UNIVERSIDAD TÉCNICA DEL NORTE

FALCUTAD DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Elaboración de una metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 para su aplicación en el Ecuador

Línea de investigación: Desarrollo, Aplicación de Software, Cyber Security.

AUTOR: Jaime Alexander Orna Lora

DIRECTOR: Ing. Víctor Hugo Benítez Bravo, MSc.

IBARRA - ECUADOR

2024

AGRADECIMIENTO

A Dios, que ha sido fuente de mi salud, fuerza y sabiduría a lo largo de mi vida.

A mis amados Padres, no existen palabras suficientes para expresar toda mi gratitud por su fe, su guía en cada paso de mi vida, su generosidad y su ayuda incansable en todos los momentos. Gracias a ustedes, he alcanzado otra meta en mi vida.

A mi esposa Kathy, por su apoyo incondicional en todos los proyectos que hemos forjado a través de los años que llevamos juntos, y que espero sirva de ejemplo para nuestros hijos Samy y Martín.

DEDICATORIA

A mis padres, por caminar junto a mí en todas las etapas de mi vida, por su amor incondicional, por creer y ser parte de mis sueños, por sus sacrificios y su apoyo constante que han sido la clave de mi éxito.

A mi esposa Kathy, que es mi compañera de vida y a nuestros hijos Samy y Martin que son la motivación para alcanzar nuevos logros.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

Yo, Víctor Hugo Benítez Bravo, certifico que el estudiante Jaime Alexander Orna Lora con Cédula N. 100222975-3 ha elaborado bajo mi tutoría la sustentación del trabajo de grado titulado: **"ELABORACIÓN DE UNA METODOLOGÍA DE BUENAS PRÁCTICAS DEL PERITO INFORMÁTICO EN TELECOMUNICACIONES BAJO LA NORMA ISO 27037 PARA SU APLICACIÓN EN EL ECUADOR".**

Este trabajo se sujeta a las normas y metodologías dispuestas en el reglamento del título a obtener, por lo tanto, autorizo la presentación a la sustentación para la calificación respectiva.

Ibarra, a los 18 días de enero de 2024

Victor Hugo Benitez

Firmado digitalmente por Victor Hugo Benitez
Fecha: 2024.01.18 10:11:10 -05'00'

MsC. Víctor Hugo Benítez Bravo

CI: 0602990699

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	1002229753		
APELLIDOS Y NOMBRES	Orna Lora Jaime Alexander		
DIRECCIÓN	Quito, El Condado		
EMAIL	alexander_sm_ak18@hotmail.com		
TELÉFONO FIJO		**TELÉFONO MÓVIL:**	0992701269

DATOS DE LA OBRA	
TÍTULO:	Elaboración de una metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 para su aplicación en el Ecuador.
AUTOR (ES):	Orna Lora Jaime Alexander
FECHA: DD/MM/AAAA	18/01/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA DE POSGRADO	☐ PREGRADO ■ POSGRADO
TITULO POR EL QUE OPTA	Maestría en Telecomunicaciones
TUTOR	Ing. Víctor Hugo Benítez Bravo, MSc

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 18 días del mes de enero del año 2024.

EL AUTOR:

Firma 

_____

Nombre: Jaime Alexander Orna Lora

INDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto se enfoca en el diseño de una Metodología para buenas prácticas del perito informático de Telecomunicaciones en Ecuador, basada en la norma ISO 27037. El objetivo principal es mejorar la calidad y eficiencia de las investigaciones de delitos informáticos en el ámbito de las telecomunicaciones. La metodología de investigación utilizada se basó en un enfoque cualitativo, que incluyó la realización de encuestas y la observación participante con expertos peritos informáticos en Telecomunicaciones en Ecuador. También se llevó a cabo un análisis de documentos y registros técnicos relevantes. El campo de aplicación de esta metodología se centra en las investigaciones de delitos informáticos en el ámbito de las telecomunicaciones, abarcando aspectos como el análisis de evidencia digital, el manejo de hardware y software forense, y la aplicación de buenas prácticas en conformidad con la norma ISO 27037. La conclusión más relevante del proyecto es que la metodología propuesta es considerada clara, completa y aplicable en la práctica por los expertos peritos informáticos en Telecomunicaciones en Ecuador. Además, se destaca que la metodología incorpora las mejores prácticas de la norma ISO 27037 y su aplicación en el contexto ecuatoriano. Esto sugiere que la metodología puede ser una herramienta valiosa para mejorar la calidad y eficiencia de las investigaciones de delitos informáticos en el ámbito de las telecomunicaciones en el país.

Palabras Clave: Metodología, Perito informático, Delitos informáticos, Telecomunicaciones, Norma ISO 27037.

ABSTRACT

This project focuses on the design of a Methodology for best practices of the telecommunication's forensic expert in Ecuador, based on ISO 27037 standard. The main objective is to improve the quality and efficiency of investigations in the field of cybercrimes in the telecommunications sector. The research methodology employed a qualitative approach, including surveys and participant observation with expert telecommunications forensic experts in Ecuador. Additionally, an analysis of relevant documents and technical records was conducted. The scope of application of this methodology is centered around cybercrime investigations in the telecommunications field, covering aspects such as digital evidence analysis, handling of forensic hardware and software, and the implementation of best practices in accordance with ISO 27037 standard. The most significant conclusion of the project is that the proposed methodology is considered clear, comprehensive, and applicable in practice by the telecommunication's forensic experts in Ecuador. Furthermore, it is highlighted that the methodology incorporates the best practices of ISO 27037 standard and their application in the Ecuadorian context. This suggests that the methodology can be a valuable tool in improving the quality and efficiency of cybercrime investigations in the telecommunications sector in the country.

Keywords: Methodology, Forensic expert, Cybercrimes, Telecommunications, ISO 27037 standard.

INTRODUCCIÓN

En el contexto actual de la sociedad de la información, la tecnología se ha convertido en un elemento clave en la resolución de casos judiciales relacionados con las telecomunicaciones y el uso de la tecnología digital. En este sentido, los peritos informáticos juegan un papel fundamental en el procesamiento y análisis de las evidencias digitales para esclarecer los hechos.

Sin embargo, es necesario contar con una metodología de buenas prácticas para que el trabajo del perito informático se realice de manera efectiva, eficiente y ética. En este sentido, el objetivo principal de esta investigación es diseñar una metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 para su aplicación en Ecuador.

Para lograr este objetivo general, se plantean los siguientes objetivos específicos: conocer el estado del arte, características y lineamientos del rol de perito informático en el procesamiento de la información de los delitos; analizar el marco legal vigente que se considera para el análisis y la revisión de la normativa internacional ISO 27037 del año 2017; verificar el campo de acción, ámbito de aplicación, hardware, software y evidencias digitales; y elaborar y validar la metodología para los peritos informáticos que se aplicaría bajo las normas de las buenas prácticas de la norma ISO 27037.

Esta investigación se justifica por la necesidad de contar con una metodología de buenas prácticas del perito informático en Telecomunicaciones que se adapte a la normativa internacional y nacional. Asimismo, se busca fortalecer la labor de los peritos informáticos en la investigación y esclarecimiento de delitos relacionados con las telecomunicaciones y el uso de la tecnología digital, contribuyendo así a la justicia y al fortalecimiento del Estado de derecho.

En cuanto a la metodología de investigación, se utilizará un enfoque cualitativo, que permitirá obtener información detallada y precisa acerca de las características y

elementos relevantes en el trabajo del perito informático. Para ello, se aplicarán técnicas de observación participante, grupo nominal y método Delphi, que permitirán la participación activa y colaborativa de expertos en la materia.

En cuanto a la estructura de la investigación, se dividirá en cuatro fases principales: planificación, adquisición, análisis y presentación. En la fase de planificación se establecerán los objetivos y alcances del proyecto, se identificarán los recursos necesarios y se establecerán las directrices para el desarrollo de la metodología. En la fase de adquisición se identificarán y recolectarán los datos necesarios, asegurando su integridad y preservación para su posterior análisis. En la fase de análisis se realizará el análisis de la evidencia digital adquirida, utilizando técnicas y herramientas forenses para identificar y evaluar la relevancia de la información. En la fase de presentación se presentarán los resultados del análisis en un informe forense, siguiendo las pautas establecidas en la norma ISO/IEC 27037:2012.

1. CAPITULO I:

EL PROBLEMA

1.1 Problema de investigación

El desarrollo de la tecnología ha permitido que la industria de las telecomunicaciones logre avances sin precedentes en este mundo globalizado, Ecuador no es la excepción, aun cuando no está a la par de las grandes potencias, pero posee gran infraestructura en esta área y cada día que pasa surgen nuevos proyectos que nos permiten disminuir la brecha tecnológica.

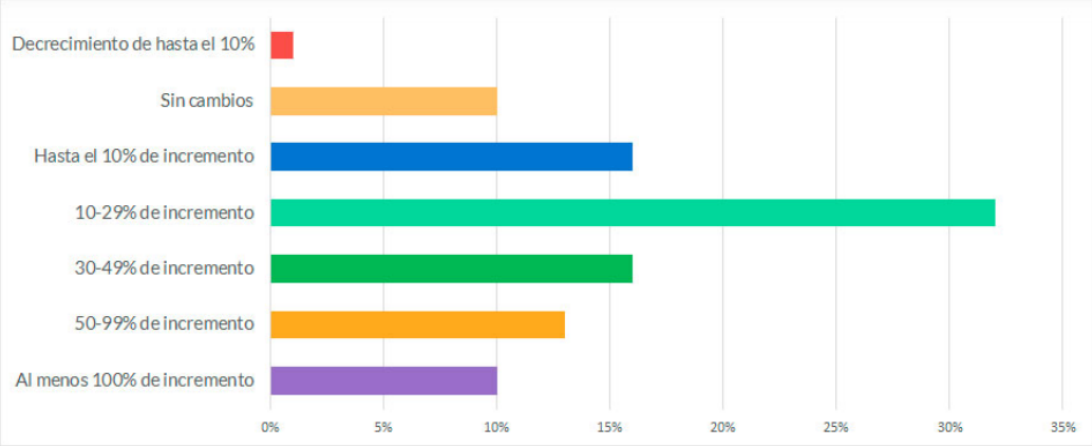
Hoy en día el progreso de las telecomunicaciones ha permitido fomentar el conocimiento de nuevos horizontes de la tecnología y es muy fácil encontrar información en la red, la investigación científica ha dada pasos gigantescos y las industrias utilizan en cada proceso las telecomunicaciones, por tanto, se debe invertir en esta área de la tecnología que nos permitirá obtener importantes réditos para el país y la sociedad. (Ferruzola Gomez & Cuenca Espinoza, 2015)

El interés generado por estas nuevas tecnologías se da principalmente por la gran cantidad de aplicaciones que se manejan, que facilitan nuestra vida cotidiana, aseguran y mejoran los procesos industriales, dotándonos de las herramientas suficientes que permiten que la información fluya de manera casi natural, permitiéndonos un desarrollo común.

El impacto de las telecomunicaciones sobre las sociedades tiene mayormente un lado positivo, aunque en ciertos casos como el aislamiento social, la dificultad de uso para nuestros mayores, violencia cibernética, los peligros de nuestros menores expuestos a depredadores en línea, menor comunicación interpersonal cara a cara, son algunos de los aspectos negativos; se puede resaltar como ventajas el crecimiento de PIB, la productividad en empleos públicos y privados, la modernización y agilidad de los procesos individuales y particulares. (Huichalaf, 2014)

En todas las actividades descritas anteriormente se almacena grandes cantidades de información privada en equipos informáticos, dicha información es muy importante para el desarrollo de las actividades de las personas, empresas e incluso del Estado, salvaguardar todos estos datos es de suma importancia por lo que se invierten gran cantidad de recursos económicos (figura 1) en dotar de elementos tecnológicos que aseguren su manipulación, recolección y almacenamiento adecuados. (Bolaños-Burgos, 2016)

Figura 1: Porcentaje de empresas que considera que va a variar el presupuesto de Ciberseguridad para los próximos tres años.



Nota: en la imagen se puede apreciar las estadísticas de asignaciones para ciber seguridad en los próximos años , fuente: (Cámara-Valencia, 2018)

La manipulación de los datos almacenados, por manos ajenas a sus usuarios, podría afectar y perjudicar moral, civil o penalmente a cualquiera persona o entidad, sea pública o privada, debido a que la información almacenada en cualquier elemento tecnológico puede ser manipulada, alterada o borrada, es decir, se pueden modificar los datos o registros. (Bahadur, 2015)

La modificación de la información de un elemento informático o telemático que vulnere los derechos del titular, afectando el software o hardware, para beneficio personal o de terceros se conoce como delito informático, este ilícito puede darse a través de una vía local o remotamente. (Pino, 2012)

Ahora bien, para validar de forma técnica estos incidentes de seguridad informática que permitan recabar, asegurar, respaldar y recuperar la información, es fundamental la presencia de personal calificado en peritaje informático, que a través de técnicas y métodos de investigación pueda reconstruir, de manera correcta el evento o secuencia de eventos de los equipos o plataformas tecnológicas.

Los procesos de la gestión de seguridad de los datos en las plataformas tecnológicas y activos de la información no cuentan con sistemas de protección absoluta, siempre existen vulnerabilidades, es aquí donde las organizaciones trabajan en la implementación de sistemas acordes a las necesidades.

En Ecuador las investigaciones periciales en el área de la informática no han sido estudiadas adecuadamente, por tanto, no se han desarrollado eficazmente y la principal causa es el desconocimiento de las tecnologías que estudian estos delitos. (J. Sampaoli, 2018)

En nuestro medio no existe un escenario maduro que permita realizar el análisis de los incidentes informáticos, existen vacíos legales y técnicos que no permiten resolverlos de manera adecuada y no existe una metodología vigente de buenas prácticas para peritos informáticos que permita analizar, estudiar y juzgar los delitos informáticos.

El presente proyecto pretende crear los lineamientos generales para la formación de nuevos profesionales con ética, que manifiesten deontología y profesionalismo en todas sus actividades periciales, a través de los artículos 190, 191, 229 a 234 del COIP, esta parte de la legislación se encarga de los delitos informáticos y medios electrónicos fraudulentos, sin embargo, se nota el poco alcance y la falta de dinámica de nuestras leyes para contrarrestar este tipo de delitos. (Codigo Organico Integral Penal, 2018)

La línea de investigación del proyecto corresponde al Desarrollo, aplicación de software, cyber security, ligado a la misión de la misión de la Universidad Técnica del Norte que genera, fomenta, y ejecuta procesos de investigación, de transferencia de conocimientos científicos, tecnológicos y de innovación.

Se alinea con el objetivo 8 del Plan Nacional de Desarrollo 2017-2021, que en su política cita en los puntos:

> 8.2 Fortalecer la transparencia en la gestión de instituciones públicas y privadas y la lucha contra la corrupción, con mejor difusión y acceso a información pública de calidad, optimizando las políticas de rendición de cuentas y promoviendo la participación y el control social.
>
> 8.4 Luchar contra la impunidad, fortaleciendo la coordinación interinstitucional y la eficacia de los procesos para la detección, investigación, juzgamiento, sanción y ejecución de penas. (Plan Nacional de Desarrollo, 2017, p. 14).

1.1.1 Pregunta de investigación

¿Cómo diseñar una metodología de buenas prácticas para el perito informático en Telecomunicaciones en Ecuador, con base en la norma ISO 27037, para mejorar la calidad y eficacia de su trabajo y así contribuir a la lucha contra los delitos informáticos en el país?

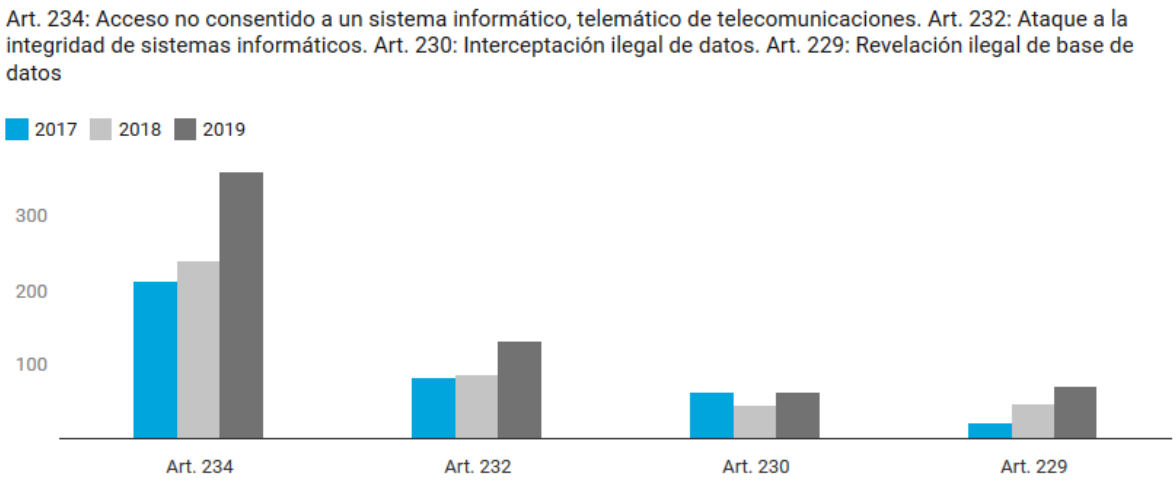
1.2 Antecedentes

Hoy en día en la Universidad Técnica del Norte existen pocos estudios referentes a los delitos informáticos y al peritaje informático.

Estos nuevos desarrollos tecnológicos de pericias en al área informática muestran un crecimiento visible en los países industrializados, donde las telecomunicaciones son el canal principal de transmisión de los datos y su uso acompaña al hombre en la mayoría de las actividades personales y laborales, lo mismo ocurre aquí en Ecuador, donde estas nuevas tecnologías se muestran como parte de la nueva era digital, donde los datos digitales corren el riesgo de ser copiados, borrados o divulgados, de tal forma que la privacidad de los usuarios se vea alterada por terceros. (Majed et al., 2020)

En la siguiente figura se muestran los delitos informáticos más comunes en Ecuador registrados y se menciona el artículo del COIP relacionado:

Figura 2: Deloitte/Fiscalía General del Estado. Delitos informáticos en el Ecuador. (Ávila, 2019)



Debido a la emergencia sanitaria estos delitos se han incrementado hasta en un 35% en el mundo entero, los criminales cibernéticos aprovechan el momento para crear confusión entre los ciudadanos y transmitir noticias falsas, del mismo modo las transacciones digitales han sido atacadas debido al confinamiento. “David López, vicepresidente de ventas para América Latina de AppGate, indica que los métodos que más han aumentado son el phishing (copia de un sitio web de uso masivo para obtener datos personales), malware (ataque informático para controlar dispositivos y obtener información) y suplantación de identidad.” (Astudillo, 2020)

Ahora bien, es necesario precautelar la seguridad de los datos digitales, a fin de evitar que se corrompan, es aquí donde aparece el análisis digital forense, que tiene el objeto de disminuir los delitos cibernéticos, terrorismo y fraudes comunes a través del análisis minucioso de los datos, permitiendo revelar a las personas que buscan beneficiarse de esto.

