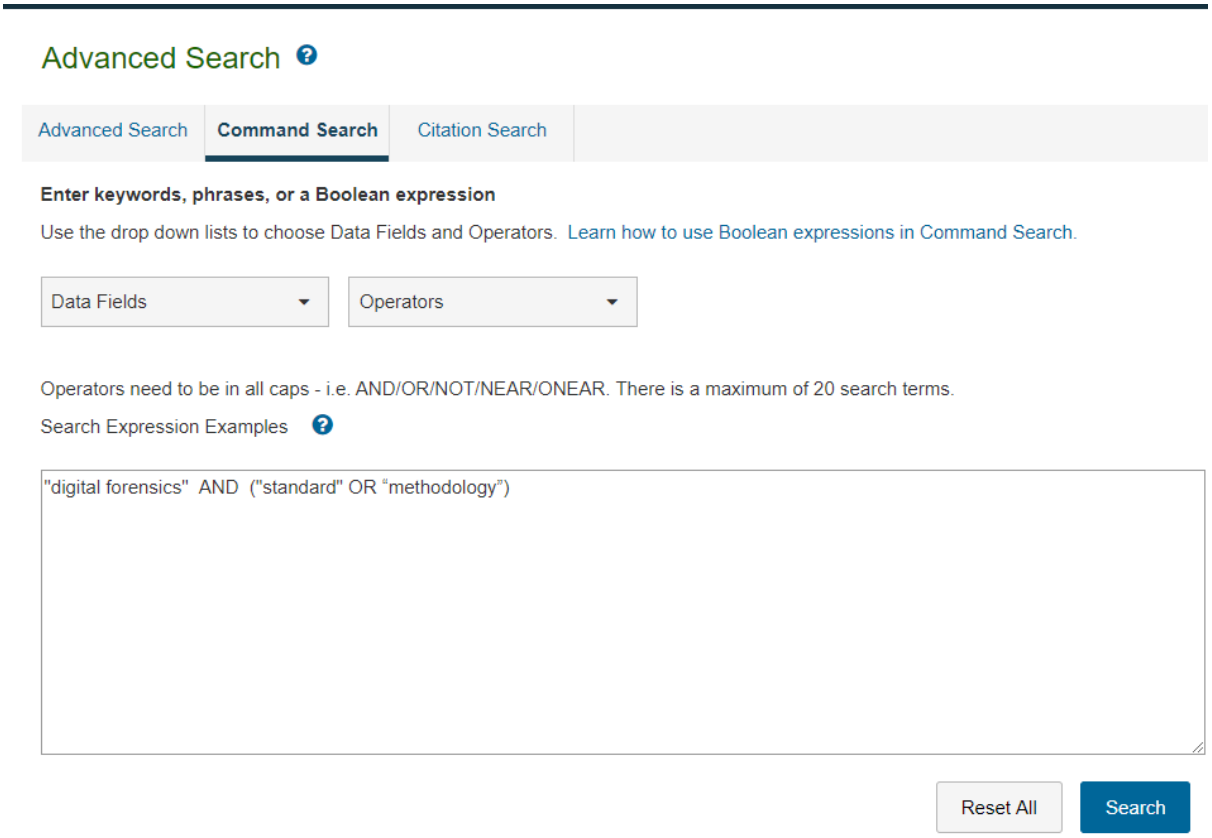


Figura a: Ejecución de la selección, fuente IEE.

Si se obtienen más de 50 resultados, se aplican filtros adicionales como rangos de fechas, por ejemplo estudios publicados en los últimos dos años:

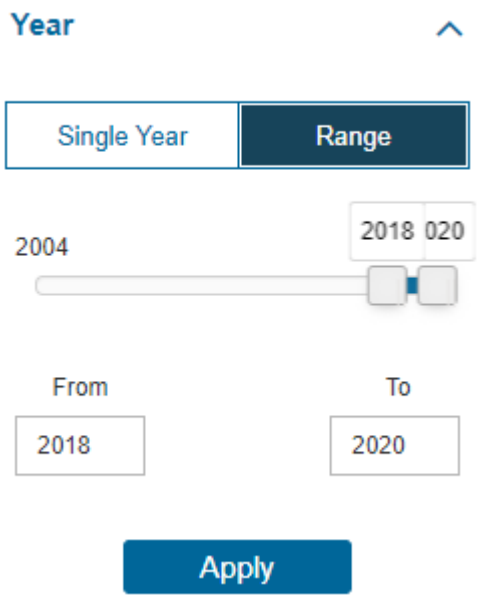


Figura b: Ejecución de la selección con filtros adicionales, fuente IEE.