Las herramientas forenses han alertado a los piratas informáticos, ya que los nuevos sistemas de Gestión de Seguridad de la Información están vigentes y en constante evolución, estos sistemas se preocupan por el aseguramiento de los datos de los usuarios, y como complemento se han desarrollado herramientas anti-forenses desde un punto de vista ético se podrán considerar a la hora de auditar un sistema comprometido o alterado en un incidente de seguridad. (Majed et al., 2020)

En la investigación realizada en la Universidad Estatal Bowling Green, se realizó el estudio sobre la "Experiencia en la incorporación de estándares (NIST INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA) en un Plan de estudios de forense digital" basados en tres temas muy importantes dentro de la especialización forense digital como son: bloqueador de escritura de hardware, recuperación de archivos eliminados y análisis forense móvil, con resultados alentadores que encaminan el presente estudio hacia la elaboración de una metodología actualizada, permitiendo que los peritos informáticos puedan contar con una herramienta tecnológica a la par de países con mayores desarrollos tecnológicos. (Roy et al., 2019)

Otro estudio para el despliegue de estas tecnologías se muestra en el artículo "Investigación sobre diseño de sistemas e implementación de informática forense basada en registros", donde se apuesta como herramienta fundamental para la recolección de la información técnicas como: seguridad del sistema informático y acceso a archivos para evitar el daño o alteración del original, tecnología para recopilar datos con seguridad, seguridad del diseño del medio de almacenamiento, tecnología de espejo reflejado, tecnología para recuperación y reconstrucción de archivos ya eliminados, recuperación de archivos de cache, recuperación de archivos temporales, recuperación de datos de tiempo, tecnología de acceso a datos de flujo de red, todos estos parámetros son necesario para el correcto desarrollo de los procesos periciales, que son el fin del presente proyecto. (Wen, 2017)

Para la elaboración de este marco metodológico pericial se utilizará como referencia las normativas internacionales, una de las más importantes es el Reglamento General de

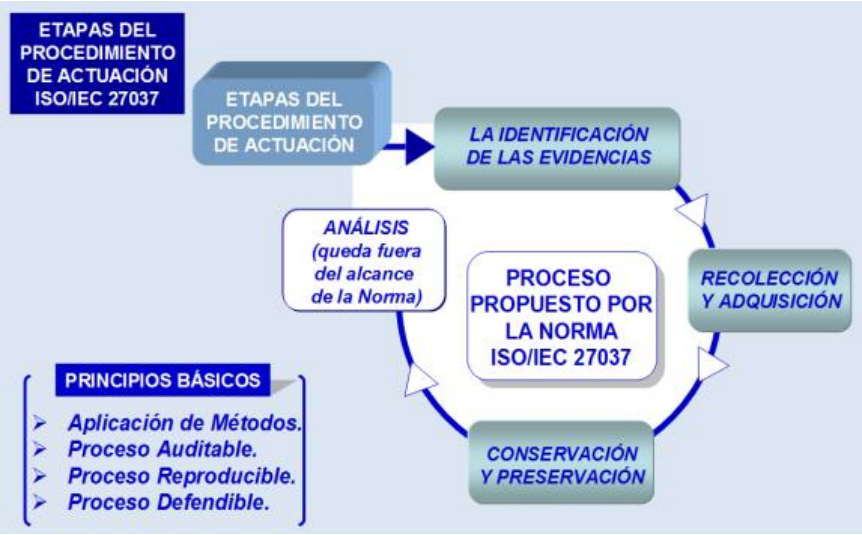
Protección de Datos RGPD (antiguamente LOPD), documento emitido por la unión europea en 2018, que sigue en estudio y se viene actualizando constantemente. A continuación, se presenta en la figura 1, los principales cambios de este reglamento:

Figura 3: Principales cambios entre las dos regulaciones LOPD y RGPD.

Nota: En la figura se puede apreciar las diferencias entre LOPD y RGPD (Brocca, 2018)

Otra normativa actualizada es la ISO/IEC 27037:2012 que tiene como objetivo la Recopilación de Evidencias, actividad que es extremadamente delicada y compleja, su valía en ámbito legal y técnico depende del proceso que se realiza durante las recolección y preservación de los datos como se muestra en la figura a continuación:

Figura 4: Fases de la actuación pericial según ISO 27037.



Nota: En la imagen se aprecia el detalle de la normativa ISO 27037.

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Diseñar una Metodología para buenas prácticas del perito informático de Telecomunicaciones en Ecuador, con base en la norma ISO 27037.

1.3.2 Objetivos específicos

- Analizar el Marco legal vigente que se considera para el análisis y la revisión de la normativa internacional ISO 27037.
- Verificar el campo de acción, ámbito de aplicación, hardware, software y evidencias digitales.
- Elaborar y validar la Metodología para los peritos informáticos que se aplicaría bajo las normas de las buenas prácticas de la norma ISO 27037.

1.4 Justificación

En la actualidad los delitos informáticos se han incrementado a gran escala en casi todas las áreas públicas o privadas, tanto personales como laborales, todo esto debido a la masiva digitalización de la información en estos sectores, donde los datos son parte fundamental de sus operaciones. El análisis digital forense es parte de las ciencias forenses, actividad que está a cargo de los peritos informáticos, que tratan la información a través de procedimientos, reglas y normas; estos funcionarios son especialistas en el manejo de evidencias, su aporte final es un reporte del estado técnico de los equipos y los datos, que permite a otras áreas como la legal, ver como estos datos han sido afectados para beneficios personales. (Navarro Clérigues, 2015)

Estos profesionales se encargan de la preservación, validación, identificación, análisis, interpretación, documentación y presentación de las evidencias digitales para que los eventos considerados como criminales sean reconstruido con el fin determinar si fueron modificados o borrados con propósitos de delinquir. (Navarro Clérigues, 2015)

En Ecuador las investigaciones periciales no tienen un gran desarrollo por la falta de conocimientos y poca inversión en el área por parte de los entes públicos y privados, y aun cuando se disponen de profesionales en el área, éstos no están alineados a las normativas internacionales, que se actualizan constantemente, dando como resultado la impunidad de casos en litigio por falta de habilidades y juicios idóneos necesarios para la correcta recolección y adquisición de pruebas, sumado a esto una inadecuada legislación contra delitos informáticos. (Bolaños-Burgos, 2016)

Todas las falencias periciales informáticas que actualmente se observan en los casos judiciales, donde es necesario la presencia de personal calificado, producen que la pericia informática no tenga la fortaleza suficiente, generando dictámenes con múltiples errores dejando casos en litigio impunes. (Bolaños-Burgos, 2016)

El análisis de las ciencias forenses, que comprenden un conjunto de disciplinas complementarias a la criminalística, perfecciona el repertorio de técnicas y métodos utilizados en la investigación pericial, cuyo propósito principal es el descubrimiento, esclarecimiento y comprobación de los delitos, así como la identificación de sus perpetradores y víctimas. La criminalística recurre a los conocimientos científicos para reconstruir los hechos y establecer la verdad de los sucesos. (Haque & Hossain, 2018)

2. CAPITULO II:

MARCO REFERENCIAL

2.1 Generalidades

Los sistemas computacionales y la informática fueron creados para facilitar las tareas de la humanidad, sean estos simples o complejas, como por ejemplo se mencionan los procedimientos que requieren de gran exactitud, que trabajan con probabilidad de error mínimas y con una rapidez que es imposible de igualar de forma manual. La evolución de estos sistemas no se detiene y cada día se crean más aplicaciones.

Como hitos del desarrollo de la informática se puede nombrar algunos:

- IBM mostró a la sociedad la primera computadora personal, que traía un procesador Intel 8088, el sistema operativo instalado fue DOS con el lenguaje BASIC, todo esto desarrollado por B. Gates y P. Allen.
- En 1990 se dio lugar a la World Wide Web, y que evolucionó en 1996, con mejores ventajas como: mayor rapidez, mayor capacidad de carga y envío de archivos, todo esto por el modem o microondas, en la actualidad se han mejorado los sistemas inalámbricos, se usa la fibra óptica y también satélites. (J. Sampaoli, 2018)
- Hoy en día la informática se usa en la mayoría de los procesos de humanidad, sean estos sociales, culturales, tecnológicos o estudiantiles, a tal punto que no es posible realizar ninguna actividad de la antes mencionadas sin utilizar un elemento o dispositivo electrónico relacionado con las plataformas de telecomunicaciones.

2.2 Informática

El termino informática tiene origen en Francia, del termino informatique, que está formada por la conjunción de las palabras information y automatique; en la era moderna se

destacan tres personajes que trabajaron en las bases del desarrollo de esta área, dos norteamericanos George R. Stibitz y Howard Hathaway Aiken, y un alemán, Konrad Zuse. (Costa Carballo, 1998)

En el diccionario de la Real Academia de la Lengua Española indica que la informática es un "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras" (Real Academia Española, 2021)

La informática es una disciplina que se ocupa del procesamiento de información mediante el uso de tecnología y herramientas informáticas. Se refiere al estudio de la información, su almacenamiento, procesamiento y transmisión utilizando computadoras y otros dispositivos electrónicos. La informática es una disciplina muy amplia que abarca una variedad de áreas, incluyendo el desarrollo de software, la ingeniería de sistemas, la inteligencia artificial, la seguridad informática, la robótica, la realidad virtual, entre otros.

Una definición más actualizada del término informática y acorde a nuestra realidad sería decir que es la ciencia que estudia el tratamiento automático de la información en equipos electrónicos y de computación, sistemas de almacenamiento, que basa su funcionamiento en ciencias como la física, la matemática, la electricidad, la electrónica.

La informática ha revolucionado la manera en que las personas interactúan y manejan la información en su vida cotidiana, desde la comunicación hasta el entretenimiento y el trabajo. La rápida evolución de la tecnología ha permitido el desarrollo de dispositivos cada vez más avanzados y eficientes, lo que ha llevado a una mayor interconexión entre los sistemas informáticos y el aumento de la velocidad de procesamiento.

2.2.1 Informática Forense

La informática forense es una disciplina especializada que combina conocimientos de informática, derecho y procedimientos forenses para investigar delitos informáticos y

recuperar y analizar evidencia digital (Overill & Collie, 2021). En la actualidad, la informática forense es una disciplina esencial para investigar delitos en el mundo digital.

La historia de la informática forense se remonta a los primeros días de la informática. En las décadas de 1970 y 1980, cuando los sistemas informáticos eran menos sofisticados, los delitos informáticos eran menos comunes y los métodos forenses para investigarlos eran muy rudimentarios. La mayoría de los investigadores de delitos informáticos eran policías o abogados con conocimientos informáticos básicos, que recopilaban la evidencia digital de manera manual, utilizando copias impresas o fotografías de las pantallas del ordenador (Vincze, 2016)

A medida que los sistemas informáticos se volvieron más avanzados y la cantidad de información digital disponible creció exponencialmente, se hizo evidente que se necesitaba una disciplina especializada para investigar delitos informáticos. En la década de 1990, surgieron las primeras herramientas de software especializadas para la informática forense, como EnCase y FTK, que permitían a los investigadores recuperar y analizar la información digital de manera más rápida y eficiente (Casey, 2019)

Con la creciente complejidad de la tecnología de la información, la informática forense se ha vuelto cada vez más importante. Los delitos informáticos, como la piratería informática, el robo de identidad y la pornografía infantil, son cada vez más comunes y sofisticados. La informática forense se ha extendido a otras áreas, como la ciberseguridad, la gestión de riesgos y la privacidad de los datos.

La informática forense se ha vuelto cada vez más importante en el mundo digital de hoy en día, y se espera que siga evolucionando a medida que surjan nuevas tecnologías y amenazas informáticas. Los expertos en informática forense trabajan con una amplia variedad de tecnologías, desde dispositivos móviles hasta redes informáticas complejas. Utilizan herramientas de software especializadas para examinar y analizar dispositivos, sistemas y redes informáticas para recuperar y analizar datos importantes. También trabajan

estrechamente con abogados y fuerzas del orden público para investigar y procesar a los responsables de delitos informáticos.

En resumen, la informática forense es una disciplina esencial para investigar delitos en el mundo digital (Casey, 2019). Desde sus primeros días, ha evolucionado para abarcar una amplia gama de delitos informáticos, y se espera que siga evolucionando a medida que surjan nuevas tecnologías y amenazas informáticas. La informática forense es una disciplina especializada que requiere conocimientos informáticos avanzados, así como una comprensión de los procedimientos legales y forenses. Es una disciplina en constante evolución y esencial para la seguridad y la protección en el mundo digital de hoy.

2.3 Delito Informático

El delito informático es cualquier actividad ilegal o ilícita que se lleva a cabo a través de medios informáticos o en línea. Esto puede incluir una amplia gama de actividades, desde el robo de información personal hasta el uso indebido de sistemas informáticos y la distribución de virus informáticos. (Vaca, 2017)

El autor ecuatoriano Pino (2012) cita en su obra otra definición de delito informático, “todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio”, De aquí que los delitos de acuerdo a los propósitos que persiguen se clasifican en :

- **Propósito de investigación de seguridad** El delito informático es cualquier acto malicioso a un computador como objeto, sujeto, instrumento o símbolo donde el perjudicado pudo haber perdido información y el criminal obtuvo una ganancia. (Pino, 2012)

- **Propósito de investigación y acusación** El delito informático es cualquier acto fuera de lo legal que ha ocurrido, se ha investigado o acusado que exige para su resolución conocimientos de tecnología. (Pino, 2012)
- **Propósito legal** El delito informático es un acto que está especificado en la ley y aplica la norma de la jurisdicción. (Pino, 2012)
- **Otros propósitos** El abuso informático, es cualquier delito que requiere necesariamente un equipo de cómputo. (Pino, 2012)

2.3.1 Tipos De Delitos Informáticos

El acceso no autorizado Es el acceso sin derecho a un sistema o a una red, donde son violadas las medidas de seguridad, llega también a ser conocido como hacking. (González et al., 2018)

El daño a los datos o programas informáticos es un delito informático que implica la destrucción, alteración, daño o eliminación de datos o programas informáticos sin el consentimiento del propietario o usuario legítimo de esos datos o programas. (González et al., 2018)

El sabotaje informático es un delito informático que implica la interrupción o daño malintencionado de sistemas informáticos, redes o dispositivos. El objetivo del sabotaje informático es causar daños a una organización, empresa o individuo, ya sea con fines políticos, ideológicos o de otro tipo. (González et al., 2018)

La interceptación no autorizada es un delito informático que implica la obtención y acceso no autorizados a datos privados y confidenciales de un individuo o una organización a través de redes de comunicación, como internet o el correo electrónico. (González et al., 2018)

El espionaje informático El espionaje informático es un delito informático que implica la obtención y acceso no autorizados a información confidencial de individuos, empresas u

organizaciones con fines de espionaje, robo de secretos comerciales o políticos, o para obtener ventaja competitiva. (González et al., 2018)

Fraude telefónico: Este delito implica el uso fraudulento de servicios de telefonía, como la clonación de tarjetas SIM o el uso ilegal de líneas telefónicas para hacer llamadas.

Spamming: Este delito consiste en enviar mensajes no solicitados en masa a través de correos electrónicos, mensajes de texto o mensajes instantáneos con fines publicitarios o fraudulentos.

Phishing: Este delito se refiere a la creación de sitios web o correos electrónicos falsos que imitan la apariencia de sitios web o empresas legítimas para engañar a los usuarios y obtener información personal o financiera.

Suplantación de identidad: Este delito implica el uso de información personal de otra persona, como su nombre o número de identificación, para cometer fraudes o delitos.

Robo de información: Este delito se refiere a la obtención no autorizada de información personal, financiera o confidencial a través de la interceptación de comunicaciones o la explotación de vulnerabilidades en sistemas de información.

2.4 El Perito en investigación

Un perito es un experto en una determinada materia o campo, que es designado o acepta proporcionar un testimonio o informe experto en un caso legal o en una investigación. Un perito puede ser un profesional con una educación y experiencia específicas, como un médico forense, un perito contable o un perito informático.

El perito es designado por un juez o por una parte involucrada en un caso legal para proporcionar testimonio experto sobre una materia específica en la que tienen conocimientos especializados. El perito puede ser llamado a presentar testimonio en un juicio o en una audiencia, o puede ser solicitado para proporcionar un informe escrito.

En la investigación criminal, un perito puede ser llamado a examinar pruebas físicas o a analizar datos para ayudar a las autoridades a determinar cómo ocurrió un delito. Los peritos también pueden ser consultados en casos civiles para ayudar a determinar la responsabilidad en un accidente o para evaluar los daños sufridos.

En resumen, el perito es un experto en un área específica, llamado a proporcionar testimonio o informe experto en un juicio o investigación legal, y su objetivo es ayudar al juez o al jurado a tomar una decisión informada y justa.

2.4.1 Tipos de peritos

Subijana & Echeburúa, (2021) , indican que existen diferentes tipos de peritos, dependiendo del campo o materia en la que tienen experiencia y conocimientos especializados. Algunos ejemplos de tipos de peritos incluyen:

- **Médico forense:** un perito médico que es especialista en medicina legal y que puede proporcionar testimonio o informes sobre lesiones o causas de muerte.
- **Perito contable:** un perito que es especialista en contabilidad y finanzas y que puede proporcionar testimonio o informes sobre asuntos financieros o contables.
- **Perito informático:** un perito que es especialista en tecnología de la información y que puede proporcionar testimonio o informes sobre problemas informáticos.
- **Perito químico:** un perito que es especialista en química y que puede proporcionar testimonio o informes sobre problemas químicos.
- **Perito en ingeniería:** un perito que es especialista en ingeniería y que puede proporcionar testimonio o informes sobre problemas relacionados con la ingeniería.
- **Perito en psicología**: un perito que es especialista en psicología y que puede proporcionar testimonio o informes sobre problemas relacionados con la salud mental o el comportamiento humano.
- **Perito en balística:** un perito especialista en el estudio de los proyectiles y el arma de fuego.

- **Perito en huellas dactilares:** un perito especialista en el estudio de las huellas dactilares y su relación con la identificación de las personas.

Estos son solo algunos ejemplos de los diferentes tipos de peritos disponibles, hay muchos más campos y especialidades.

2.5 Perito informático

Un perito informático es un experto en tecnología de la información que es designado o acepta proporcionar un testimonio o informe experto en un caso legal o en una investigación relacionada con problemas informáticos. El autor Poma (2019)indica que el perito informático puede ser un profesional con una educación y experiencia específicas en campos como la informática forense, la seguridad de la información o la recuperación de datos.

Un perito informático puede ser llamado a investigar una variedad de problemas informáticos, como:

- Fraude informático
- Robo de información
- Ataques cibernéticos
- Interrupciones de servicio en sistemas informáticos
- Discrepancias en registros de sistemas informáticos

El perito informático utiliza herramientas y técnicas especializadas para analizar los datos de un sistema informático y recopilar evidencia para ayudar en una investigación. Esto puede incluir el análisis de registros de sistemas, el análisis de tráfico de red, y la recuperación de datos.(Veber et al., 2015)

El perito informático también puede ser responsable de proporcionar testimonio experto en juicios legales relacionados con problemas informáticos. Puede ser consultado para

proporcionar asesoramiento y ayudar a las empresas a desarrollar políticas y procedimientos para prevenir problemas informáticos.(Choi et al., 2019)

En resumen, el perito informático es un experto en tecnología de la información, llamado a proporcionar testimonio o informe experto en un juicio o investigación legal relacionada con problemas informáticos, y su objetivo es ayudar al juez o al jurado a tomar una decisión informada y justa. En resumen, el personal calificado como perito informático es un profesional definido por la Ley, que mediante sus estudios y la experiencia adquiere los conocimientos especializados en área tecnológica, lo que le faculta para realizar asesoría judicial.

2.5.1 Funciones del perito informático

Las funciones de un perito informático pueden variar dependiendo de la situación específica en la que se utiliza su experiencia y conocimientos, Poma, (2019) explica que algunas de sus funciones comunes incluyen:

- **Análisis de incidentes:** el perito informático puede ser llamado a investigar y analizar incidentes informáticos, como ataques cibernéticos, robos de información o interrupciones de servicio.
- **Recuperación de datos:** el perito informático puede utilizar herramientas y técnicas especializadas para recuperar datos de sistemas informáticos dañados o comprometidos.
- **Análisis forense:** el perito informático puede utilizar técnicas forenses para recopilar, analizar y presentar evidencia en un juicio o investigación legal.
- **Testimonio experto:** el perito informático puede proporcionar testimonio experto en un juicio o audiencia, explicando su análisis e interpretación de la evidencia informática.
- **Asesoramiento:** el perito informático puede proporcionar asesoramiento a las empresas o a las autoridades sobre cómo prevenir o mitigar problemas informáticos.