Al aplicar todas las cadenas de búsqueda y refinar los resultados, se procedió a utilizar los criterios de exclusión para obtener una lista final de estudios seleccionados, dicho proceso puede ser consultado en el apéndice de este documento.

Título del documento	Autores	Año	PDF Link	SJR
A proposed digital forensic investigation framework for an eGovernment structure for Uganda	Ivans Kigwana; Victor R. Kebande; H.S Venter	2017	https://ieeexplore.ieee.org/document/8102348	0.144

Generic Digital Forensic Requirements	Precilla M. Dimpe ; Okuthe P. Kogeda	2018	https://ieeexplore.ieee.org/document/8535924	-
A Sample of digital forensic quality assurance in the South African criminal justice system	Jason Jordaan	2012	https://ieeexplore.ieee.org/document/6320431	0.245
A Systematic Literature Review On Digital Evidence Admissibility: Methodologies, Challenges and Research Directions	Elizabeth Ozioma Edward ; Joseph A. Ojeniyi	2019	https://ieeexplore.ieee.org/document/9043250	0.124
Standard Representation for Digital Forensic Processing	Radina Stoykova ; Katrin Franke	2020	https://ieeexplore.ieee.org/document/9133704	0.127
A Case Based Reasoning Framework for Improving the Trustworthiness of Digital Forensic Investigations	Graeme Horsman ; Christopher Laing ; Paul Vickers	2012	https://ieeexplore.ieee.org/document/6296036	0.3

Guidelines for Recognize, Collect, Extract, Protect, and Report Digital Evidence	Rodrigo Arturo Proaño Escalante ; Andrés Fernando Gavilanes Molina	2017	https://ieeexplore.ieee.org/document/8328105	-
National digital forensics framework for Bangladesh	Mohammad Mahfuzul Haque; Syed Akther Hossain	2017	https://ieeexplore.ieee.org/document/8275133	0.149

Tabla a.Estudios encontrados en IEEE.

Ejecución de la selección en la fuente Scopus

Se aplican cada una de las cadenas de búsqueda especificadas en la sección 1.9.1.2.3 de esta investigación, por ejemplo la cadena:

- (“digital forensics” OR “digital evidence”) AND “guidelines”

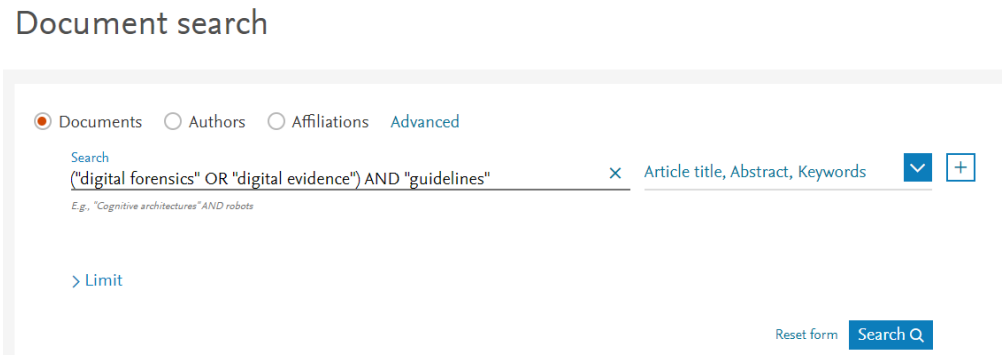


Figura c: Ejecución de la selección, fuente Scopus.