- **Evaluación de seguridad:** El perito informático puede evaluar la seguridad de los sistemas informáticos y su capacidad para proteger los datos y prevenir incidentes.
- **Investigación:** El perito informático puede investigar la causa de un incidente o problema informático.
- **Evaluación de daños:** El perito informático puede evaluar el daño causado por un incidente o problema informático y proporcionar informes sobre los costos para reparar o recuperar los sistemas informáticos afectados.

Se puede inferir que el perito informático es un experto en tecnología de la información que puede proporcionar asesoramiento, investigar incidentes, recuperar datos, proporcionar testimonio experto, y evaluar la seguridad y el daño causado por problemas informáticos.

2.5.2 Tipos de peritos informáticos

Existen varios tipos de peritos informáticos, cada uno con un enfoque específico en una materia o campo relacionado con la tecnología de la información. Algunos ejemplos de los diferentes tipos de peritos informáticos incluyen:

Perito de Oficio Son los profesionales que ha sido seleccionados por el juez de un listado de funcionarios públicos. (J. Sampaoli, 2018)

Perito de Parte Son los profesionales propuestos por una de las partes y se desenvuelven en cualquier fuero. En ocasiones realizan dictámenes oficiales en conjunto con los peritos oficiales. Su idoneidad debe ser acreditada con un título habilitante y realizar el respectivo juramento para aceptar el cargo. Los honorarios son pagados por la parte que propuso (J. Sampaoli, 2018). Aquí es frecuente encontrar profesionales que verifican el contenido, lo analizan críticamente respecto a otros peritajes:

- **Contraperitaje informático** Son profesionales encargados de realizar un análisis crítico de las conclusiones de otro informe pericial, que por lo general

es presentado por la contraparte del litigio y si existiesen errores rebatir dicho documento. (García, 2015)

- **Metaperitaje informático** Son profesionales que analizan otros peritajes informáticos, pero desde el punto de vista pericial, es decir, se realiza un peritaje sobre otro peritaje informático. El objetivo principal es demostrar la falta de exigencia técnica o metodológico del peritaje realizado para poner en duda las conclusiones del documento presentado y que sea invalidado como prueba. (García, 2015)

Según la función que es llevada a cabo por los peritos informáticos, se puede derivar en:

Perito informático forense: Un perito que se especializa en la recuperación de datos y la investigación de incidentes informáticos con fines legales.

Perito informático de seguridad: Un perito que se especializa en la seguridad informática y puede proporcionar asesoramiento y soluciones para prevenir ataques cibernéticos y proteger la información.

Perito informático en recuperación de datos: Un perito que se especializa en la recuperación de datos de sistemas informáticos dañados o comprometidos.

Perito informático de redes: Un perito que se especializa en la configuración y el mantenimiento de redes informáticas.

Perito informático en inteligencia artificial: Un perito que se especializa en la aplicación de la inteligencia artificial en la tecnología de la información y la automatización de procesos.

Perito informático en sistemas: Un perito que se especializa en la configuración, el mantenimiento y el análisis de sistemas informáticos.

2.5.3 Peritaje Tecnológico de Gestión

El peritaje tecnológico de gestión es una herramienta que se utiliza para evaluar la capacidad y eficiencia de los sistemas de información en una organización y determinar si se están utilizando de manera adecuada para lograr los objetivos empresariales.

Según Marín et al., (2021) tipo de peritaje puede abarcar diferentes áreas, como la seguridad de la información, la gestión de proyectos tecnológicos, el análisis de datos, la gestión de la infraestructura tecnológica, entre otras.

El objetivo principal del peritaje tecnológico de gestión es asegurar que los sistemas de información sean efectivos, eficientes y seguros, y que estén alineados con los objetivos estratégicos de la organización.

> Son profesionales cuya función es la recolección de evidencias vinculadas con el cumplimiento de responsabilidades contractuales que asumen las partes las partes en relación a niveles de calidad o de servicio. Su área de trabajo es la gestión, explotación de proyectos o de servicios, consultorías o auditorias informáticas.

2.5.4 Peritaje Tecnológico de Mediación

García, (2015) explica que el peritaje tecnológico de mediación es un proceso mediante el cual un perito experto en tecnología de la información y en resolución de conflictos ayuda a dos o más partes a llegar a un acuerdo en un caso relacionado con temas tecnológicos.

En este tipo de peritaje, el perito actúa como un mediador neutral y ayuda a las partes a comprender los aspectos técnicos del caso, identificar los puntos de acuerdo y desacuerdo, y a encontrar soluciones que satisfagan los intereses de ambas partes.

El peritaje tecnológico de mediación puede ser útil en una amplia gama de situaciones, como en conflictos de propiedad intelectual, disputas en el ámbito de la tecnología, litigios relacionados con el comercio electrónico, entre otros.

Para llevar a cabo un peritaje tecnológico de mediación, el perito debe tener conocimientos técnicos sólidos y habilidades de comunicación efectiva y resolución de conflictos. Además, debe ser imparcial y objetivo, y no tener ningún interés personal en el resultado del caso.

2.5.5 Tasación Tecnológica

La tasación tecnológica es un proceso mediante el cual se determina el valor de un activo tecnológico o de un conjunto de activos tecnológicos. Estos activos pueden incluir patentes, marcas comerciales, software, hardware, procesos, sistemas de información, entre otros.

Como indica (Cabero et al., 2020) la tasación tecnológica es importante en diferentes contextos, como en la evaluación de una empresa para su venta o fusión, la obtención de financiamiento, la determinación del valor de una propiedad intelectual, la evaluación de la rentabilidad de un proyecto, entre otros.

Para llevar a cabo una tasación tecnológica, se requiere de un perito con amplios conocimientos y experiencia en tecnología de la información y en valoración de activos. El perito utiliza diferentes métodos de valoración, como el enfoque de costo, el enfoque de mercado y el enfoque de ingresos, para determinar el valor de los activos tecnológicos.

2.5.6 Consultor técnico

Un consultor técnico es un experto en tecnología que ofrece asesoramiento y soluciones técnicas a empresas y organizaciones para ayudarles a mejorar su rendimiento y cumplir con sus objetivos de negocio.

Los consultores técnicos trabajan en diferentes áreas de la tecnología, como infraestructura de TI, desarrollo de software, seguridad informática, análisis de datos, inteligencia artificial, entre otras.

El rol del consultor técnico es analizar los problemas o desafíos que enfrenta una empresa y encontrar soluciones prácticas y efectivas utilizando su experiencia y conocimientos técnicos. También pueden proporcionar asesoramiento en la implementación de nuevas tecnologías o sistemas, y en la optimización de los procesos y sistemas existentes (J. Sampaoli, 2018).

2.6 Principios del Peritaje

(Vincze, 2016), indica que los principios del peritaje son los fundamentos y principios éticos que guían la conducta y el comportamiento de un perito en su trabajo. Algunos de los principios comunes del peritaje incluyen:

Objetividad: El perito debe ser imparcial e independiente en su análisis e investigación, evitando cualquier tipo de prejuicio o sesgo.

Competencia: El perito debe tener la capacitación, experiencia y conocimientos necesarios para llevar a cabo su trabajo de manera profesional y confiable.

Confidencialidad: El perito debe proteger la confidencialidad de la información a la que tiene acceso en el curso de su trabajo.

Responsabilidad: El perito debe ser responsable de sus acciones y decisiones, y debe responder por cualquier negligencia o mal desempeño en su trabajo.

Integridad: El perito debe actuar con integridad y ética en todas sus acciones, evitando cualquier tipo de conducta deshonesta o poco ética.

Transparencia: El perito debe ser transparente en su metodología y presentación de informes, y debe poder justificar y explicar sus conclusiones.

Responsabilidad social: El perito debe tener en cuenta el impacto social y ambiental de sus acciones y decisiones, y debe actuar de manera responsable y ética.

Estos principios son fundamentales para garantizar la confiabilidad y la validez de los informes y conclusiones del perito, y para proteger la confianza del público en el trabajo de los peritos.

2.7 El Peritaje Vs El Peritaje Forense

Pizarro, (2018), menciona que ambos términos se refieren a la evaluación técnica de un objeto o proceso por parte de un experto en la materia, pero hay una diferencia importante entre ambos y es:

El peritaje es una evaluación técnica realizada por un experto en la materia con el objetivo de proporcionar una opinión especializada en un caso particular. Por ejemplo, un perito puede ser llamado para evaluar el valor de mercado de un bien o para evaluar la calidad de un trabajo realizado por un contratista.

Por otro lado, el peritaje forense es una evaluación técnica realizada por un experto en la materia en el ámbito judicial, con el objetivo de recopilar, analizar y presentar pruebas digitales, electrónicas o informáticas que puedan ser utilizadas en un proceso judicial. El peritaje forense se enfoca en la recolección y el análisis de pruebas para su presentación en el juicio, y se rige por procedimientos específicos para garantizar la validez y la confiabilidad de las pruebas(Vincze, 2016).

En resumen, mientras que el peritaje se enfoca en proporcionar una opinión especializada en un caso particular, el peritaje forense se enfoca en la recopilación y el

análisis de pruebas digitales, electrónicas o informáticas en el ámbito judicial, con el objetivo de proporcionar pruebas que puedan ser utilizadas en un proceso legal.

2.8 Principios del Peritaje Informático en telecomunicaciones

El peritaje informático en telecomunicaciones implica la aplicación de los principios generales del peritaje informático a situaciones específicas relacionadas con las tecnologías de las comunicaciones. Sampaoli & Bender, (2018) mencionan que algunos de los principios clave del peritaje informático en telecomunicaciones son:

Conocimiento técnico: El perito debe tener un conocimiento técnico sólido en las tecnologías de las comunicaciones, incluyendo los sistemas de red, los protocolos de comunicación, la telefonía, el cableado y otros aspectos relacionados.

Imparcialidad: El perito debe ser imparcial e independiente, sin tener un interés personal en el resultado del caso. Debe evaluar objetivamente la evidencia y presentar conclusiones justas y precisas.

Precisión y rigor: El perito debe llevar a cabo un análisis riguroso y preciso de la evidencia y los datos, utilizando herramientas y técnicas adecuadas para garantizar la integridad y la exactitud de los resultados.

Informe claro y comprensible: El perito debe presentar sus conclusiones y opiniones en un informe claro y fácil de entender, que explique los datos y la evidencia utilizados, el razonamiento detrás de las conclusiones, y las implicaciones para el caso.

Confidencialidad: El perito debe mantener la confidencialidad de la información y los datos utilizados en el análisis, asegurando que solo sean accesibles por las partes autorizadas.

2.9 Normas Usadas en Peritaje Informático y Telecomunicaciones

En su análisis Chávez (2020) indica que en el peritaje informático, se emplean varias normas técnicas que proporcionan un marco para la evaluación de sistemas, equipos y aplicaciones informáticas. A continuación, se detallan algunas de las normas técnicas más comunes que se emplean en el peritaje informático:

ISO/IEC 27001: Esta norma establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Es una de las normas más importantes en el peritaje informático, ya que se enfoca en la seguridad de la información en la gestión de sistemas y equipos informáticos. La norma establece los requisitos para la planificación, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del SGSI.

ISO/IEC 27002: Esta norma proporciona directrices para la implementación de controles de seguridad de la información. La norma se enfoca en los aspectos técnicos, físicos y administrativos de la seguridad de la información. La norma establece un conjunto de controles de seguridad de la información que pueden ser implementados en una organización para proteger la información confidencial(Internacional Organization for Standardization, 2020).

ISO/IEC 27037:2012 establece directrices para la identificación, recopilación, adquisición y preservación de evidencia digital en el contexto de la investigación y el análisis forense. Esta norma es relevante para el peritaje informático de telecomunicaciones, ya que proporciona un marco para la identificación y recolección de evidencia digital en casos relacionados con sistemas y equipos de telecomunicaciones(Internacional Organization for Standardization, 2018).

ISO/IEC 12207: Esta norma establece los requisitos para el ciclo de vida del software. La norma proporciona un marco para la gestión del desarrollo, la operación y el mantenimiento del software. La norma se enfoca en los procesos de software, los planes de

gestión del proyecto, los requisitos del software, el diseño y la implementación, la verificación y validación, la gestión de la configuración y la gestión del mantenimiento.

ISO/IEC 15504: Esta norma establece un marco para la evaluación de procesos de software. La norma proporciona una metodología para evaluar la capacidad de los procesos de software y mejorarlos. La norma se enfoca en la gestión de procesos, la ingeniería de procesos, el soporte de procesos y la mejora continua.

IEEE 829: Esta norma establece los requisitos para la documentación de pruebas de software. La norma proporciona un conjunto de directrices para la documentación de pruebas de software, incluyendo la planificación de pruebas, la especificación de requisitos de pruebas, la documentación de diseño de pruebas, la documentación de procedimientos de pruebas y la documentación de resultados de pruebas.

En resumen, en el peritaje informático se emplean varias normas técnicas que proporcionan un marco para la evaluación de sistemas, equipos y aplicaciones informáticas. Las normas técnicas establecen los requisitos para la gestión de la seguridad de la información, el ciclo de vida del software, la evaluación de procesos de software y la documentación de pruebas de software.

2.10 Norma ISO 27037

La norma ISO 27037:2022 como explica International Organization for Standardization, (2022) es una norma internacional para la gestión de incidentes de seguridad cibernética. Esta norma establece los requisitos para la planificación, preparación, detección, respuesta y recuperación de incidentes de seguridad cibernética. La implementación de esta norma ayudará a las organizaciones a establecer una estructura sólida para la gestión de incidentes de seguridad cibernética, aumentando su capacidad para detectar, responder y recuperarse de incidentes de seguridad cibernética de manera eficaz.

La norma ISO 27037 se basa en el ciclo de vida de incidentes, que incluye la planificación, la preparación, la detección, la respuesta y la recuperación. La planificación es esencial para establecer una estructura sólida para la gestión de incidentes de seguridad cibernética. Esto incluye establecer roles y responsabilidades, establecer procedimientos y establecer medidas para medir el rendimiento.

La preparación es esencial para estar listo para responder a incidentes de seguridad cibernética. Esto incluye establecer controles de seguridad cibernética, establecer un plan de contingencia y establecer un plan de recuperación. La detección de incidentes de seguridad cibernética es esencial para detectar incidentes de seguridad cibernética y responder rápidamente. Esto incluye establecer un sistema de detección de incidentes de seguridad cibernética y establecer procedimientos para responder a incidentes de seguridad cibernética(Elaine, 2022).

La respuesta a incidentes de seguridad cibernética es esencial para mitigar el impacto de incidentes de seguridad cibernética. Esto incluye establecer procedimientos para responder a incidentes de seguridad cibernética y establecer medidas para mitigar el impacto de incidentes de seguridad cibernética.

La recuperación de incidentes de seguridad cibernética es esencial para recuperarse de incidentes de seguridad cibernética. Esto incluye establecer procedimientos para recuperarse de incidentes de seguridad cibernética y establecer medidas para prevenir incidentes de seguridad cibernética en el futuro(Anampa et al., 2021).

En conclusión, la norma ISO 27037 es una norma importante para la gestión de incidentes de seguridad cibernética, la documentación proporcionada por la norma ISO se distribuye en las siguientes secciones:

Tabla 1:

Secciones de la normativa ISO 27037.

1. Introducción	**Visión general y ámbito de aplicación**
2. Normas de referencia	Normas relacionadas con la seguridad de la información
3. Términos y definiciones	Definiciones de términos clave utilizados en la norma
4. Principios de la auditoría	Principios que deben guiar el proceso de auditoría
5. Gestión del programa de auditoría	Planificación, programación y realización de auditorías
6. Realización de la auditoría	Selección del equipo auditor, recopilación de información, evaluación de la conformidad
7. Competencia y evaluación del auditor	Requisitos para la competencia y la evaluación del desempeño de los auditores
8. Informes de auditoría	Requisitos para la elaboración de informes de auditoría

9. Seguimiento de la auditoría	Requisitos para el seguimiento de las recomendaciones y las acciones correctivas derivadas de la auditoría
10. Gestión de los registros de auditoría	Requisitos para la gestión de los registros de auditoría

Nota: En la tabla 1 se puede apreciar como la normativa distribuye el acceso a información de esta, fuente (Elaine, 2022)

2.10.1 SO/IEC 27037:2012 peritaje según la tipología de dispositivos

Rosero (2019), indica que esta Norma Internacional proporciona pautas para actividades específicas en el manejo de evidencia digital. Las actividades incluyen identificación, recolección, adquisición y preservación de evidencia digital que pueda tener valor probatorio. Ofrece orientación a individuos en situaciones comunes encontradas durante el proceso de manejo y ayuda a las organizaciones en procedimientos disciplinarios y en facilitar el intercambio de posibles pruebas digitales entre jurisdicciones.

Esta Norma Internacional proporciona orientación para dispositivos como :

- Medios de almacenamiento digital utilizados en computadoras estándar, como discos duros, disquetes, discos ópticos y magneto-ópticos, dispositivos de datos con funciones similares.
- Teléfonos móviles, Asistentes Digitales Personales (PDA), Dispositivos Electrónicos Personales (PED), tarjetas de memoria.
- Sistemas de navegación móvil.
- Cámaras digitales de fotos y video (incluyendo CCTV).
- Computadoras estándar con conexiones de red.

- Redes basadas en TCP/IP y otros protocolos digitales.
- Dispositivos con funciones similares a las anteriores.

Las circunstancias incluyen los dispositivos mencionados anteriormente que existen en diversas formas. Por ejemplo, un sistema automotriz puede incluir un sistema de navegación móvil, almacenamiento de datos y sistemas de sensores.

La norma ISO/IEC 27037:2012 no proporciona una guía específica para el peritaje según la tipología de dispositivos, sino que establece un proceso detallado para la identificación, recopilación, adquisición y preservación de evidencia digital en general (Montes De Oca, 2021).

Dicho esto, los peritos informáticos suelen seguir un proceso general para llevar a cabo la identificación, recolección y adquisición de evidencia digital según la tipología de dispositivos. Este proceso general puede variar según el caso y las circunstancias específicas, pero podría incluir los siguientes pasos:

Identificación de la fuente de la evidencia: El perito debe identificar el dispositivo o los dispositivos relevantes para el caso en cuestión, ya sea una computadora, un servidor, un teléfono móvil, un enrutador, entre otros.

Evaluación de la calidad de la evidencia: El perito debe evaluar la calidad de la evidencia disponible en el dispositivo, asegurándose de que la información sea relevante para el caso y no haya sido alterada o eliminada.

Recolección y adquisición de la evidencia: El perito debe recolectar y adquirir la evidencia digital de manera forense, utilizando técnicas apropiadas para evitar alteraciones o eliminaciones de la información.

Preservación de la integridad de la evidencia: El perito debe preservar la integridad de la evidencia a lo largo del proceso de recolección y adquisición, asegurándose de que no se pierda, altere o modifique la información.

Documentación de la evidencia: El perito debe documentar cuidadosamente el proceso de recolección y adquisición de la evidencia, incluyendo detalles como la fecha y hora de la recolección, los dispositivos y los métodos utilizados.

Presentación de informes y conclusiones basados en la evidencia recolectada: El perito debe presentar informes y conclusiones basados en la evidencia recolectada, utilizando técnicas de análisis y evaluación forense para determinar la autenticidad y relevancia de la información.

Es importante destacar que cada caso es único y puede requerir diferentes pasos y técnicas según la tipología de dispositivos involucrados y las circunstancias específicas. Los peritos informáticos deben estar actualizados y capacitados en las últimas técnicas y tecnologías para llevar a cabo una investigación efectiva y precisa.

2.11 Marco Legal

En Ecuador, el marco legal del peritaje informático está regulado por varias leyes y normas, entre ellas:

1. La Constitución de la República del Ecuador: establece el derecho a la privacidad y la protección de datos personales, así como el derecho a un juicio justo y al debido proceso legal.
2. La Ley Orgánica de la Policía Nacional: regula las funciones y responsabilidades de la Policía Nacional en la investigación de delitos informáticos.
3. La Ley de Seguridad Cibernética: establece la responsabilidad del Estado en la protección de la seguridad cibernética del país y la creación de un sistema nacional de seguridad cibernética.
4. La Ley de Protección de Datos Personales: regula la recopilación, almacenamiento, uso y protección de datos personales en el país.