Si se obtienen más de 50 resultados, se aplican filtros adicionales como rangos de fechas, por ejemplo estudios publicados en los últimos dos años:

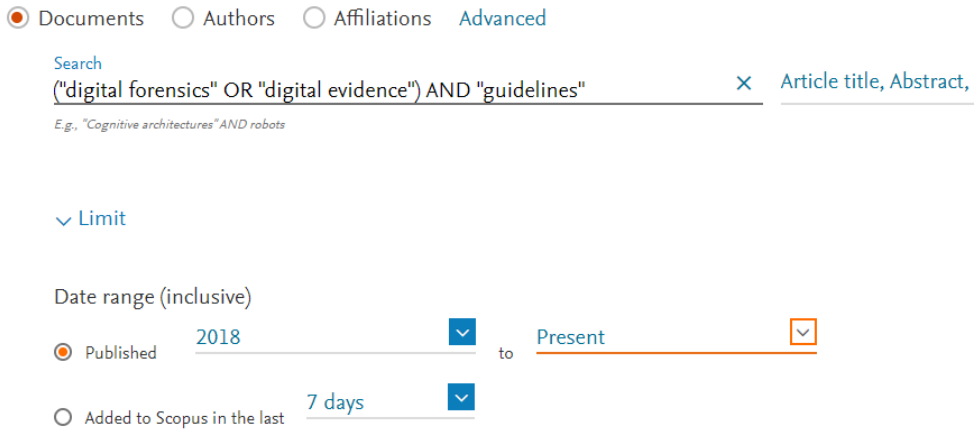


Figura d: Ejecución de la selección con filtros adicionales, fuente Scopus.

Al aplicar todas las cadenas de búsqueda y refinar los resultados, se procede a utilizar los criterios de exclusión para obtener una lista final de estudios seleccionados.

Título del documento	Autores	Año	PDF Link	SJR
Trust in digital records: An increasingly cloudy legal area	Duranti, L., Rogers, C.	2012	https://www.sciencedirect.com/science/article/pii/S0267364912001458?via%3Dihub	0.668
Framework for establishing confidence	Rasjid, Z.E., Soewito	2019	http://www.icicel.org/ell/contents/2019/8/el-13-08-02.pdf	0.194

level of digital evidence admissibility	, B., Witjaksono, G., Abdurahman, E.			
Relativism digital forensics investigations model: A case for the emerging economies	Yeboah-Ofori, A., Yeboah-Boateng, E., Gustav Yankson, H.	2019	https://ieeexplore.ieee.org/document/9058341	-
Rethinking digital forensics	Jones, A., Vidalis, S.	2019	https://www.researchgate.net/publication/332137113_Rethinking_Digital_Forensics	-
A generic framework for digital evidence traceability	Karie, N., Kebande, V., Venter, H.	2016	https://www.researchgate.net/publication/305145851_A_Generic_Framework_for_Digital_Evidence_Traceability	0.137
Digital forensic analysis of cybercrimes: Best practices	Sabillon, R., Serra-Ruiz, J.,	2017	https://www.researchgate.net/publication/314732188_Digital_Forensic_Analysis_of_Cybercrimes_Best_Practices_a	0.139

and methodologies	Cavaller, V., Cano, J.J.		nd_Methodologies	
Digital forensics framework for reviewing and investigating cyber attacks	Athanasios Dimitriadis, Nenad Ivezic, Boonserm Kulvatunyou, Ioannis Mavridis	2019	https://reader.elsevier.com/reader/sd/pii/S2590005619300153?token=C772043BFE4B7733B786999B53930E2C26A0022C0D7E5136BD441EEDC05B92A590FD3A3429C9EFBA0A2F4FDB72A9F2AF	-
On the importance of standardising the process of generating digital forensic report	Nickson. M.Karie, Victor R.Kebandeb	2019	https://www.sciencedirect.com/science/article/pii/S2665910719300088	0.867
Towards Sound Forensic Arguments: Structured Argumentation	Virginia N.L.Franqueira	2020	https://www.sciencedirect.com/science/article/pii/S2666281720300184	0.867

Applied to Digital Forensics Practice				
A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn?	Helen Page, Graeme Horsman	2018	https://www.sciencedirect.com/science/article/abs/pii/S1355030618302211	0.889
A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement	Sungmi Park, Nikolay Akatyev	2018	https://www.sciencedirect.com/science/article/pii/S1742287618300446	0.552
Quality standards for	GillianTully, Neil	2020	https://www.sciencedirect.com/science/article/pii/S26662	0.867

digital forensics: Learning from experience in England & Wales	Cohen		82519300374	

Tabla b.Estudios encontrados en Scopus.

Evaluación de la calidad de los estudios seleccionados

Para la evaluación de la calidad de los estudios seleccionados se consultan las métricas de la publicación o conferencia de donde proviene el estudio. Para esto se utiliza el sitio especializado Scimago y su puntaje conocido como SJ que representa el número promedio de citas ponderadas recibidas en un año, por artículos publicados en una revista en los 3 años anteriores.

En los casos donde no se encontraron datos en Scimago sobre una conferencia de un año específico, se utilizan las de años anteriores. Sin embargo, en algunas ocasiones no se encuentran datos lo cual puede ser debido a lo reciente de la publicación o simplemente a que no ha sido indexada. En general se asume que los estudios tienen una calidad aceptable al estar publicados en la IEEE y en Scopus, ya que para ello deben pasar varios filtros de calidad, sin embargo como parte de un esfuerzo para agregar robustez a la investigación, se utiliza Scimago cuando sea posible.

Anexo B: Legislación sobre delitos informáticos en Costa Rica

Artículos del Código Penal establecidos mediante la ley número 8148 del año 2001:

Artículo 196 bis.- Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.

Artículo 217 bis.- Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

Artículo 229 bis.- Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años.

En dichos artículos de la ley se establecen claramente las sanciones que se impondrán a aquellas personas que sean encontradas como culpables bajo uno o varios de los delitos citados anteriormente. Las penas van desde unos meses en

prisión, hasta de uno a diez años de cárcel, siendo ésta la pena más elevada. Además, la Sección de Delitos Informáticos se apoya en otras leyes especiales en donde se detallan artículos donde se castigan los delitos informáticos. Principalmente se apoyan en las siguientes leyes y reglamentos:

1. Ley General de Aduanas, Capítulo II, Artículos 221 y 222.
2. Ley de la Administración Financiera de la República y sus Presupuestos.
3. Artículo 111: Ley de Derechos de Autor, Derechos Conexos.
4. Otros reglamentos y manuales que algunas instituciones públicas han creado con el fin de regular el buen uso de los sistemas informáticos.

Artículos del Código Penal establecidos mediante la ley número 9048 del año 2012:

Artículo 167.- Corrupción. Será sancionado con pena de prisión de tres a ocho años quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta. La pena será de cuatro a diez años de prisión, si el actor, utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busca encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz; utiliza a estas personas para promover la corrupción o las obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o verlos ejecutar.

Artículo 196.- Violación de correspondencia o comunicaciones. Será reprimido con pena de prisión de tres a seis años quien, con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización, se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidos a otra persona. La pena será de cuatro a ocho años de prisión si las conductas descritas son realizadas por:

a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.
b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 196 bis.- Violación de datos personales. Será sancionado con pena de prisión de tres a seis años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de cuatro a ocho años de prisión cuando las conductas descritas en esta norma:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

b) Cuando los datos sean de carácter público o estén contenidos en bases de datos públicas.

c) Si la información vulnerada corresponde a un menor de edad o incapaz.

d) Cuando las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

Artículo 214.- Extorsión. Será reprimido con pena de prisión de cuatro a ocho años al que para procurar un lucro obligue a otro, con intimidación o con amenazas

graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero.

La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica.

Artículo 217 bis.- Estafa informática. Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 229 bis.- Daño informático. Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.

Artículo 288.- Espionaje. Será reprimido con prisión de cuatro a ocho años al que procure u obtenga indebidamente informaciones secretas políticas o de los cuerpos de policía nacionales o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la nación, o afecte la lucha contra el narcotráfico o el crimen organizado.