5. La Ley de Delitos Informáticos: establece las sanciones y medidas penales para los delitos informáticos, como el robo de información, el acceso no autorizado a sistemas informáticos y la difamación en línea.

A continuación, se mencionará a detalle cada una de las leyes y normativas legales referentes a peritaje informático existentes en el país

2.11.1 Constitución de la República del Ecuador

En en la Constitución de la República del Ecuador, elaborada por Asamblea Nacional del Ecuador (2008) se menciona en el artículo 66 sobre los derechos de libertad en el numeral número 19 lo siguiente:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (p. 29)

El artículo anterior ampara a la Dirección Nacional de Registros Públicos (DINARP), en la propuesta de una ley de Protección de Datos personales que es necesaria en la actualidad para habilitar la confianza digital. Esta ley busca proteger a las personas titulares de los datos con la intención de que ellos puedan decidir a quién brindar o no su información personal siendo que confían en los proveedores de servicios digitales. Entre otros la Dirección Nacional de Registros Públicos, (2021), menciona que los sistemas de servicios que son parte de la Dirección Nacional de Registros Públicos (SINARDAP) que están sujetos a la normativa en materia de protección de datos personales son:

- Ficha Simplificada
- Ficha de Registro Único del Ciudadano
- Ficha de Información Ciudadana

- Infodigital
- Dato Seguro
- Visualizadores a medida
- Consumos masivos de información
- Paquetes de consumo preestablecidos
- Interoperabilidad
- Sistema de Agendamiento de Turnos
- Sistema de Notificaciones Electrónicas
- Sistema de Actos Notariales y Registrales
- Habilitación o entrega del Sistema Nacional de Registro de la Propiedad
- Servicios registrales mercantiles
- Autorizaciones excepcionales; y,
- Los demás que determine la Dirección Nacional de Registro de Datos Públicos.

2.11.2 Código integral penal COIP

Dentro del COIP se encuentran tipificados los delitos informáticos con pena de prisión en Ecuador son los siguientes:

- Pornografía infantil (art. 103) – 13 a 16 años de prisión.
- Violación del derecho a la intimidad (art. 178) – de 1 a 3 años de prisión.
- Revelación ilegal de información de bases de datos (art. 229) – de 1 a 3 años de prisión.
- Interceptación de comunicaciones (art. 476) – de 3 a 5 años de prisión.
- Ataque a la integridad de sistemas informáticos (art. 232) – de 3 a 5 años de prisión.
- Delitos contra la información pública reservada legalmente (art. 233) – de 3 a 5 años de prisión.
- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones (art. 234) – de 3 a 5 años de prisión.

- Pharming y Phishing – de 3 a 5 años de prisión.
- Fraude informático – de 3 a 5 años de prisión.

3. CAPITULO III:

MARCO METODOLÓGICO

Como se trata de una metodología de buenas prácticas para peritos informáticos en telecomunicaciones, lo más adecuado es desarrollar el proyecto con un enfoque cualitativo. De esta manera, se puede recopilar y analizar información tanto de fuentes documentales como de la experiencia de expertos en el campo de las telecomunicaciones, y de esta forma asegurarse de que la metodología tenga una base sólida y esté en línea con las mejores prácticas actuales. Además, este enfoque permitiría validar y ajustar la metodología a través de la retroalimentación de expertos en el campo, lo que garantiza su efectividad y utilidad práctica.

3.1 Descripción del área de estudio

Ecuador, oficialmente conocido como la República del Ecuador, es un país ubicado en la costa del Pacífico de Sudamérica. Limita al norte con Colombia, al este y sur con Perú, y al oeste con el Océano Pacífico. Su territorio se divide en cuatro regiones geográficas principales: la costa, la sierra, la región amazónica y las Islas Galápagos. La capital del país es Quito y su ciudad más poblada es Guayaquil. Con una población estimada de más de 17 millones de habitantes, Ecuador es conocido por su diversidad cultural, paisajes impresionantes, recursos naturales y una economía en desarrollo. Además, ha sido objeto de varios estudios e investigaciones en diferentes áreas, incluyendo la economía, la educación, la salud, la política y la seguridad ciudadana. En este sentido, Ecuador es un país de gran interés para la comunidad académica y científica internacional, así como para las organizaciones gubernamentales y no gubernamentales que buscan mejorar el bienestar y la calidad de vida de su población.

Figura 5: Área de estudio.

Nota: en la figura 5 se puede observar el área de estudio de la presente investigación, fuente (Google Maps, 2022)

Muestra

Para el presente proyecto se considera un grupo de 8 expertos peritos forenses de instituciones públicas y privadas en Ecuador, la investigación con este grupo de estudio se aplicó un enfoque cualitativo para obtener información detallada y profunda sobre las buenas prácticas de los peritos informáticos en telecomunicaciones. En este enfoque, se utilizó técnicas como la encuesta y la observación participante para obtener información sobre las experiencias y conocimientos de los peritos informáticos en el campo de las telecomunicaciones.

Además, se realizó un análisis de documentos y registros técnicos para complementar la información obtenida en la encuesta y observaciones. La selección de los 8 peritos informáticos para el estudio se realizaría mediante un muestreo no probabilístico intencional,

seleccionando aquellos que tengan mayor experiencia y conocimiento en el área de las telecomunicaciones y que representen diferentes instituciones públicas y privadas en Ecuador.

En cuanto a la metodología de la guía de buenas prácticas, se aplica un enfoque participativo e inclusivo, involucrando a los 8 peritos informáticos seleccionados y a otros expertos en el área, para identificar y definir las buenas prácticas a incluir en la guía. Se utilizó técnicas de grupo nominal y el método Delphi para recopilar y validar la información obtenida de los participantes.

3.2 Enfoque de la Investigación

Hernández & Collado, (2018), exponen que en un enfoque cualitativo, se busca comprender y describir el fenómeno de estudio desde la perspectiva de los participantes involucrados y su contexto, a través de la recolección y análisis de datos no numéricos. Se busca profundizar en las experiencias, percepciones y significados que los individuos tienen respecto al fenómeno en cuestión, para poder interpretarlos y comprenderlos en su complejidad. En este sentido, se utiliza una variedad de técnicas de recolección de datos, como la observación, entrevistas, grupos focales, análisis documental y otros, para obtener información rica y detallada. La investigación cualitativa busca generar teorías y explicaciones que se basan en los datos recopilados, y su objetivo principal es la comprensión y la interpretación del fenómeno estudiado, en lugar de medir o cuantificar las variables involucradas.

3.3 Tipos de investigación

3.3.1 De campo

Según Ishtiaq, (2019) la investigación de campo es un método de recolección de datos que implica la observación directa y la interacción con los sujetos en su entorno natural. Este enfoque se utiliza comúnmente en estudios cualitativos y se basa en la idea de que los

fenómenos sociales y humanos sólo pueden ser comprendidos plenamente a través de la observación detallada de su comportamiento y las interacciones que ocurren en su contexto natural. Los investigadores que utilizan la investigación de campo deben estar preparados para sumergirse en la cultura y el entorno del sujeto de estudio y ser capaces de registrar y analizar cuidadosamente los datos obtenidos. Además, se recomienda que los investigadores sigan los protocolos éticos adecuados para proteger los derechos de los sujetos y garantizar la confidencialidad de los datos recolectados.

3.3.2 Documental

Según Hernández y Collado, (2018) , la investigación documental es un método de recolección de datos que se basa en el análisis y la interpretación de documentos y registros escritos, tales como archivos, publicaciones, informes y otros medios escritos. Este enfoque se utiliza comúnmente en estudios cualitativos y cuantitativos, y es especialmente útil para examinar eventos históricos o estudiar cambios y tendencias a lo largo del tiempo.

Los investigadores que utilizan la investigación documental deben ser capaces de identificar y acceder a las fuentes de información relevantes, y estar preparados para analizar y sintetizar los datos obtenidos de manera sistemática y rigurosa. Además, se recomienda que los investigadores sigan los protocolos éticos adecuados para garantizar la privacidad y confidencialidad de los datos recolectados.

3.3.3 Descriptiva

Según Toscano, (2018) la investigación descriptiva es un método de recolección de datos que busca describir, analizar y presentar la información de manera objetiva y sistemática, sin buscar explicaciones causales o de relación entre variables. Este enfoque se utiliza comúnmente en estudios cuantitativos y es útil para obtener información detallada sobre características, tendencias y patrones en una población o grupo de estudio. Los investigadores que utilizan la investigación descriptiva deben ser capaces de definir claramente el problema o la cuestión a investigar, y seleccionar las muestras y las

herramientas de recolección de datos apropiadas para obtener información relevante y confiable. Además, se recomienda que los investigadores sigan los protocolos éticos adecuados para proteger los derechos de los sujetos y garantizar la confidencialidad de los datos recolectados.

3.4 Herramientas

3.4.1 Encuesta:

En investigación, una encuesta es una técnica de recolección de datos que consiste en formular preguntas estandarizadas a un grupo de personas con el fin de obtener información sobre sus opiniones, actitudes, creencias, experiencias o comportamientos en relación a un tema o problema específico (Gonzáles & Gallardo, 2021). Las encuestas pueden ser realizadas de forma presencial, telefónica, por correo o en línea, y pueden incluir preguntas abiertas o cerradas, preguntas de opción múltiple, escalas de opinión o preguntas de clasificación.

Las encuestas son ampliamente utilizadas en estudios de opinión pública, marketing, salud pública, ciencias sociales y otros campos, y pueden proporcionar información valiosa y representativa sobre las percepciones y comportamientos de una población determinada.

3.4.2 Observación participativa

La observación participante es una técnica de investigación cualitativa que implica la inserción del investigador en el contexto que se está estudiando y la participación activa en las actividades que allí se desarrollan. A través de la observación participante, el investigador busca obtener información sobre las prácticas, comportamientos, actitudes y valores de los individuos y grupos que forman parte del contexto de estudio(Hernández & Collado, 2018b).

Esta técnica se basa en la idea de que el investigador puede obtener una comprensión más profunda y completa del fenómeno que se está estudiando al involucrarse directamente

en el mismo. Durante la observación participante, el investigador puede tomar notas, registrar conversaciones y realizar entrevistas informales con los participantes para recopilar información y datos relevantes.

3.5 Procedimiento de Investigación

Para la elaboración de una metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037, se recomienda elaborar una metodología de buenas prácticas que permita al perito informático en Telecomunicaciones llevar a cabo su trabajo de manera efectiva y cumpliendo con los estándares internacionales de calidad y seguridad en la gestión de la información. Este proyecto se desarrolló en cuatro fases principales:

Fase 1. Planificación, donde se establecen los objetivos y alcances de la guía, se definen los temas y subtemas a tratar y se identifican los recursos necesarios para su desarrollo. En esta fase también se establecen las directrices para la elaboración de la guía, como el formato, la estructura y el estilo.

Fase 2. Adquisición, en la que se identifican y recolectan los datos necesarios para la elaboración de la guía. Estos datos pueden incluir investigaciones previas, mejores prácticas y recomendaciones de expertos en el área, así como también las normas y regulaciones aplicables. Es importante asegurar la integridad y preservación de los datos recopilados para su posterior análisis.

Fase 3. Elaboración, en la que se utiliza la información adquirida para desarrollar los temas y subtemas de la guía. En esta fase se pueden incluir ejemplos prácticos, listas de verificación, herramientas y plantillas que faciliten la aplicación de las mejores prácticas y recomendaciones.

Fase 4. Revisión y presentación de la guía. En esta fase se realizan revisiones y comentarios de expertos en el área para garantizar la calidad y efectividad de la guía. Se

pueden realizar pruebas piloto para evaluar su aplicabilidad y efectividad en situaciones reales. Una vez finalizada la revisión, se presenta la guía en el formato y estilo establecido en la fase de planificación, asegurándose de que sea clara, concisa y fácil de entender para los usuarios.

3.6 Operacionalización de variables

Tabla 2:

Operacionalización de variables.

Variables	Definición	Dimensión	Indicadores	ITEM	Técnicas e Instrumentos
metodología de buenas prácticas del perito informático en telecomunicaciones basada en la norma ISO 27037	Esta variable representa el método propuesto para la realización de las buenas prácticas del perito informático en Telecomunicaciones en el contexto ecuatoriano, siguiendo las pautas establecidas en la norma ISO 27037. Se trata de una variable que se implementará y se aplicará durante el	Marco legal y normativo	Identificación de la normativa aplicable Cumplimiento de los lineamientos de la norma ISO 27037	1	Encuesta-Cuestionario
		Procesamiento de evidencias digitales	- Técnicas de adquisición y preservación de evidencia Análisis de la evidencia digital Evaluación de la relevancia de la información	2,3,4	

	desarrollo de la investigación..	Formación y experiencia del perito informático	Conocimientos técnicos especializados Experiencia en el manejo de casos de telecomunicaciones	5,6,7,8	
Efectividad y calidad de las prácticas forenses en el análisis de evidencia digital en casos relacionados con las telecomunicaciones en Ecuador	Esta variable representa la calidad del trabajo realizado por los peritos informáticos en Telecomunicaciones en el Ecuador, y se medirá a través de la evaluación de los resultados obtenidos a partir de la aplicación de la metodología propuesta. La calidad del trabajo del perito informático puede verse afectada por diversos factores, como la formación y experiencia del perito, la aplicación de buenas prácticas y estándares	Precisión en la adquisición y preservación de evidencia	No alteración de la evidencia digital Documentación adecuada de la evidencia	9,10,13	Encuesta-Cuestionario
		Rigurosidad en el análisis de la evidencia digital	Identificación y análisis de la totalidad de la evidencia Evaluación adecuada de la relevancia de la información	9,11,14	
		Claridad y precisión en el informe forense	Redacción clara y concisa Descripción detallada de los procedimientos y técnicas utilizados Conclusiones claras y fundamentadas	12, 15, 16	

	internacionales, entre otros.

Nota: en la tabla 2 se puede apreciar la operacionalización de las variables, desarrollado por los investigadores

3.7 Consideraciones bioéticas

. En relación al tema de este proyecto, es importante considerar las implicaciones éticas en la obtención y manejo de la información digital. Los peritos informáticos tienen acceso a información sensible y confidencial, por lo que es crucial asegurar su confidencialidad, en cumplimiento de esto se presentan las siguientes consideraciones:

- Garantizar la privacidad y confidencialidad de la información recolectada y analizada, así como respetar los derechos de los individuos involucrados.
- Obtener el consentimiento informado y explícito de los participantes en el estudio.
- Realizar el estudio de manera ética, evitando cualquier tipo de discriminación o daño a los participantes.
- Garantizar la integridad y preservación de la evidencia digital recolectada.
- Utilizar técnicas y herramientas forenses adecuadas y validadas para el análisis de la evidencia.
- Evitar el uso de información o resultados obtenidos de manera ilegal o no autorizada.
- Garantizar la imparcialidad y objetividad en el análisis y presentación de los resultados.
- Considerar las implicaciones legales y sociales de los resultados obtenidos y actuar en consecuencia.

4. CAPITULO IV:

MARCO PRACTICO

4.1 Resultados y discusión

4.1.1 Análisis de encuesta

El cuestionario consta de dos secciones, la primera se enfoca en la calidad del trabajo del perito informático y la segunda en la metodología de buenas prácticas bajo la norma ISO 27037. En cada sección se encuentran preguntas que buscan conocer su opinión y percepción acerca de diferentes dimensiones que se han identificado como importantes para la evaluación de la calidad del trabajo del perito informático y la efectividad de la metodología de buenas prácticas.

El cuestionario se elaboró con 8 funcionarios públicos en base a una escala Likert de 5 puntos en las que las posibles opciones son:

- Totalmente en desacuerdo
- En desacuerdo
- Neutral
- De acuerdo
- Totalmente de acuerdo

Para la variable independiente: Metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 para su aplicación en el Ecuador.

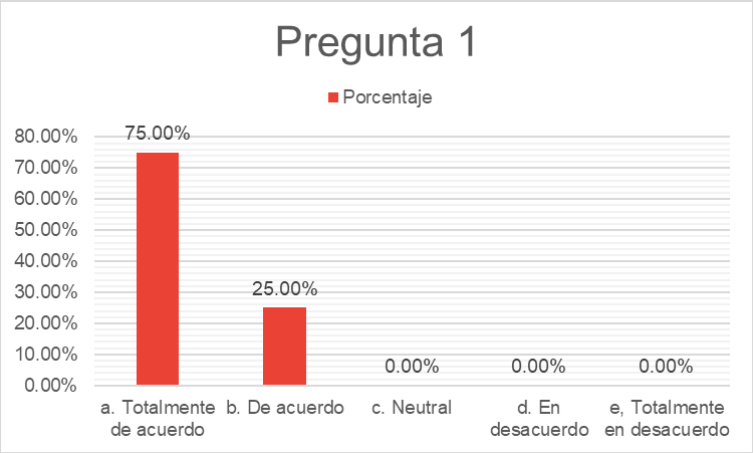
Pregunta 1: En general, ¿considera que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 es adecuada para su aplicación en el Ecuador?

Tabla 3:
Resultados pregunta 1.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	6	75.00%
b. De acuerdo	2	25.00%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 3 se puede apreciar los resultados obtenidos en la pregunta 1, fuente encuesta aplicada el 2022

Figura 6: Resultados pregunta 1**.**



Nota: En la Figura 6 se puede apreciar los resultados obtenidos en la pregunta 1, fuente encuesta aplicada el 2022

Análisis:

La pregunta 1 del cuestionario tuvo una alta tasa de respuesta positiva, con un 75% de los encuestados respondiendo "totalmente de acuerdo" y el 25% restante respondiendo "de acuerdo". Esto sugiere que la metodología de buenas prácticas del perito informático en telecomunicaciones bajo la norma ISO 27037 es vista de manera positiva por los encuestados y se considera adecuada para su aplicación en el Ecuador.

Sería útil profundizar en las razones detrás de las respuestas positivas para entender mejor cómo la metodología de buenas prácticas del perito informático en telecomunicaciones bajo la norma ISO 27037 se ajusta a las necesidades y requisitos de los peritos informáticos en Ecuador, y para identificar posibles áreas de mejora.

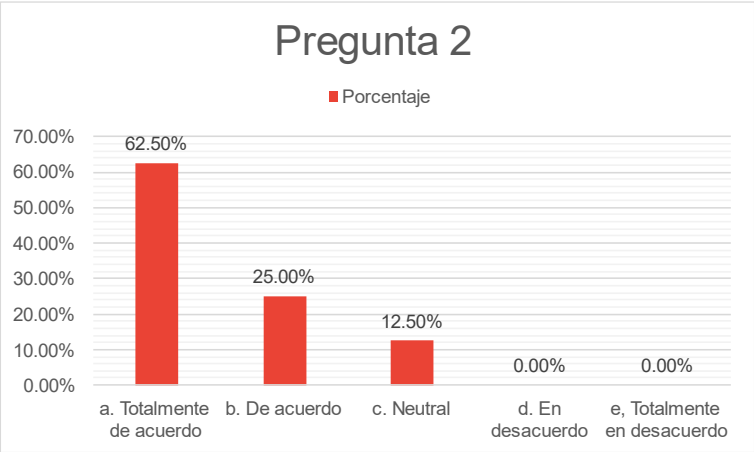
Pregunta 2: ¿Considera que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 le permite realizar de manera eficiente y efectiva su trabajo como perito informático?

Tabla 4:
Resultados pregunta 2.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	5	62.50%
b. De acuerdo	2	25.00%
c. Neutral	1	12.50%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 4 se puede apreciar los resultados obtenidos en la pregunta 2, fuente encuesta aplicada el 2022

Figura 7: Resultados pregunta 2.