La pena será de cinco a diez años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.

Artículo 229.- Daño agravado. Se impondrá prisión de seis meses a cuatro años: a) Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos.

Artículo 229 ter.- Sabotaje informático. Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

La pena será de cuatro a ocho años de prisión cuando:

a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.
b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.
d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

Artículo 230.- Suplantación de identidad. Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero. La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz.

Artículo 231.- Espionaje informático. Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.

Artículo 232.- Instalación o propagación de programas informáticos maliciosos. Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.

La misma pena se impondrá en los siguientes casos:

a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.
b) A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.
c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.
d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.

e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

I. Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.
II. Afecte el funcionamiento de servicios públicos.
III. Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.
IV. Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.
V. Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.
VI. Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.

Artículo 233.- Suplantación de páginas electrónicas. Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

Artículo 234.- Facilitación del delito informático. Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

Artículo 235.- Narcotráfico y crimen organizado. La pena se duplicará cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.

Artículo 236.- Difusión de información falsa. Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.

Anexo C: Boleta única de cadena de custodia de indicios

BOLETA ÚNICA DE CADENA DE CUSTODIA DE INDICIOS

Número Único: _____ N° Consecutivo del indicio: _____

Lugar de recolección:_____

_____

Nombre del(de la) recolector(a): _____

Fecha de recolección (día/mes/año): _____Hora (formato 24 horas): _____

Descripción del paquete e indicio: _____

_____

	Nombre Completo	**Organización donde pertenece quien entrega/recibe**	**Fecha**	**Hora**	**Firma**
Entrega					
Recibe					
Entrega					
Recibe					
Entrega					
Recibe					

Anexo D: Documento de transporte de evidencia

DOCUMENTO DE TRANSPORTE DE EVIDENCIA

Número Único: _____ N° Consecutivo del indicio: _____

Lugar de entrega: _____

_____

Nombre de quien entrega: _____

Nombre de quien recibe: _____

Fecha de entrega (día/mes/año): _____Hora (formato 24 horas): _____

Descripción del paquete e indicio: _____

_____

_____

_____

_____ _____

Firma de quien entrega Firma de quien recibe

Lista de actividades a la que fue sometida la evidencia antes de su entrega:

Fecha	**Actividad**	**Responsable**	**Firma**

Adjuntar fotos del estado de la evidencia antes de su entrega.

Anexo E: Boleta de control de indicios

INDICIO Y/O EVIDENCIA

LUGAR:	**FECHA:**	**HORA:**
Articulo:		
Número Único:		
Personas Ofendida:		
Persona Imputada:		
Dirección:		
Recolectado por:		
Técnica utilizada para el levantamiento del indicio:		
Descripción del indicio:		
Nombre e Identificación del responsable de la recolección:		
Firma:		

Anexo F: Plantilla dictamen pericial

ACTORA
VS
DEMANDADO
JUICIO: ORDINARIO CIVIL
EXPEDIENTE: 12345678/2022

C. JUEZ UNO DOS TRES CUATRO, CON RESIDENCIA EN ALGÚN LUGAR DE UN GRAN PAÍS.
P r e s e n t e.

El que suscribe, José Arcadio Buendía, perito designados por PANCHO LÓPEZ, "PARTE ACTORA", para rendir dictamen pericial en materia de informática, con domicilio ubicado en Avenida de los Insurgentes Sur 1863-301, Colonia Guadalupe Inn, Delegación Álvaro Obregón, C. P. 01020, Ciudad de Heredia, se identifica con carnet profesional número 123145, emitido a mi favor por el Colegio de Profesionales en Informática y Computación..

Respetuosamente vengo a entregar el siguiente dictamen pericial:

DICTAMEN

I. PLANTEAMIENTO DEL PROBLEMA

De forma neutral explicar ¿qué van a analizar los peritos, qué es lo que se está cuestionando?

II. OBJETIVOS

De forma NEUTRAL, decir qué objetivos se buscan.