Nota: En la Figura 7 se puede apreciar los resultados obtenidos en la pregunta 2, fuente encuesta aplicada el 2022

Análisis:

De los 8 encuestados, el 87.5% (7 personas) están de acuerdo o totalmente de acuerdo en que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 les permite realizar de manera eficiente y efectiva su trabajo como perito informático. Solo una persona (12.5%) se muestra neutral ante esta afirmación.

Estos resultados sugieren que la mayoría de los peritos informáticos encuestados consideran que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 es efectiva en su trabajo. Sin embargo, también se debe tener en cuenta la opinión de la persona que se mostró neutral, ya que podría haber aspectos de la metodología que no esté seguro de su eficacia.

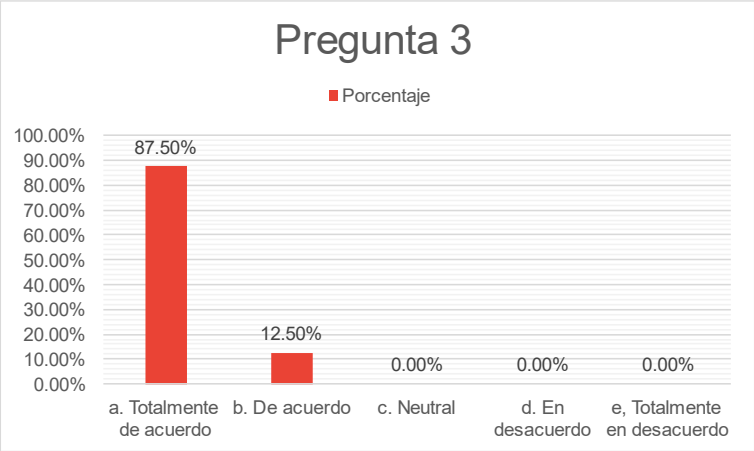
Pregunta 3: ¿La metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 proporciona una guía clara para llevar a cabo la investigación?

Tabla 5:
Resultados pregunta 3.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	7	87.50%
b. De acuerdo	1	12.50%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 5 se puede apreciar los resultados obtenidos en la pregunta 3, fuente encuesta aplicada el 2022

Figura 8: Resultados pregunta 3.



Nota: En la Figura 8 se puede apreciar los resultados obtenidos en la pregunta 3, fuente encuesta aplicada el 2022

Análisis:

En la pregunta 3, se observa que el 87.5% de los encuestados están totalmente de acuerdo en que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 proporciona una guía clara para llevar a cabo la investigación. Además, el 12.5% restante está de acuerdo con esta afirmación. En general, se puede inferir que los encuestados perciben que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 proporciona una guía clara para realizar las investigaciones.

Pregunta 4: ¿La metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 le permite identificar y preservar adecuadamente las evidencias digitales?

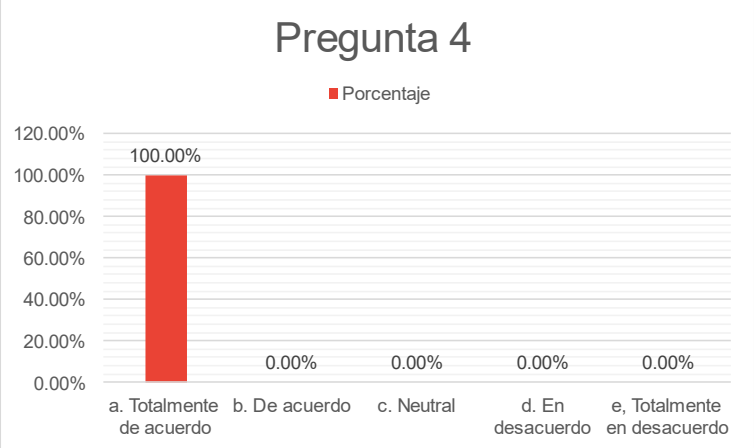
Tabla 6:
Resultados pregunta 4.

Respuesta	Frecuencia	Porcentaje

a. Totalmente de acuerdo	8	100.00%
b. De acuerdo	0	0.00%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 6 se puede apreciar los resultados obtenidos en la pregunta 4, fuente encuesta aplicada el 2022

Figura 9: Resultados pregunta 4**.**



Nota: En la Figura 9 se puede apreciar los resultados obtenidos en la pregunta 4, fuente encuesta aplicada el 2022

Análisis:

De acuerdo con los resultados de la tabla 6, se puede inferir que los encuestados están completamente de acuerdo en que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 les permite identificar y preservar adecuadamente las evidencias digitales. Esta respuesta unánime sugiere que la metodología proporciona un marco efectivo para el manejo de evidencias digitales en investigaciones relacionadas con telecomunicaciones.

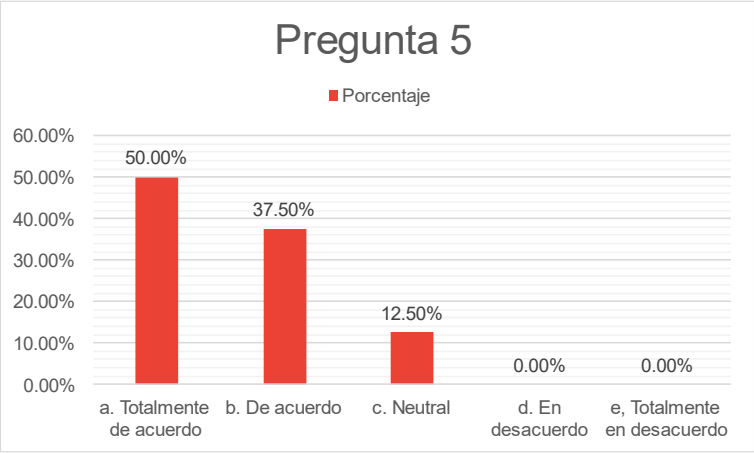
Pregunta 5: ¿La metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 le proporciona un marco adecuado para el análisis de la evidencia digital?

Tabla 7:
Resultados pregunta 5.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	4	50.00%
b. De acuerdo	3	37.50%
c. Neutral	1	12.50%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 7 se puede apreciar los resultados obtenidos en la pregunta 5, fuente encuesta aplicada el 2022

Figura 10: Resultados pregunta 5.



Nota: En la Figura 10 se puede apreciar los resultados obtenidos en la pregunta 5, fuente encuesta aplicada el 2022

Análisis:

Según los resultados de la pregunta 5, el 87.5% de los encuestados está de acuerdo o totalmente de acuerdo en que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 proporciona un marco adecuado para el análisis de la evidencia digital, mientras que el 12.5% restante se mantiene neutral. Esto sugiere que la mayoría de los peritos informáticos en Telecomunicaciones en el Ecuador consideran que la metodología ISO 27037 proporciona un marco adecuado para el análisis de la evidencia digital. Sin embargo, la proporción de aquellos que se mantienen neutrales indica que algunos encuestados podrían tener reservas o dudas sobre la efectividad de la metodología en este aspecto. Es necesario profundizar en los resultados de la encuesta y explorar las posibles razones detrás de las respuestas neutrales para determinar si es necesario realizar mejoras en la metodología o en la capacitación de los peritos informáticos en este campo.

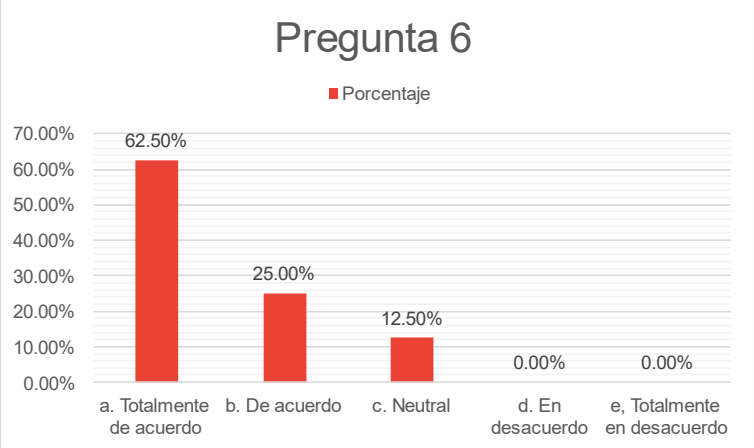
Pregunta 6: ¿La metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 considera adecuadamente el marco legal aplicable en el Ecuador?

Tabla 8:
Resultados pregunta 6.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	5	62.50%
b. De acuerdo	2	25.00%
c. Neutral	1	12.50%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 8 se puede apreciar los resultados obtenidos en la pregunta 6, fuente encuesta aplicada el 2022

Figura 11: Resultados pregunta 6.



Nota: En la Figura 11 se puede apreciar los resultados obtenidos en la pregunta 6, fuente encuesta aplicada el 2022

Análisis:

La pregunta 6 indagó sobre si los encuestados consideran que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 considera adecuadamente el marco legal aplicable en el Ecuador. Los resultados mostraron que el 62.50% de los encuestados estuvieron totalmente de acuerdo, el 25.00% estuvo de acuerdo, y el 12.50% se mantuvo neutral. Ninguno de los encuestados se encontró en desacuerdo o totalmente en desacuerdo.

A partir de estos resultados, se puede inferir que la mayoría de los encuestados consideran que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 toma en cuenta adecuadamente el marco legal aplicable en el Ecuador, lo cual puede ser un indicador de que la metodología es apropiada para su implementación en el contexto ecuatoriano. Sin embargo, se debe tener en cuenta que un porcentaje significativo de los encuestados se mantuvo neutral o en desacuerdo, lo cual sugiere que podría haber cierta variabilidad en las percepciones de los encuestados sobre este tema en particular.

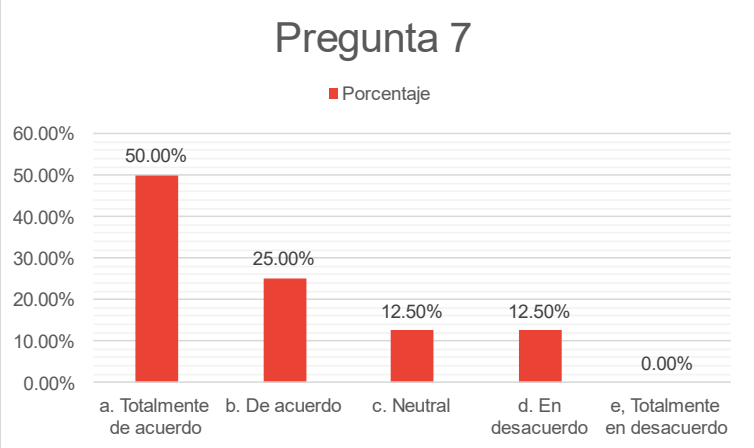
Pregunta 7: ¿La metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 es fácil de aplicar en la práctica?

Tabla 9:
Resultados pregunta 7.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	4	50.00%
b. De acuerdo	2	25.00%
c. Neutral	1	12.50%
d. En desacuerdo	1	12.50%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 9 se puede apreciar los resultados obtenidos en la pregunta 7, fuente encuesta aplicada el 2022

Figura 12: Resultados pregunta 7.



Nota: En la Figura 12 se puede apreciar los resultados obtenidos en la pregunta 7, fuente encuesta aplicada el 2022

Análisis:

La pregunta 7 se refiere a la facilidad de aplicación de la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037. Los resultados muestran que el 50% de los encuestados están totalmente de acuerdo en que la metodología es fácil de aplicar en la práctica, mientras que el 25% está de acuerdo. Sin embargo, el 12.5% de los encuestados se muestra neutral y el 12.5% está en desacuerdo en que la metodología es fácil de aplicar. Este resultado sugiere que aunque la mayoría de los encuestados considera que la metodología es fácil de aplicar, aún hay una proporción significativa de encuestados que no tienen una opinión clara sobre la facilidad de aplicación. Por lo tanto, es necesario explorar más a fondo las posibles razones detrás de estas respuestas y abordar cualquier problema de usabilidad o barreras percibidas que puedan existir para garantizar la eficacia y eficiencia de la metodología en la práctica.

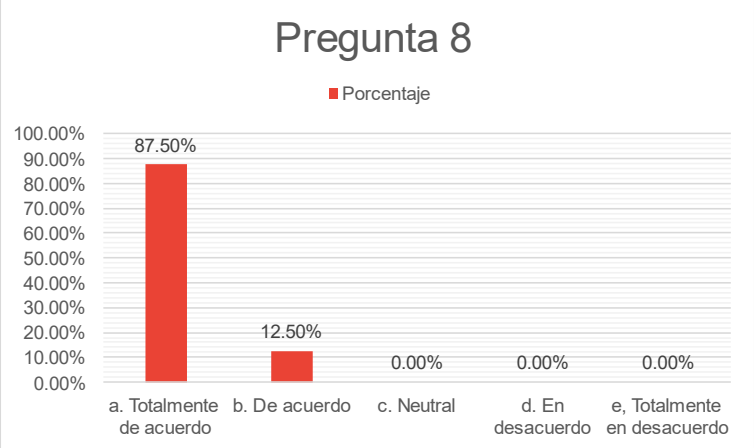
Pregunta 8: ¿Considera que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 debería ser adoptada como estándar en el Ecuador?

Tabla 10:
Resultados pregunta 8.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	7	87.50%
b. De acuerdo	1	12.50%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 10 se puede apreciar los resultados obtenidos en la pregunta 8, fuente encuesta aplicada el 2022

Figura 13: Resultados pregunta 8**.**



Nota: En la Figura 13 se puede apreciar los resultados obtenidos en la pregunta 8, fuente encuesta aplicada el 2022

Análisis:

Los resultados de la pregunta 8 indican que la gran mayoría de los encuestados están de acuerdo en que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 debería ser adoptada como estándar en el Ecuador. Esto sugiere que hay una aceptación generalizada de la importancia de establecer estándares para la práctica del peritaje informático en el país. Además, estos resultados pueden ser útiles para los responsables de la toma de decisiones en el ámbito de la justicia y la seguridad informática en el Ecuador para considerar la implementación de la norma ISO 27037 como una práctica estándar en la investigación de delitos informáticos.

Para la variable dependiente: Calidad del trabajo del perito informático en Telecomunicaciones en el Ecuador.

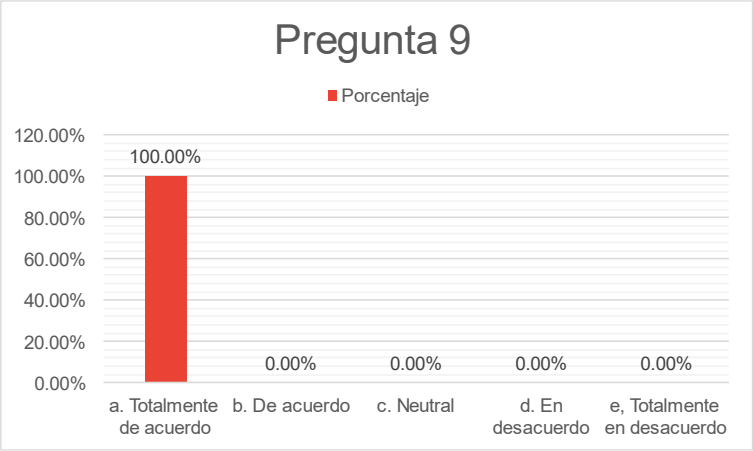
Pregunta 9: ¿Considera que el trabajo del perito informático en Telecomunicaciones en el Ecuador es riguroso y preciso?

Tabla 11:
Resultados pregunta 9.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	8	100.00%
b. De acuerdo	0	0.00%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 11 se puede apreciar los resultados obtenidos en la pregunta 9, fuente encuesta aplicada el 2022

Figura 14: Resultados pregunta 9.



Nota: En la Figura 14 se puede apreciar los resultados obtenidos en la pregunta 9, fuente encuesta aplicada el 2022

Análisis:

La pregunta 9 obtuvo un resultado del 100% en la respuesta "Totalmente de acuerdo" lo que sugiere que los encuestados consideran que el trabajo del perito informático en Telecomunicaciones en el Ecuador es riguroso y preciso. Este resultado es consistente con la literatura existente sobre la importancia de la precisión y rigurosidad en el trabajo de los peritos informáticos en telecomunicaciones, ya que esto es esencial para garantizar la confiabilidad de las pruebas presentadas en el proceso judicial. Además, la precisión y rigurosidad son también importantes para garantizar la integridad de la evidencia digital y evitar su contaminación o alteración durante el proceso de recolección y análisis. En este sentido, la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 puede contribuir a mejorar la calidad del trabajo del perito informático en el Ecuador, y, por ende, a mejorar la fiabilidad de las pruebas presentadas en el proceso judicial.

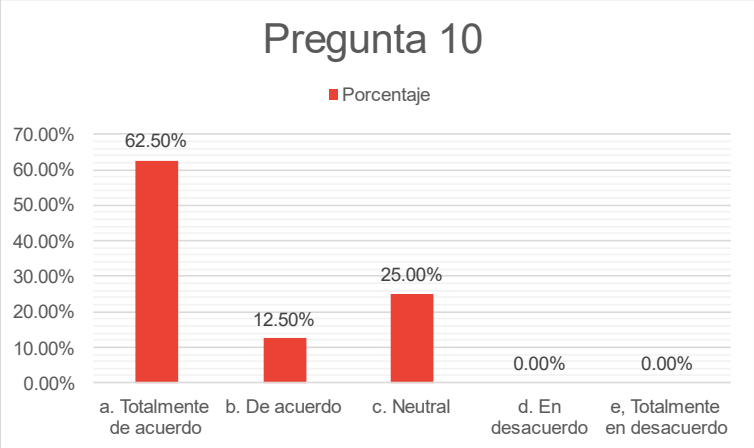
Pregunta 10: ¿Considera que el trabajo del perito informático en Telecomunicaciones en el Ecuador es confiable y veraz?

Tabla 12:
Resultados pregunta 10.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	5	62.50%
b. De acuerdo	1	12.50%
c. Neutral	2	25.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 12 se puede apreciar los resultados obtenidos en la pregunta 10, fuente encuesta aplicada el 2022

Figura 15: Resultados pregunta 10.



Nota: En la Figura 15 se puede apreciar los resultados obtenidos en la pregunta 10, fuente encuesta aplicada el 2022

Análisis:

Según los resultados obtenidos en la pregunta 10, el 62.50% de los encuestados están totalmente de acuerdo en que el trabajo del perito informático en Telecomunicaciones en el Ecuador es confiable y veraz, mientras que el 12.50% está de acuerdo y el 25.00% se mantiene neutral en su respuesta. No se registraron respuestas en desacuerdo.

Sería interesante contrastar estos resultados con estudios previos o fuentes externas para determinar si esta percepción es consistente con la opinión general del sector y la sociedad en general. También es importante considerar que la percepción de la confiabilidad y veracidad del trabajo del perito informático puede estar influenciada por factores como la reputación y la credibilidad de las personas o entidades involucradas en el proceso.

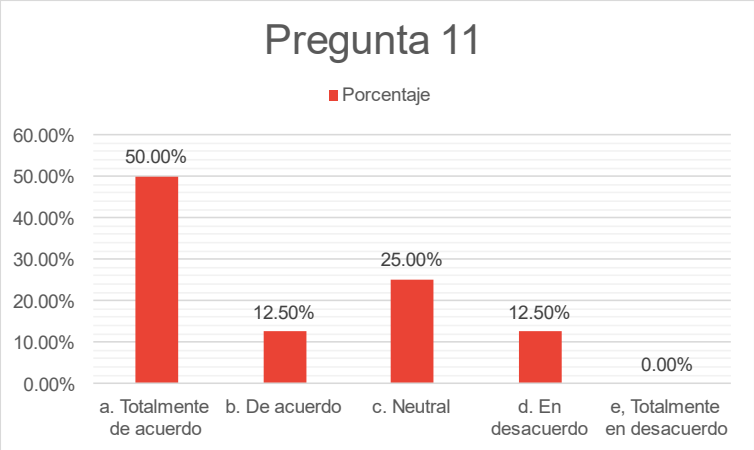
Pregunta 11: ¿El trabajo del perito informático en Telecomunicaciones en el Ecuador considera adecuadamente la privacidad y seguridad de la información?

Tabla 13:
Resultados pregunta 11.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	4	50.00%
b. De acuerdo	1	12.50%
c. Neutral	2	25.00%
d. En desacuerdo	1	12.50%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 13 se puede apreciar los resultados obtenidos en la pregunta 11, fuente encuesta aplicada el 2022

Figura 16: Resultados pregunta 11**.**



Nota: En la Figura 16 se puede apreciar los resultados obtenidos en la pregunta 11, fuente encuesta aplicada el 2022

Análisis:

En la tabla se puede observar que el 50% de los encuestados están totalmente de acuerdo en que el trabajo del perito informático en Telecomunicaciones en Ecuador considera adecuadamente la privacidad y seguridad de la información, mientras que el 12.5% está de acuerdo y el 12.5% está en desacuerdo. Además, el 25% de los encuestados respondió como neutral. Estos resultados sugieren que hay una percepción dividida en cuanto a la consideración de la privacidad y seguridad de la información en el trabajo del perito informático en Telecomunicaciones en el Ecuador. Es importante destacar la necesidad de que los peritos informáticos tomen medidas adecuadas para garantizar la privacidad y seguridad de la información durante su trabajo, ya que esto puede tener un impacto significativo en los procesos judiciales y en la confianza del público en el sistema legal.

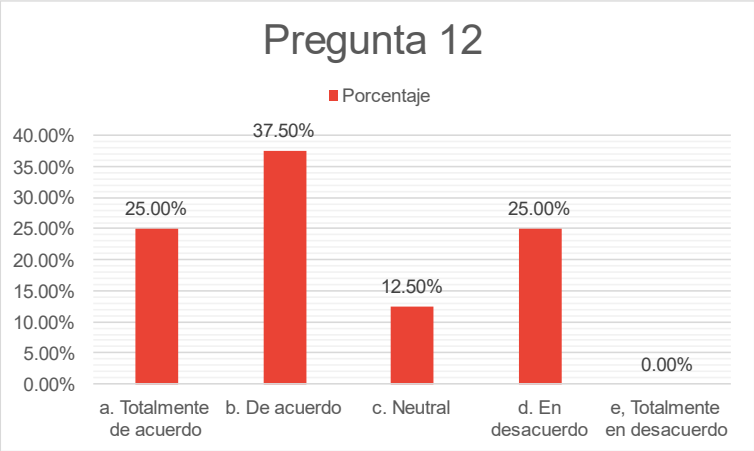
Pregunta 12: ¿El trabajo del perito informático en Telecomunicaciones en el Ecuador se realiza en un tiempo razonable y eficiente?

Tabla 14:
Resultados pregunta 12.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	2	25.00%
b. De acuerdo	3	37.50%
c. Neutral	1	12.50%
d. En desacuerdo	2	25.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 14 se puede apreciar los resultados obtenidos en la pregunta 12, fuente encuesta aplicada el 2022

Figura 17: Resultados pregunta 12**.**



Nota: En la Figura 17 se puede apreciar los resultados obtenidos en la pregunta 12, fuente encuesta aplicada el 2022

Análisis:

La pregunta 1 del cuestionario tuvo una alta tasa de respuesta positiva, con un 62.5% de los encuestados respondiendo "totalmente de acuerdo" y el 25% restante respondiendo "en desacuerdo" y 12.5% neutral. Esto sugiere que la metodología de buenas prácticas del perito informático en telecomunicaciones bajo la norma ISO 27037 es vista de manera positiva por los encuestados y se considera adecuada para su aplicación en el Ecuador.

Sería útil profundizar en las razones detrás de las respuestas negativas para entender mejor cómo la metodología de buenas prácticas del perito informático en telecomunicaciones bajo la norma ISO 27037 se ajusta a las necesidades y requisitos de los peritos informáticos en Ecuador, y para identificar posibles áreas de mejora.

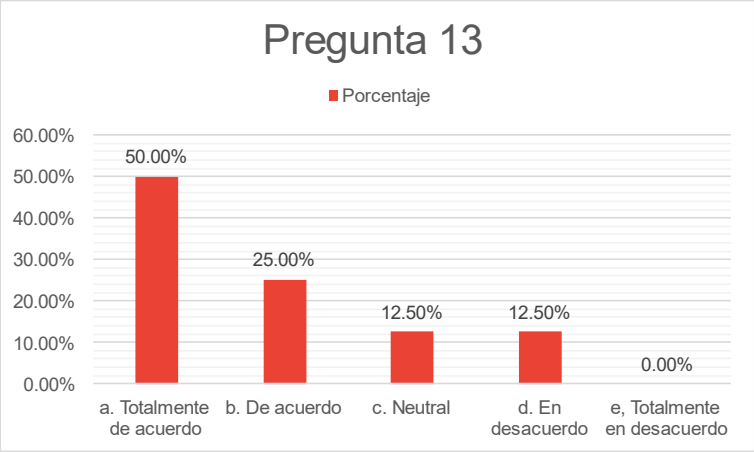
Pregunta 13: ¿El trabajo del perito informático en Telecomunicaciones en el Ecuador considera adecuadamente las necesidades y demandas del cliente o la institución?

Tabla 15:
Resultados pregunta 13.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	4	50.00%
b. De acuerdo	2	25.00%
c. Neutral	1	12.50%
d. En desacuerdo	1	12.50%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 15 se puede apreciar los resultados obtenidos en la pregunta 13, fuente encuesta aplicada el 2022

Figura 18: Resultados pregunta 13.



Nota: En la Figura 18 se puede apreciar los resultados obtenidos en la pregunta 13, fuente encuesta aplicada el 2022

Análisis:

En la pregunta 13, se puede observar que el 75% de los encuestados están de acuerdo o totalmente de acuerdo en que el trabajo del perito informático en Telecomunicaciones en Ecuador considera adecuadamente las necesidades y demandas del cliente o la institución. Sin embargo, un 12.5% de los encuestados están en desacuerdo con esta afirmación, lo que sugiere que todavía hay espacio para mejorar la atención al cliente y la satisfacción de sus necesidades en el trabajo de los peritos informáticos en el país. Es importante destacar que la percepción de los clientes y las instituciones sobre el trabajo del perito informático puede influir significativamente en su reputación y éxito profesional, por lo que es importante seguir trabajando en mejorar la calidad de su servicio.

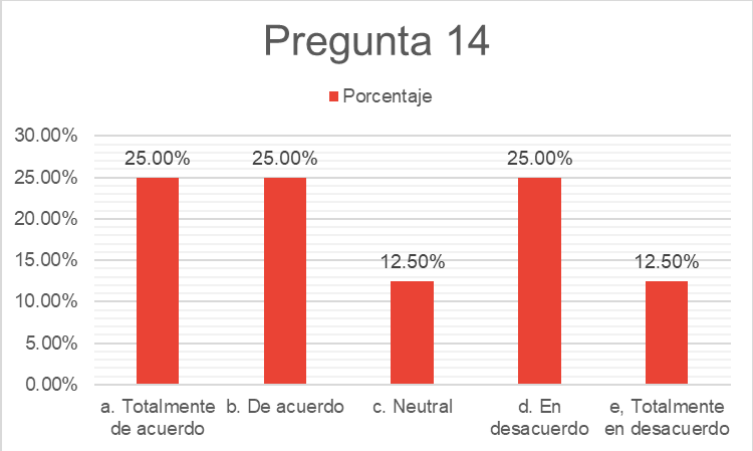
Pregunta 14: ¿El trabajo del perito informático en Telecomunicaciones en el Ecuador utiliza tecnología y herramientas actualizadas?

Tabla 16:
Resultados pregunta 14.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	2	25.00%
b. De acuerdo	2	25.00%
c. Neutral	1	12.50%
d. En desacuerdo	2	25.00%
e, Totalmente en desacuerdo	1	12.50%
TOTAL	8	100.00%

Nota: En la tabla 16 se puede apreciar los resultados obtenidos en la pregunta 14, fuente encuesta aplicada el 2022

Figura 19: Resultados pregunta 14.



Nota: En la Figura 19 se puede apreciar los resultados obtenidos en la pregunta 14, fuente encuesta aplicada el 2022

Análisis:

La pregunta 14 busca conocer la opinión de los encuestados sobre si el trabajo del perito informático en Telecomunicaciones en el Ecuador utiliza tecnología y herramientas actualizadas. En la tabla 17 se muestra que la mayoría de los encuestados (50%) no están totalmente de acuerdo o en desacuerdo con esta afirmación, mientras que el 50% restante se divide en igual proporción entre los que están de acuerdo y los que tienen una opinión neutral.

Es importante destacar que el uso de tecnología y herramientas actualizadas es fundamental para el trabajo de un perito informático, ya que esto puede influir en la precisión y confiabilidad de las conclusiones a las que se llega en una investigación. Es posible que los encuestados que tienen una opinión neutral o negativa sobre este tema consideren que hay una falta de actualización en la tecnología y herramientas utilizadas en el trabajo de los peritos informáticos en el Ecuador.

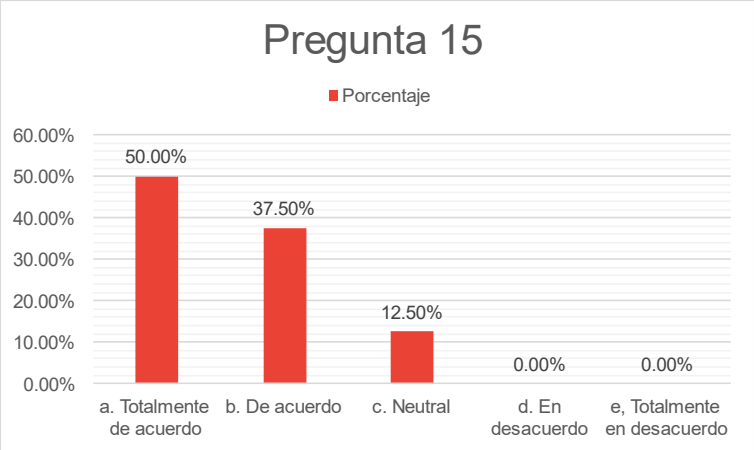
Pregunta 15: ¿El trabajo del perito informático en Telecomunicaciones en el Ecuador se realiza de manera ética y profesional?

Tabla 17:
Resultados pregunta 15.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	4	50.00%
b. De acuerdo	3	37.50%
c. Neutral	1	12.50%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 17 se puede apreciar los resultados obtenidos en la pregunta 15, fuente encuesta aplicada el 2022

Figura 20: Resultados pregunta 15.



Nota: En la Figura 20 se puede apreciar los resultados obtenidos en la pregunta 15, fuente encuesta aplicada el 2022

Análisis:

En la pregunta 15 de la encuesta aplicada, se puede observar que el 87.5% de los encuestados están de acuerdo en que el trabajo del perito informático en Telecomunicaciones en el Ecuador se realiza de manera ética y profesional, ya que 4 personas respondieron "Totalmente de acuerdo" y 3 personas respondieron "De acuerdo". Mientras tanto, el 12.5% restante respondió "Neutral". No hubo ninguna respuesta en las categorías "En desacuerdo" o "Totalmente en desacuerdo".

Estos resultados sugieren que en general, los encuestados tienen una opinión favorable sobre la ética y profesionalismo de los peritos informáticos en el Ecuador. Sin embargo, es importante tener en cuenta que la muestra de la encuesta es limitada y puede no ser representativa de la opinión general del público en el país. Además, sería necesario realizar estudios adicionales para evaluar con mayor detalle la ética y profesionalismo del trabajo de los peritos informáticos en Telecomunicaciones en el Ecuador.

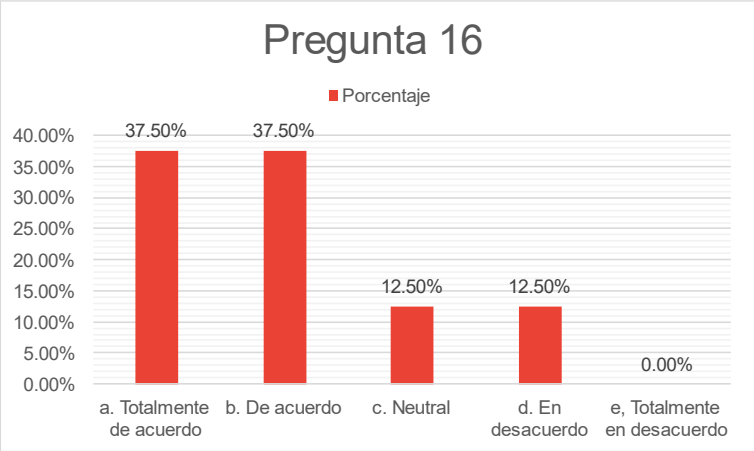
Pregunta 16: ¿El trabajo del perito informático en Telecomunicaciones en el Ecuador se realiza con una adecuada comunicación y colaboración con otras partes involucradas en el proceso?

Tabla 18:
Resultados pregunta 16.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	3	37.50%
b. De acuerdo	3	37.50%
c. Neutral	1	12.50%
d. En desacuerdo	1	12.50%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 18 se puede apreciar los resultados obtenidos en la pregunta 16, fuente encuesta aplicada el 2022

Figura 21: Resultados pregunta 16.



Nota: En la Figura 21 se puede apreciar los resultados obtenidos en la pregunta 16, fuente encuesta aplicada el 2022

Análisis:

En la tabla 19 se muestran los resultados obtenidos en la pregunta 16 de la encuesta aplicada en el Ecuador en 2022, en la cual se consultó sobre si el trabajo del perito informático en Telecomunicaciones se realiza con una adecuada comunicación y colaboración con otras partes involucradas en el proceso.

De los participantes de la encuesta, el 37.5% respondió "Totalmente de acuerdo" y otro 37.5% respondió "De acuerdo", indicando que consideran que el trabajo del perito informático en Telecomunicaciones en el Ecuador se realiza con una adecuada comunicación y colaboración con otras partes involucradas en el proceso. El 12.5% respondió "Neutral" y otro 12.5% respondió "En desacuerdo".

Se puede inferir que, según la percepción de los encuestados, existe una variedad de opiniones respecto a la adecuada comunicación y colaboración del perito informático en Telecomunicaciones con otras partes involucradas en el proceso en el Ecuador. Esto podría ser indicativo de la necesidad de mejorar la comunicación y colaboración en este ámbito.

4.2 Discusión General de la encuesta

El cuestionario aplicado tuvo como objetivo conocer la opinión de los peritos informáticos en Telecomunicaciones en Ecuador sobre la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 y la calidad de su trabajo. En general, los resultados muestran que los peritos informáticos en Telecomunicaciones en Ecuador consideran que la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 es adecuada para su aplicación en el país. Además, la gran mayoría de los encuestados considera que la metodología proporciona una guía clara para llevar a cabo la investigación y permite identificar y preservar adecuadamente las evidencias digitales.

Sin embargo, también se evidencian ciertas preocupaciones sobre la aplicación práctica de la metodología, especialmente en lo que se refiere a su facilidad de uso y a la adecuada consideración del marco legal aplicable en Ecuador.

En cuanto a la calidad del trabajo de los peritos informáticos en Telecomunicaciones en Ecuador, se observa que en general se considera que es riguroso y preciso, y que se realiza de manera ética y profesional. No obstante, se perciben ciertas dudas sobre su confiabilidad y veracidad, y sobre si considera adecuadamente la privacidad y seguridad de la información.

Finalmente, en cuanto a la comunicación y colaboración con otras partes involucradas en el proceso, se evidencia que existe una opinión dividida entre los encuestados, lo que sugiere que aún hay espacio para mejorar en este aspecto. En conclusión, aunque en general los peritos informáticos en Telecomunicaciones en Ecuador parecen estar satisfechos con la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037, aún existen desafíos en su aplicación práctica y en la calidad del trabajo realizado. Esto sugiere la necesidad de una mayor capacitación y actualización en las herramientas y tecnologías utilizadas por los peritos informáticos en el país, así como de un mayor enfoque en la comunicación y colaboración con otras partes involucradas en el proceso.

4.3 Propuesta Metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 para su aplicación en el Ecuador

4.3.1 Introducción

La elaboración de una metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 para su aplicación en el Ecuador tiene como objetivo proporcionar una guía clara y precisa para la realización de investigaciones informáticas y peritajes en el ámbito de las telecomunicaciones, en cumplimiento de las leyes y regulaciones vigentes en el país.

En este contexto, la metodología se enfoca en establecer un marco de referencia adecuado para que los peritos informáticos puedan identificar, preservar y analizar las evidencias digitales, garantizando su integridad y confiabilidad. Además, se busca considerar las necesidades y demandas del cliente o la institución, así como las normativas relacionadas con la protección de datos personales y la propiedad intelectual.

La presente metodología está diseñada para ser aplicada por peritos informáticos que realicen investigaciones en el ámbito de las telecomunicaciones en el Ecuador, y busca contribuir al fortalecimiento de la seguridad jurídica y la protección de los derechos de las personas y empresas involucradas en los procesos de investigación.

4.3.2 Objetivos

4.3.2.1 Objetivo general:

Desarrollar una metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 que permita a los peritos informáticos llevar a cabo investigaciones forenses de manera eficiente, efectiva, ética y conforme a las normativas y leyes vigentes en el Ecuador.

4.3.2.2 Objetivos específicos

- Definir los procedimientos y técnicas para la recolección, análisis e interpretación de evidencia digital en casos de investigación en el ámbito de las telecomunicaciones, de acuerdo con la norma ISO 27037 y la legislación ecuatoriana aplicable.
- Establecer los protocolos y procedimientos para la preservación y custodia adecuada de la evidencia digital, garantizando su integridad y seguridad durante el proceso de investigación.
- Proporcionar un marco de referencia que permita al perito informático en Telecomunicaciones cumplir con los principios éticos y profesionales requeridos para el desarrollo de su trabajo, respetando los derechos y privacidad de las personas involucradas en la investigación.
- Garantizar la colaboración y comunicación efectiva con las partes involucradas en el proceso de investigación, incluyendo al cliente o institución, autoridades judiciales y otros peritos o expertos involucrados, con el fin de alcanzar una solución efectiva y justa.

4.3.3 Identificación de los usuarios o destinatarios de la guía y sus necesidades.

La guía de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 está dirigida principalmente a peritos informáticos que trabajan en el Ecuador y que están involucrados en la investigación de incidentes en sistemas de telecomunicaciones y en la recopilación y análisis de evidencia digital en el contexto de procesos legales o judiciales.

Tabla 19:
Beneficiarios de la Metodología.

Beneficiarios	Detalle de Beneficiario	Necesidad
Peritos informáticos	Profesionales que realizan investigaciones y análisis de evidencias digitales en casos judiciales y privados	Conocer las mejores prácticas para llevar a cabo sus labores de manera efectiva y eficiente, en cumplimiento de las normativas y leyes vigentes.
Abogados	Profesionales que trabajan en el ámbito legal y que pueden requerir la asesoría de peritos informáticos en casos que involucren tecnologías de la información	Comprender los métodos y prácticas utilizados por los peritos informáticos en la recolección, análisis y presentación de evidencias digitales.
Jueces y fiscales	Profesionales que deben tomar decisiones en casos legales que involucran evidencias digitales	Entender cómo se recolectan, analizan y presentan las evidencias digitales para tomar decisiones informadas en casos legales.
Empresas e instituciones	Entidades que pueden requerir los servicios de peritos informáticos para investigaciones internas o casos legales	Conocer las prácticas recomendadas para preservar y analizar adecuadamente las evidencias digitales en casos legales o investigaciones internas.
Estudiantes y académicos	Personas interesadas en el ámbito de la informática forense y la seguridad informática	Aprender sobre las mejores prácticas y metodologías utilizadas en la recolección, análisis y presentación de evidencias digitales.