III. FORMULACIÓN DE HIPÓTESIS

Narrar cuál es el origen de los elementos cuestionados e indicar ya cargando el dictamen a su favor, que hipótesis están defendiendo ustedes.

IV. MÉTODO EMPLEADO

- Explicar el método científico o normas que utilizaste para realizar la investigación, estas son relativas al caso y varían en cada caso en particular.

V. TÉCNICAS EMPLEADAS

Explicar qué técnicas usaste para analizar la evidencia y llegar a las conclusiones

VI. CONSIDERACIONES TÉCNICAS PREVIAS

Si existen fé de hechos, protesta de cargos, declaración jurada, o elementos digitales que son relevantes, se puede hacer mención de ellos, por ejemplo, de acuerdo a la inspección el servidor 12345 estaba encendido el día que se hizo el análisis.

VII. CONSIDERACIONES TÉCNICAS DETERMINADAS

Narrar cómo viste la evidencia y que fue lo que hiciste para extraer la evidencia.

VIII. CUESTIONARIO

1. *Diga el perito los elementos …*

P R O T E S T O L O N E C E S A R I O

Guanacaste, Costa Rica, a xx de XXXXX de 2022.

Ing. José Arcadio Buendía

PERITO EN INFORMÁTICA

Anexo G: Declaración Jurada - Protesta de cargo

ACTORA
VS
DEMANDADO
JUICIO: ORDINARIO CIVIL
EXPEDIENTE: 12345678/2022

C. JUEZ UNO DOS TRES CUATRO, CON RESIDENCIA EN ALGÚN LUGAR DE UN GRAN PAÍS.
P r e s e n t e.

José Arcadio Buendía, licenciado en ingeniería en sistemas de información, perito designado por la parte AAAAAAAAAA, PEDRO PICAPIEDRA, en mi carácter de Perito en materia Informática Forense, para lo cual anexo ORIGINAL del carnet profesional número 123145 (CON NUMERO ESCRITO), emitido a mi favor por el Colegio de Profesionales en Informática y Computación, respetuosamente vengo a manifestar lo siguiente:

Que por medio del presente documento comparezco y ACEPTO el cargo conferido como perito en materia de informática forense, MANIFESTANDO, BAJO PROTESTA DE DECIR VERDAD, que tengo experiencia para lo cual anexo ORIGINAL de mi más reciente capacitación en “informática forense”, y la capacidad suficiente para emitir dictamen pericial sobre el particular dado que conozco los puntos cuestionados y pormenores relativos a la pericial, quedo también obligado a rendir dentro del término el dictamen respectivo toda vez que tengo la capacidad para emitir el mismo sobre el particular, y manifiesto que desempeñaré mis funciones con prontitud y bajo los principios de objetividad, probidad y profesionalismo.

Manifiesto además, que llevaré a cabo mi análisis pericial siguiendo los estándares internacionales y buenas prácticas sobre el cómputo forense, cumpliendo en cada fase de la investigación con lineamientos base tales como:

Reconocimiento

- El analista debe contar con las calificaciones requeridas para completar una investigación de delitos informáticos.
- Se debe levantar la cadena de custodia utilizando los formatos oficiales del ministerio de seguridad pública o los recomendados por estándares internacionales
- El analista deberá contar con las herramientas mínimas necesarias
- La escena del incidente debe ser documentada de manera visual
- Identificar los dispositivos digitales que necesitan ser recogidos
- El estado de los dispositivos debe mantenerse tal y como se encuentra
- Identificar sistemas de videovigilancia
- Identificar los servicios prestados por los dispositivos de red
- Identificar posibles cargadores de batería y cables de los dispositivos
- Utilizar un detector de señales inalámbricas
- Identificar a las personas responsables de las instalaciones/dispositivos en el lugar de los hechos
- El proceso de identificación de la evidencia digital debe ser documentado
- La evidencia digital debe ser clasificada en base a su volatilidad
- Utilizar algún documento de referencia reconocido para la identificación de la evidencia digital

Recolección

- La evidencia física debe ser recolectada
- Realizar un análisis de rastros biológicos previo a la manipulación de los dispositivos electrónicos
- Documentar el proceso de etiquetado y empaquetado de la evidencia digital
- Justificar la exclusión de dispositivos digitales en el proceso de recolección
- Crear una copia de los datos volátiles y del estado actual de los dispositivos antes de apagarlos

- Remover la batería en vez de presionar el botón de apagado en el caso de las laptops
- Apagar los dispositivos desconectando directamente la fuente eléctrica
- Recoger los dispositivos encendidos sin interrumpir el suministro de electricidad
- Tomar las precauciones necesarias para evitar que la electricidad estática genere daños al retirar un disco duro
- Los dispositivos de la red deben ser aislados
- Se deben revisar los sistemas de videovigilancia

Extracción

- La documentación del proceso de extracción debe permitir que sea reproducible y verificable por terceros
- Tanto las fuentes originales como las copias realizadas deben ser verificadas utilizando una función de verificación comprobada
- Extracciones parciales deben ser realizadas de ser necesario
- Crear copias maestras y copias de trabajo
- Los datos volátiles deben ser extraídos
- Utilizar un contenedor lógico para almacenar los datos volátiles
- Se debe aplicar la función hash a los dispositivos de almacenamiento originales y sus copias para garantizar su autenticidad
- Utilizar la firma digital sobre la posible evidencia digital extraída
- Extraer información de los sistemas de videovigilancia
- Utilizar herramientas confiables en el proceso de extracción
- Asociar al analista con la posible evidencia digital extraída
- Revisar que los dispositivos en apariencia apagados estén realmente apagados
- Utilizar buenas prácticas provenientes de algún documento de referencia reconocido para extracción en medios de almacenamiento

Protección

- Utilizar un estándar o documento de referencia reconocido para seguir las prácticas adecuadas sobre la manipulación segura de la evidencia digital
- Durante el empaquetado se debe proteger a cada dispositivo electrónico según sus características y naturaleza
- La evidencia digital debe contar con un documento de transporte.
- Los encargados de la recepción de la evidencia digital deben contar con las calificaciones requeridas para garantizar su integridad y seguridad jurídica.
- La persona que entrega la evidencia digital debe ser la misma que se registra en el último eslabón de entrega.
- La bodega para custodia de evidencia debe cumplir con los siguientes requerimientos.
- El personal involucrado en la labor forense digital no deberá verse involucrado en fuga de información o en dar interpretaciones subjetivas que puedan tomarse como difusión de información falsa

Análisis

- El análisis debe incluir la identificación de personas, lugares, artículos y eventos, y determinar cómo se relacionan estos elementos para que se pueda llegar a una conclusión.
- Comprobar que los hashes de la copia de trabajo coinciden con los de la copia maestra.
- El analista debe examinar las copias de trabajo, no las copias maestras
- Se deben revisar los encabezados de los archivos para determinar su contenido
- El analista debe tener un conjunto de herramientas forenses para el examen y análisis de datos
- El analista debe reconstruir el orden cronológico de los eventos
- No alterar los tiempos MAC durante el análisis
- El analista debe reunir datos de varias fuentes
- Incluir cualquier información que desprenda una acción como parte de la boleta única de cadena de custodia.

Informe

- Se debe confeccionar la Boleta Única de Cadena de Custodia
- Se debe adjuntar la boleta de control de indicios a la boleta única de cadena de custodia.
- Se debe adjuntar a la boleta única de cadena de custodia todos los documentos relevantes para garantizar su trazabilidad.
- Trazabilidad paralela a la Boleta Única de Cadena de Custodia.
- El documento de cadena de custodia debe incluir un dictamen pericial sobre la evidencia digital obtenida del análisis
- El documento de cadena de custodia debe incluir un reporte técnico sobre la evidencia digital obtenida del análisis

POR LO ANTES EXPUESTO A USTED C. JUEZ UN DOS TRES CUATRO, RESPETUOSAMENTE LE SOLICITO SE SIRVA:

ÚNICO. Tenerme por presentado en términos del presente escrito, aceptando el cargo conferido como perito en materia de informática forense, y protestando su fiel y legal desempeño.