Nota: en la tabla 19 se puede observar a los posibles beneficiarios de la guía metodológica, adaptado de (Rosero, 2019)

4.3.4 Definiciones relevantes

A continuación, se exponen algunas definiciones que son relevantes para la presente metodología:

Acceso no autorizado: Intento o acción de ingresar a un sistema o red de telecomunicaciones sin la debida autorización.

Cadena de custodia: Procedimiento documentado que garantiza la integridad y autenticidad de las evidencias digitales, desde su obtención hasta su presentación en el proceso judicial.

Ciberseguridad: Conjunto de medidas y estrategias utilizadas para proteger los sistemas, redes y dispositivos de telecomunicaciones contra amenazas cibernéticas.

Evidencia digital: Información almacenada o transmitida en forma digital que puede ser utilizada como prueba en un proceso judicial.

Forense digital: Conjunto de técnicas y herramientas utilizadas para recolectar, analizar e interpretar evidencias digitales en un proceso judicial.

Integridad de la información: Garantía de que la información no ha sido alterada de manera no autorizada.

Metadatos: Información adicional almacenada en los archivos digitales que describe su contenido y características.

Norma ISO 27037: Norma internacional que establece buenas prácticas para la obtención, análisis e interpretación de evidencias digitales.

Perito informático: Experto en el análisis de sistemas y dispositivos de telecomunicaciones, que realiza investigaciones forenses para recolectar y analizar evidencias digitales.

Privacidad de la información: Derecho de las personas a controlar la recopilación, uso, divulgación y almacenamiento de su información personal.

Propiedad intelectual: Derechos legales sobre obras originales de creación, como patentes, marcas, derechos de autor y diseños industriales.

Protocolo de red: Conjunto de reglas y procedimientos que definen cómo los dispositivos de telecomunicaciones se comunican entre sí en una red.

Seguridad de la información: Protección de la información contra el acceso no autorizado, el uso indebido, la divulgación y la destrucción.

Telecomunicaciones: Transmisión de información a través de dispositivos y sistemas electrónicos.

Vulnerabilidad: Debilidad o punto débil en un sistema o red de telecomunicaciones que puede ser explotado por amenazas cibernéticas.

4.3.5 Contexto legal y regulatorio en el Ecuador

En Ecuador, la Constitución es la ley suprema del país y establece los principios y valores fundamentales que rigen la vida política, social y jurídica del país. En el ámbito legal y regulatorio de las tecnologías de la información y las comunicaciones (TIC), el principal marco regulatorio es la Ley Orgánica de Telecomunicaciones, que establece las normas para el uso, acceso y gestión del espectro radioeléctrico, las telecomunicaciones y los servicios de radiodifusión.

Además, el Ecuador cuenta con la Ley Orgánica de Protección de Datos Personales, que establece los principios y reglas para la protección de la privacidad y los datos personales de los ciudadanos. Asimismo, existen otras leyes y regulaciones relacionadas con las TIC, como la Ley de Comercio Electrónico, la Ley de Firma Electrónica, la Ley de Propiedad Intelectual y la Ley de Seguridad y Defensa Nacional. A continuación, se tratará a detalle los elementos legales más relevantes en relación con la presente metodología de buenas prácticas.

4.3.5.1 Constitución del Ecuador

En cuanto a las autoridades encargadas de regular y supervisar el cumplimiento de estas normas, se encuentra la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), el Consejo Nacional de Telecomunicaciones (CONATEL), la Superintendencia de Información y Comunicación (SUPERCOM) y la Agencia de Protección de Datos Personales (APDP).

En la Constitución del Ecuador de(Asamblea Nacional del Ecuador, 2008), se hace referencia a varios artículos que tienen relación con el proyecto de Metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037. A continuación, se mencionan algunos de los artículos relevantes:

Artículo 23: Este artículo establece el derecho a la intimidad personal y familiar, y a la protección de los datos personales. La Metodología de buenas prácticas del perito informático en Telecomunicaciones debe asegurar que se respeten estos derechos en el proceso de investigación de evidencias digitales.

Artículo 66: Este artículo reconoce el derecho al acceso universal y equitativo a las tecnologías de la información y comunicación. La Metodología de buenas prácticas del perito informático en Telecomunicaciones debe considerar este derecho y garantizar que se utilicen tecnologías actualizadas en el proceso de investigación.

Artículo 227: Este artículo establece la responsabilidad de los servidores públicos de rendir cuentas y garantizar la transparencia en su gestión. La Metodología de buenas prácticas del perito informático en Telecomunicaciones debe asegurar que se cumpla con estas responsabilidades en el proceso de investigación.

Artículo 229: Este artículo establece el principio de la presunción de inocencia y el derecho a la defensa en los procesos judiciales. La Metodología de buenas prácticas del perito informático en Telecomunicaciones debe considerar estos principios y garantizar que se respeten en el proceso de investigación.

Artículo 230: Este artículo establece el derecho al debido proceso en los procesos judiciales. La Metodología de buenas prácticas del perito informático en Telecomunicaciones debe garantizar que se respete este derecho en el proceso de investigación.

4.3.5.2 Ley Orgánica de Telecomunicaciones

La Ley Orgánica de Telecomunicaciones de (Asamblea Nacional del Ecuador, 2015), es una norma legal en el Ecuador que regula el sector de las telecomunicaciones en el país. Fue aprobada en 2013 y establece las obligaciones, derechos y regulaciones para la prestación de servicios de telecomunicaciones.

Entre los aspectos relevantes de esta ley, se encuentran:

Artículo 2: que establece los objetivos y fines de la Ley, entre los cuales se encuentra la protección de los derechos de los usuarios de los servicios de telecomunicaciones.

Artículo 13: que establece la obligación de los operadores de telecomunicaciones de respetar la privacidad y confidencialidad de la información de los usuarios.

Artículo 44: que establece la obligación de los operadores de telecomunicaciones de preservar la confidencialidad de las comunicaciones y datos de los usuarios, salvo en los casos previstos por la ley.

Artículo 45: que establece la obligación de los operadores de telecomunicaciones de colaborar con las autoridades competentes en la investigación de delitos y la protección de la seguridad nacional.

Artículo 47: que establece la obligación de los operadores de telecomunicaciones de implementar medidas de seguridad para proteger la integridad, confidencialidad y disponibilidad de los servicios y datos de los usuarios.

Artículo 50: que establece la obligación de los operadores de telecomunicaciones de conservar y proteger los datos de tráfico y localización de las comunicaciones.

Artículo 66: que establece las condiciones para la interceptación y grabación de las comunicaciones por parte de los operadores de telecomunicaciones.

Artículo 67: que establece las condiciones y procedimientos para la cooperación entre los operadores de telecomunicaciones y las autoridades competentes en la investigación de delitos.

En cuanto a la relación con el proyecto de Metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037, esta ley puede ser relevante en aspectos como la protección de la privacidad de los usuarios de los servicios de telecomunicaciones y la regulación de los procedimientos para la obtención y análisis de evidencia digital en el marco de investigaciones relacionadas con el sector de las telecomunicaciones.

4.3.5.3 Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales (LOPD) de Asamblea nacional, (2021), es una ley ecuatoriana que regula el tratamiento y protección de datos personales en el país. Fue aprobada en 2018 y establece las obligaciones y derechos de las personas naturales y jurídicas que procesan datos personales.

En relación con el proyecto de Metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037, la LOPD es relevante ya que los peritos informáticos a menudo trabajan con datos personales en el contexto de sus investigaciones y análisis forenses. Por lo tanto, deben cumplir con las disposiciones de la LOPD, incluyendo la obtención del consentimiento adecuado para el procesamiento de datos personales, la implementación de medidas de seguridad para proteger dichos datos y la notificación a las autoridades en caso de una violación de seguridad que pueda afectar la privacidad de los datos personales. Entre los artículos más relevantes se encuentran:

Artículo 3: que define el ámbito de aplicación de la ley y establece que se aplica a todo tratamiento de datos personales realizado en el Ecuador, ya sea por entidades públicas o privadas.

Artículo 6: que establece los principios que deben guiar el tratamiento de datos personales, incluyendo el principio de consentimiento informado, el principio de finalidad, el principio de calidad de los datos, entre otros.

Artículo 7: que establece que el tratamiento de datos personales debe estar fundamentado en una base legal y que el consentimiento del titular de los datos debe ser libre, previo, expreso e informado.

Artículo 10: que establece los derechos de los titulares de los datos personales, incluyendo el derecho de acceso, rectificación, cancelación y oposición (derechos ARCO).

Artículo 16: que establece las medidas de seguridad que deben implementarse para proteger los datos personales y prevenir su pérdida, destrucción, alteración, acceso no autorizado, entre otros.

Es importante mencionar también que la LOPD establece la figura del Responsable de Tratamiento de Datos Personales, quien es el encargado de garantizar el cumplimiento de la ley y debe ser designado por todas las personas naturales y jurídicas que procesan datos personales. Los peritos informáticos que trabajan con datos personales como parte de su trabajo como peritos, también deben cumplir con esta obligación.

Ley de Comercio Electrónico, Firmas y Mensajes de Datos

En cuanto a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos de (Congreso Nacional del Ecuador, 2002) , esta establece la regulación de las firmas electrónicas y su uso en el ámbito público y privado. Entre los artículos más relevantes se encuentran:

Artículo 2: define el ámbito de aplicación de la ley, incluyendo las personas naturales o jurídicas, públicas o privadas, que utilicen firma electrónica en documentos y transacciones electrónicas.

Artículo 4: establece que la firma electrónica tendrá la misma validez jurídica que la firma manuscrita siempre que cumpla con los requisitos de autenticidad e integridad establecidos en la ley.

Artículo 6: dispone que la firma electrónica avanzada tendrá la presunción de ser auténtica e íntegra, salvo prueba en contrario.

Artículo 8: establece que las entidades de certificación tendrán la responsabilidad de emitir, renovar, revocar y administrar los certificados electrónicos.

Artículo 9: establece los requisitos que deben cumplir las entidades de certificación para su autorización y funcionamiento.

4.3.5.4 Ley de Propiedad Intelectual

En cuanto a la Ley de Propiedad Intelectual de (Asamblea Nacional, 2014), esta norma establece la protección legal de los derechos de propiedad intelectual en el Ecuador, incluyendo los derechos de autor, las patentes, marcas y diseños industriales, entre otros. A continuación, se presentan algunos de los artículos más relevantes de esta ley y su relación con el proyecto de metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037:

Artículo 14: Define lo que se considera una obra protegida por derechos de autor y establece que los derechos de autor son inalienables, irrenunciables e imprescriptibles. La metodología de buenas prácticas del perito informático puede incluir información protegida por derechos de autor, por lo que es importante respetar estos derechos y asegurarse de que se obtiene la autorización correspondiente antes de utilizar dicha información.

Artículo 70: Establece las excepciones y limitaciones al derecho de autor, incluyendo el derecho a utilizar obras protegidas para fines de investigación y análisis. Esto puede ser relevante para el trabajo del perito informático, ya que puede requerir el uso de obras protegidas para llevar a cabo sus investigaciones.

Artículo 71: Establece que la creación de obras derivadas de obras protegidas por derechos de autor está sujeta a la autorización del titular de los derechos. En el contexto del trabajo del perito informático, esto puede ser relevante si se necesitan crear copias o versiones modificadas de ciertos materiales para llevar a cabo las investigaciones.

Artículo 73: Establece que el uso de obras protegidas por derechos de autor para fines de seguridad nacional o protección de la propiedad pública está sujeto a la autorización del titular de los derechos o, en su defecto, del Ministerio de Cultura y Patrimonio. Esta disposición puede ser relevante para el trabajo del perito informático si se requiere el acceso a información protegida por derechos de autor para llevar a cabo investigaciones en el contexto de la seguridad nacional.

Artículo 99: Establece las sanciones para la violación de los derechos de propiedad intelectual, incluyendo los derechos de autor. Esto es relevante para el trabajo del perito informático, ya que es importante respetar los derechos de propiedad intelectual y asegurarse de que se obtiene la autorización correspondiente antes de utilizar información protegida.

4.3.5.5 Ley Orgánica de Defensa Nacional

La Ley Orgánica de Defensa Nacional establece las políticas, estrategias y acciones del Estado para garantizar la defensa nacional y la soberanía del país. En relación a un proyecto de metodología de buenas prácticas del perito informático en telecomunicaciones, algunos artículos relevantes podrían ser:

Artículo 7: Establece que la defensa nacional es responsabilidad de todos los ecuatorianos y que su cumplimiento es inexcusable.

Artículo 8: Señala que el Consejo de Seguridad Nacional es el órgano encargado de asesorar al Presidente de la República en materia de defensa y seguridad nacional.

Artículo 19: Establece la obligación del Estado de garantizar la seguridad de la información y de los sistemas de información que se utilicen en el ámbito de la defensa nacional.

Artículo 23: Regula el uso de la información clasificada y establece las medidas de seguridad que deben adoptarse para su protección.

Artículo 24: Regula el uso de las tecnologías de la información y la comunicación en el ámbito de la defensa nacional y establece la necesidad de contar con medidas de seguridad adecuadas.

La relación de estos artículos con el proyecto de metodología de buenas prácticas del perito informático en telecomunicaciones radica en la importancia de garantizar la seguridad de la información y los sistemas de información utilizados en la defensa nacional, lo que puede incluir la investigación de delitos informáticos y el peritaje informático en casos relacionados con la seguridad nacional. Además, estos artículos establecen la necesidad de contar con medidas de seguridad adecuadas y la regulación del uso de las tecnologías de la información y la comunicación en este ámbito, lo que puede ser relevante para la aplicación de la metodología de buenas prácticas del perito informático en telecomunicaciones.

4.3.6 Principios de la norma ISO 27037

La norma ISO 27037 según Anampa et al. (2021), establece los principios fundamentales para la realización de investigaciones digitales y la identificación, adquisición, preservación y análisis de evidencias digitales. A continuación, se detallan los principios de esta norma:

Legalidad: se debe llevar a cabo la investigación digital en cumplimiento con la legislación y regulaciones aplicables, respetando los derechos de privacidad y propiedad.

Integridad: se deben proteger las evidencias digitales para garantizar su exactitud, integridad y autenticidad, y evitar su alteración o eliminación.

Transparencia: se debe llevar a cabo la investigación digital de forma transparente y documentada, de manera que los resultados puedan ser comprobados y validados por terceros.

Imparcialidad: se deben llevar a cabo las investigaciones digitales de forma imparcial y sin sesgos, basándose únicamente en las evidencias disponibles.

Relevancia: se deben identificar y recopilar únicamente las evidencias digitales relevantes para la investigación.

Confidencialidad: se debe proteger la confidencialidad de las evidencias digitales y la información obtenida durante la investigación.

Competencia: se deben llevar a cabo las investigaciones digitales por personal competente y capacitado en la materia.

Colaboración: se debe fomentar la colaboración y comunicación entre todas las partes involucradas en la investigación, incluyendo al perito informático, el cliente, el abogado y otras partes interesadas.

Mejora continua: se deben implementar procesos y procedimientos para la mejora continua de las investigaciones digitales y el uso de buenas prácticas.

4.3.7 Fases de la metodología basado en la Norma ISO 27037

4.3.7.1 Fase 1: identificación de la necesidad de la investigación

La fase 1 de la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 es la identificación de la necesidad de la investigación. Esta fase es crucial ya que permite determinar los motivos que justifican la realización de la investigación y, por tanto, su alcance.

La fase de identificación de la necesidad de la investigación se puede dividir en cuatro etapas:

Definición del objetivo de la investigación: En esta etapa se define el propósito de la investigación, es decir, el objetivo que se pretende alcanzar con la investigación. Este objetivo debe estar claramente definido y debe estar en línea con las necesidades de la organización o entidad que solicita la investigación.

Identificación del alcance de la investigación: En esta etapa se define el alcance de la investigación, es decir, los límites que se imponen a la investigación. El alcance debe estar en consonancia con el objetivo de la investigación y debe ser lo suficientemente amplio para permitir la recopilación de toda la información relevante, pero lo suficientemente preciso para evitar la recopilación de información innecesaria.

Evaluación de los riesgos y amenazas: En esta etapa se evalúan los riesgos y amenazas que pueden afectar a la investigación. Esta evaluación debe tener en cuenta los riesgos y amenazas internos y externos, así como los riesgos y amenazas técnicos y legales.

Identificación de las fuentes de información: En esta etapa se identifican las fuentes de información que se utilizarán en la investigación. Las fuentes de información pueden ser diversas, desde registros de sistemas y bases de datos hasta documentos en papel y entrevistas con personas involucradas en el caso. Es importante identificar las fuentes de información relevantes y asegurarse de que se puedan acceder de forma legal y adecuada.

Tabla 20:
Etapas de la Fase 1.

Etapa	Detalle	Aplicación Práctica
Identificación de la necesidad de la investigación	Esta etapa consiste en identificar la necesidad de la investigación, determinando el objetivo de la misma y estableciendo los límites de la investigación.	Un cliente de una empresa de telecomunicaciones reporta que su línea telefónica ha sido intervenida y desea determinar si hay evidencia de intervención y quién ha sido el responsable..
Recopilación de información relevante	En esta etapa, se recopila toda la información relevante sobre el caso a investigar, incluyendo documentos, dispositivos electrónicos, registros de actividad y testimonios de testigos.	El perito informático recopila los registros de llamadas, facturas telefónicas y cualquier otro documento relevante para la investigación.
Análisis de la información recopilada	En esta etapa, se analiza la información recopilada para identificar patrones y tendencias, y se determina la relevancia y validez de la información.	El perito informático utiliza herramientas forenses para analizar los registros de llamadas y determinar si hay evidencia de intervención.
Evaluación de los resultados del análisis	En esta etapa, se evalúan los resultados del análisis para determinar si se cumplen los objetivos de la investigación y si se han recopilado pruebas suficientes para apoyar las conclusiones.	El perito informático presenta un informe detallado de la investigación al cliente y al tribunal, que incluye los resultados del análisis de los registros de llamadas y cualquier otra evidencia relevante encontrada.

Nota: En la tabla 20 se detalla cada etapa de la fase 1 de la metodología con un ejemplo de aplicación en cada etapa, adaptado de (Internacional Organization for Standardization, 2018).

En resumen, la fase de identificación de la necesidad de la investigación es crítica para el éxito de la investigación, ya que permite establecer los objetivos y alcances de la misma, evaluar los riesgos y amenazas y determinar las fuentes de información que se utilizarán en la investigación. Es importante que esta fase se lleve a cabo de manera exhaustiva y precisa para garantizar la validez y fiabilidad de la investigación.

4.3.7.2 Fase 2: Planificación y preparación de la investigación

La Fase 2 de la norma ISO 27037 se centra en la planificación y preparación de la investigación. En esta fase, se deben establecer los objetivos de la investigación, determinar

las fuentes de información, planificar el alcance y la metodología de la investigación, establecer los requisitos de recursos y asegurar la protección de la evidencia.

A continuación, se detalla cada una de las etapas de la Fase 2:

Establecimiento de los objetivos de la investigación: En esta etapa se definen los objetivos de la investigación, incluyendo qué se espera lograr y qué tipo de evidencia se requiere para lograr los objetivos establecidos.

Planificación del alcance y la metodología de la investigación: En esta etapa se determina el alcance de la investigación y se establece la metodología de la misma, incluyendo los procedimientos y técnicas que se utilizarán para la obtención y análisis de la evidencia.

La etapa de planificación de la investigación en la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 implica la elaboración de un plan de investigación que permita llevar a cabo el proceso de forma estructurada y eficiente. A continuación, se detallan algunos puntos que debe contener el plan de investigación:

Objetivos: Es fundamental definir los objetivos de la investigación para orientar el trabajo del perito informático y establecer metas claras.

Alcance: Debe establecerse el alcance de la investigación, es decir, las áreas específicas que se investigarán.

Recursos: Es importante identificar los recursos necesarios para llevar a cabo la investigación, tales como herramientas tecnológicas, personal y presupuesto.

Planificación temporal: Se debe establecer un cronograma que permita planificar el tiempo necesario para realizar cada tarea y cumplir con los plazos establecidos.