P R O T E S T O L O N E C E S A R I O

Guanacaste, Costa Rica, a xx de XXXXX de 2022.

Ing. José Arcadio Buendía

Anexo H: Lista de recursos forenses

Herramientas para la práctica del cómputo forense:

Fase	Descripción	Nombre	URL
Recolección, Análisis, Reporte	Ayuda a localizar evidencia hasta presentarla en la corte	EnCase Forensic	https://security.opentext.com/encase-forensic
Recolección	Dispositivos de bloqueo de escritura	Tableau Forensic SATA/IDE Bridge	https://security.opentext.com/tableau/hardware/details/t35u
		Forensic ComboDock, model FCDv5.5	https://wiebetech.com/products/forensic-combodock-v5-5/
Recolección	Software de bloqueo de escritura	SAFE Block	https://www.forensicsoft.com/products/safe-block
		WriteBlocking Validation Utility	https://www.cru-inc.com/support/software-downloads/writeblocking-validation-utility/
Extracción	Imagen forense	Tableau Forensic Imagers and Duplicators overview	https://security.opentext.com/tableau/hardware/forensic-imagers-duplicators
		FTK® Imager	https://go.exterro.com/l/43312/2022-01-21/f6h1s3
		Guymager	https://guymager.sourceforge.io/
Extracción, Análisis	Búsqueda por palabras clave	MailXaminer	https://www.mailxaminer.com/keywords.html
		Autopsy	https://www.autopsy.com/

		Android Analyzer Module	https://sleuthkit.org/autopsy/docs/user-docs/3.1/android_analyzer_page.html
		Interesting Files Identifier Module	http://sleuthkit.org/autopsy/docs/user-docs/4.12.0/interesting_files_identifier_page.html#:~:text=The%20Interesting%20Files%20module%20allows,files%20with%20a%20certain%20type
Extracción	Recuperación de datos	Scalpel	https://github.com/machn1k/Scalpel-2.0
		Bulk_extractor	https://github.com/simsong/bulk_extractor
		foremost	https://github.com/jonstewart/foremost
		EVTXtract	https://github.com/williballenthin/EVTXtract
		EXIF Tool - Herramienta para esteganografía	https://exiftool.org/
Análisis	Análisis en caliente, recuperación de memoría volátil.	Volatility	https://github.com/volatilityfoundation/volatility
		FTK® Imager	https://go.exterro.com/l/43312/2022-01-21/f6h1s3
		Agave 64 - Es un grupo de herramienta Windows para el análisis en caliente. 1. CurrProcess: Todos los procesos activos y las librerias que llama. 2. DisckCounter: ver los discos. 3. DriveLetterView: todas las	https://archive.org/details/Agave64

		unidades inclusive las usbs. 4. LastActivityView: Ver la actividad de las carpetas. 5. MyEventView: Visor de eventos mas potente que el de Windows. 6. RecentFilesView: Visualizador de archivos incluso aquellos que ya no están. 7. USBDeview: Se ven las usb que se han conectado cuando y la ultima vez. 8. WhatInStartup: Que se levanta con la maquina, ver los ejecutables. 9. WinAudit: Todo el inventario de la maquina incluso hasta los procesos que no son de windows.	
Análisis	Esta página analiza cualquier archivo para determinar si ha sido reportado como un virus o malware.	Virus Total	https://www.virustotal.com/#/home/upload
Protección	Suma de chequeo o checksum (Crear hash)	IgorWare Hasher	https://www.igorware.com/hasher/download
		HasCheck	https://github.com/gurnec/HashCheck

		HashMyFiles	https://www.nirsoft.net/utils/hash_my_files.html
		OSForensics	https://www.osforensics.com/download.html
Análisis	Análisis de tráfico de red	Wireshark	https://www.wireshark.org/download.html
		NetworkMiner	https://www.netresec.com/?page=NetworkMiner
Análisis	Sistema de Prevención de Intrusos	Snort	https://www.snort.org/
		Suricata	https://suricata.io/