Análisis de riesgos: Se deben identificar los riesgos asociados al proceso de investigación y establecer medidas para prevenirlos o mitigarlos.

Evaluación de pruebas: Es necesario definir los criterios para la evaluación de las pruebas recolectadas y establecer un procedimiento para su análisis.

Comunicación con las partes involucradas: Se debe establecer un plan de comunicación para mantener informadas a las partes involucradas en la investigación, incluyendo al cliente y a los tribunales si fuera necesario.

Documentación: Es importante establecer un procedimiento de documentación que permita registrar todas las acciones realizadas durante la investigación, desde la recolección de evidencia hasta la presentación de informes.

Establecimiento de los requisitos de recursos y la protección de la evidencia: En esta etapa se definen los recursos necesarios para llevar a cabo la investigación, incluyendo el personal, equipos, herramientas y tecnología. Además, se deben establecer las medidas necesarias para proteger la evidencia durante el proceso de investigación.

Tabla 21:
Etapas de la fase 2.

Etapa	Detalle	Aplicación práctica en Telecomunicaciones
Identificación de objetivos y alcance	Identificar los objetivos y alcance de la investigación.	Definir claramente los objetivos de la investigación y establecer el alcance de la misma en relación a la problemática planteada. Por ejemplo, identificar posibles vulnerabilidades en un sistema de telecomunicaciones específico.
Establecimiento de equipo y recursos	Identificar y asignar los recursos necesarios para llevar a cabo la investigación.	Seleccionar y asignar al equipo de trabajo los recursos necesarios para realizar la investigación de manera efectiva, como herramientas de análisis de datos y software especializado.
Identificación de riesgos y restricciones	Identificar y analizar los riesgos y restricciones que puedan afectar el desarrollo de la investigación.	Evaluar los posibles riesgos y restricciones que puedan surgir durante la investigación, como la falta de acceso a determinados dispositivos o la necesidad de obtener permisos de acceso a la información.

Planificación de la investigación	Establecer un plan detallado de la investigación, incluyendo los plazos, objetivos, recursos y restricciones identificados.	Elaborar un plan detallado de la investigación, que contemple los objetivos, alcance, recursos y restricciones identificados en las etapas anteriores, con un cronograma de trabajo y fechas límite para cada tarea. Por ejemplo, establecer un plan de investigación para identificar posibles vulnerabilidades en una red de telecomunicaciones, que incluya la revisión de logs de acceso y el análisis de la configuración de dispositivos de red.

Nota: En la tabla 21 se detalla cada etapa de la fase 2 de la metodología con un ejemplo de aplicación en cada etapa, adaptado de (Internacional Organization for Standardization, 2018).

En el contexto de las telecomunicaciones, la Fase 2 de la norma ISO 27037 es esencial para garantizar que se realice una investigación rigurosa y precisa de las evidencias digitales en el marco de las buenas prácticas del perito informático. Es importante que se establezcan objetivos claros y una metodología adecuada para recopilar y analizar la información de manera efectiva, asegurando al mismo tiempo la protección de la evidencia y la privacidad de los datos de los usuarios.

4.3.7.3 Fase 3: Adquisición de la evidencia digital

La fase 3 de la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 se enfoca en la adquisición de la evidencia digital de manera forense, siguiendo una serie de pasos y principios que aseguren la integridad y autenticidad de los datos.

Esta fase incluye las siguientes etapas:

Identificación de la fuente de la evidencia: en esta etapa se debe identificar la fuente de la evidencia digital, ya sea un dispositivo de almacenamiento, red, sistema o aplicación.

Planificación de la adquisición: en esta etapa se deben definir las herramientas y técnicas de adquisición de la evidencia, así como el personal encargado de realizar la tarea.

Recolección de la evidencia: en esta etapa se procede a la recolección de la evidencia digital, siguiendo un protocolo forense para garantizar la integridad y autenticidad de los datos.

La autenticación de la evidencia digital es una etapa crucial en la adquisición de la evidencia, ya que garantiza que la misma no ha sido manipulada o alterada durante su recolección y preservación. Para llevar a cabo esta etapa, se pueden utilizar técnicas como la firma digital, el hash y la criptografía.

La firma digital se utiliza para garantizar la autenticidad e integridad de la evidencia digital. Para esto, se utiliza un certificado digital emitido por una entidad de confianza que garantiza la identidad del firmante y la integridad de la información.

El hash es una técnica criptográfica que se utiliza para garantizar que la información no ha sido modificada. El hash se calcula a partir de la información original y se compara con el hash de la información adquirida para verificar si ha habido alguna modificación.

La criptografía se utiliza para proteger la información de la evidencia digital durante la transmisión y almacenamiento. Se pueden utilizar técnicas como el cifrado de datos y la autenticación de claves para garantizar la confidencialidad e integridad de la información.

Verificación de la evidencia: en esta etapa se verifica la integridad y autenticidad de la evidencia recolectada, a través de la utilización de técnicas de validación.

La verificación de la evidencia digital es una etapa crucial en la adquisición de la misma, ya que permite asegurarse de la integridad y autenticidad de la evidencia. La verificación se realiza mediante la comparación de la evidencia adquirida con la información original, para determinar si ha habido algún tipo de alteración o modificación.

Entre las técnicas de verificación de la evidencia digital se encuentran la verificación de hash, la verificación de firmas digitales y la comparación de metadatos.

La verificación de hash consiste en calcular el valor hash de la evidencia original y compararlo con el valor hash de la evidencia adquirida. Si los valores coinciden, se puede afirmar que la evidencia adquirida es auténtica e íntegra.

La verificación de firmas digitales se utiliza para garantizar la autenticidad de la evidencia digital, ya que permite verificar que la evidencia ha sido firmada digitalmente por el propietario original. Esta técnica se basa en el uso de claves públicas y privadas para garantizar la integridad de la firma digital.

La comparación de metadatos se utiliza para verificar la autenticidad de la evidencia digital mediante la comparación de los metadatos de la evidencia adquirida con los metadatos de la evidencia original. Los metadatos incluyen información como la fecha de creación, la fecha de modificación, el tamaño del archivo, entre otros. Si los metadatos coinciden, se puede afirmar que la evidencia adquirida es auténtica e íntegra.

Almacenamiento de la evidencia: en esta etapa se debe almacenar la evidencia recolectada en un lugar seguro y controlado, garantizando la preservación de la cadena de custodia.

La etapa de Almacenamiento de la evidencia es una de las más críticas dentro de la fase de Adquisición de la evidencia digital, ya que se debe garantizar la integridad, autenticidad y confidencialidad de la evidencia digital recolectada.

Durante esta etapa se deben tomar medidas para evitar la alteración, daño o pérdida de la evidencia digital, así como establecer un adecuado registro de control de acceso y trazabilidad sobre la misma.

Es importante tener en cuenta que la evidencia digital debe ser almacenada en un ambiente controlado, seguro y libre de riesgos, y que la manipulación de la misma debe ser realizada por personal capacitado y autorizado.

En la práctica, algunas de las acciones a considerar en esta etapa son:

- Asignar un identificador único a cada evidencia recolectada.
- Almacenar la evidencia en dispositivos de almacenamiento externos, como discos duros externos, dispositivos USB o discos ópticos.
- Establecer procedimientos de copia de seguridad y recuperación de la información.
- Garantizar la confidencialidad de la información almacenada mediante el uso de medidas de seguridad, como la encriptación o el acceso restringido a la evidencia.
- Implementar medidas de control de acceso y trazabilidad para registrar las acciones realizadas sobre la evidencia, incluyendo el acceso, la manipulación y el traslado de la misma.

Documentación de la evidencia: en esta etapa se documentan todas las acciones realizadas en el proceso de adquisición de la evidencia digital, incluyendo el lugar y fecha de recolección, las herramientas y técnicas utilizadas, y el personal encargado de la tarea.

En esta etapa, se debe registrar toda la información relativa a la evidencia digital recolectada para poder establecer una cadena de custodia confiable y para poder presentar la evidencia de manera clara y coherente en un proceso legal. La documentación debe incluir información sobre el tipo de evidencia digital recolectada, la fecha y hora de la recolección, el lugar donde se encontró la evidencia, los dispositivos y herramientas utilizados para la recolección, así como cualquier otra información relevante. Es importante que la documentación sea clara, precisa y completa para evitar cualquier malentendido o confusión durante el proceso de análisis de la evidencia digital. Además, la documentación debe ser almacenada de manera segura y accesible para garantizar la integridad y la confidencialidad de la evidencia recolectada

Tabla 22:

Etapas Fase 3.

Etapa	Detalle	Aplicación práctica en telecomunicaciones
Identificación de la fuente de información	Identificar la fuente de información a examinar	Identificar el dispositivo o sistema donde se encuentra la información relevante en una investigación de fraude en una empresa de telecomunicaciones
Adquisición de la evidencia digital	Realizar una copia forense de la evidencia digital	Realizar una copia forense de los registros de llamadas en un servidor telefónico para analizar los patrones de tráfico de llamadas
Autenticación de la evidencia digital	Verificar la autenticidad y validez de la evidencia digital	Verificar la autenticidad de los correos electrónicos presentados como evidencia en una investigación de acoso en línea
Análisis de la evidencia digital	Analizar la información obtenida y extraer datos relevantes	Analizar los registros de navegación en un dispositivo móvil para determinar si se han visitado sitios web ilegales
Interpretación y correlación de la evidencia digital	Interpretar y correlacionar la información obtenida para llegar a conclusiones	Correlacionar los registros de llamadas y mensajes de texto para determinar si hubo comunicación entre dos personas en una investigación de fraude telefónico
Documentación de la evidencia digital	Documentar todo el proceso y las conclusiones obtenidas	Documentar el proceso de análisis y las conclusiones en un informe pericial presentado en un juicio relacionado con una violación de propiedad intelectual en el ámbito de las telecomunicaciones

Nota: En la tabla 22 se detalla cada etapa de la fase 3 de la metodología con un ejemplo de aplicación en cada etapa, adaptado de (Internacional Organization for Standardization, 2018).

Es importante destacar que esta fase debe ser realizada por personal capacitado y con experiencia en la adquisición de evidencia digital forense, para evitar errores y garantizar la validez de la evidencia recolectada.

4.3.7.4 Fase 4: Análisis y evaluación de la evidencia digital

La fase 4 de la metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 corresponde al análisis y evaluación de la evidencia digital recolectada en la fase anterior. En esta fase, el perito informático debe

utilizar las herramientas adecuadas para procesar y analizar la información obtenida, con el fin de extraer los datos relevantes para el caso en cuestión.

La fase 4 consta de las siguientes etapas:

Identificación de patrones y tendencias: en esta etapa se buscan patrones y tendencias que puedan ser relevantes para la investigación en curso. Se pueden utilizar herramientas de análisis de datos, como software de minería de datos, para facilitar esta tarea.

La identificación de patrones y tendencias es una de las etapas importantes en la fase de análisis y evaluación de la evidencia digital. Esta etapa se refiere al proceso de buscar patrones o tendencias en los datos para identificar relaciones y establecer conexiones. En el contexto de la investigación forense, la identificación de patrones y tendencias puede ser útil para descubrir patrones de comportamiento delictivo, identificar vínculos entre sospechosos y víctimas, y encontrar relaciones entre diferentes elementos de la evidencia.

Para llevar a cabo esta etapa, se pueden utilizar técnicas como la minería de datos, el análisis de redes sociales y el análisis de patrones. Estas técnicas pueden ayudar a identificar patrones en grandes conjuntos de datos y visualizar las relaciones entre diferentes elementos. En el contexto de las telecomunicaciones, por ejemplo, se puede utilizar la identificación de patrones y tendencias para analizar los patrones de tráfico en una red, identificar los patrones de uso de un dispositivo móvil o identificar patrones de actividad sospechosa en una cuenta de correo electrónico.

Análisis de la autenticidad de la evidencia: en esta etapa se verifica la autenticidad de la evidencia digital y se asegura que no haya sido manipulada o alterada. Se utilizan técnicas de análisis forense digital para garantizar la integridad de la información.

Para realizar este análisis, es necesario comparar la evidencia obtenida con otras fuentes de información, verificar su integridad y comprobar su consistencia. Es fundamental

mantener la cadena de custodia de la evidencia durante todo el proceso para asegurar su autenticidad.

En telecomunicaciones, el análisis de la autenticidad de la evidencia es esencial para garantizar que la información recopilada sea fiable y pueda ser utilizada en un procedimiento legal. Por ejemplo, en caso de un delito informático, la evidencia recopilada puede ser utilizada para demostrar la culpabilidad del sospechoso.

Análisis de la integridad de la evidencia: en esta etapa se verifica la integridad de la evidencia digital y se comprueba que no haya sido modificada o dañada durante la recolección o el almacenamiento. Se pueden utilizar herramientas de verificación de integridad para facilitar esta tarea.

El análisis de la integridad de la evidencia digital se refiere a la evaluación de la integridad de los datos digitales recolectados y asegurar que no han sido alterados, eliminados o manipulados. La integridad de la evidencia es crucial para la aceptación de la misma en procesos legales, ya que garantiza su autenticidad y fiabilidad.

Para llevar a cabo este análisis, se utilizan técnicas de validación y verificación de la integridad de los datos digitales, como la verificación de los hashes (resúmenes criptográficos) de los archivos, el análisis de la cadena de custodia para asegurar la integridad del proceso de recolección de la evidencia, y la verificación de las firmas digitales utilizadas para garantizar la autenticidad de los datos.

En la práctica del peritaje informático en telecomunicaciones en el Ecuador, es fundamental asegurar la integridad de la evidencia recolectada, ya que esta será utilizada en procesos legales y puede tener un impacto significativo en la resolución de casos. Por lo tanto, es necesario contar con herramientas y técnicas adecuadas para la verificación de la integridad de la evidencia digital y asegurar su validez y confiabilidad.

Análisis de la confidencialidad de la evidencia: en esta etapa se verifica que la evidencia digital se haya mantenido confidencial durante todo el proceso de investigación. Se pueden utilizar herramientas de análisis de acceso y control de permisos para verificar el cumplimiento de las políticas de seguridad y privacidad.

En la fase de análisis y evaluación de la evidencia digital, una de las tareas importantes del perito informático es el análisis de la confidencialidad de la evidencia, es decir, la evaluación de si la información recolectada está protegida adecuadamente contra accesos no autorizados.

Para llevar a cabo esta tarea, el perito debe evaluar si se han tomado medidas de seguridad adecuadas, como la utilización de contraseñas seguras y la encriptación de la información, y verificar si estas medidas han sido implementadas correctamente.

Además, el perito debe evaluar si la información ha sido divulgada a terceros sin autorización y si se ha mantenido la confidencialidad de la información durante todo el proceso de recolección y análisis.

En el contexto de las telecomunicaciones, esto es especialmente importante ya que la información transmitida a través de las redes de comunicación puede ser altamente sensible y confidencial, por lo que es necesario garantizar su protección adecuada en todo momento.

Análisis de la relevancia de la evidencia: en esta etapa se determina la relevancia de la evidencia digital para el caso en cuestión. Se evalúa la relación entre la información recolectada y las preguntas clave de la investigación para identificar las pruebas más relevantes.

Para llevar a cabo esta etapa, es importante tener una comprensión completa de las circunstancias que rodean el caso y de las preguntas que deben responderse con la evidencia. Se pueden aplicar técnicas de análisis de datos para ayudar a identificar patrones y conexiones relevantes en la evidencia.

En el contexto de la peritación informática en telecomunicaciones, la relevancia de la evidencia puede estar relacionada con la violación de la seguridad de un sistema de comunicaciones, el mal uso de la información personal, la identificación de los responsables de un delito en línea, entre otros. Es esencial que el análisis de la relevancia de la evidencia se realice de manera rigurosa y objetiva para garantizar la validez de los hallazgos.

Tabla 23:
Etapas de la fase 4.

Etapa	Detalle	Aplicación práctica en telecomunicaciones
Identificación y clasificación de la evidencia digital	Identificar la evidencia digital y clasificarla según su relevancia para el caso en cuestión.	Identificar y clasificar la evidencia digital en una investigación de fraude informático.
Extracción y preservación de la evidencia digital	Extraer la evidencia digital de los dispositivos de almacenamiento y preservarla de manera que su integridad no sea comprometida.	Extraer y preservar la evidencia digital de un dispositivo móvil en una investigación por acoso cibernético.
Análisis de la evidencia digital	Analizar la evidencia digital de manera detallada, utilizando herramientas y técnicas forenses para identificar patrones, relaciones y cualquier otro elemento relevante para el caso.	Analizar la evidencia digital en una investigación de fraude financiero en una empresa de telecomunicaciones.
Interpretación de los resultados	Interpretar los resultados obtenidos durante el análisis de la evidencia digital y determinar su relevancia para el caso.	Interpretar los resultados del análisis de la evidencia digital para determinar la culpabilidad o inocencia de un sospechoso en un caso de acoso en línea.
Elaboración del informe pericial	Elaborar un informe pericial que incluya los resultados del análisis de la evidencia digital y su interpretación, así como cualquier otra información relevante para el caso.	Elaborar un informe pericial que incluya los resultados del análisis de la evidencia digital en una investigación de un ciberataque a una empresa de telecomunicaciones.
Presentación del informe pericial	Presentar el informe pericial ante las autoridades pertinentes, explicando claramente los resultados del análisis y su interpretación.	Presentar el informe pericial en una audiencia judicial en un caso de fraude informático en una empresa de telecomunicaciones.

Nota: En la tabla 23 se detalla cada etapa de la fase 2 de la metodología con un ejemplo de aplicación en cada etapa, adaptado de (Internacional Organization for Standardization, 2018).

Análisis de la suficiencia de la evidencia: en esta etapa se determina si la cantidad y calidad de la evidencia digital recolectada es suficiente para respaldar las conclusiones y recomendaciones del informe pericial. Se pueden utilizar técnicas de análisis estadístico para medir la validez y confiabilidad de los datos obtenidos.

4.3.7.5 Fase 5: Presentación del informe de la investigación

Preparación del informe: En esta etapa se define la estructura del informe y se selecciona el formato adecuado para presentar la información de manera clara y concisa.

La preparación del informe es una etapa crucial en el proceso de investigación del perito informático en telecomunicaciones, ya que es la fase en la que se presentan los resultados de la investigación y se ofrecen recomendaciones basadas en las pruebas encontradas. Esta etapa se compone de las siguientes etapas:

1. Identificación de los destinatarios del informe: en esta etapa se debe identificar a las partes interesadas que recibirán el informe y determinar la mejor manera de comunicar los resultados a cada una de ellas.
2. Estructura del informe: en esta etapa se define la estructura del informe, incluyendo la introducción, el cuerpo del informe, las conclusiones y las recomendaciones.
3. Redacción del informe: en esta etapa se redacta el informe utilizando un lenguaje claro y conciso, evitando el uso de tecnicismos o jerga técnica que pueda ser confusa para las partes interesadas.
4. Revisión del informe: en esta etapa se realiza una revisión exhaustiva del informe para garantizar que se haya abordado adecuadamente la necesidad de investigación identificada en la Fase 1 y que el informe sea completo y coherente.

5. Presentación del informe: en esta etapa se presenta el informe a las partes interesadas y se discuten los resultados y las recomendaciones. Es importante asegurarse de que las partes interesadas comprendan claramente los resultados de la investigación y las recomendaciones ofrecidas.
6. Entrega del informe: en esta etapa se entrega el informe a las partes interesadas, se recopila cualquier retroalimentación adicional y se finaliza el proceso de investigación.

La aplicación práctica de esta etapa en telecomunicaciones puede incluir la presentación del informe a un tribunal, un cliente o una organización, donde se describen las pruebas encontradas y se hacen recomendaciones sobre cómo abordar cualquier problema identificado.

Redacción del informe: En esta etapa se redacta el informe de acuerdo a la estructura definida en la etapa anterior, incluyendo toda la información relevante obtenida durante la investigación.

Es importante que el informe sea redactado de manera objetiva y sin prejuicios, presentando únicamente los hechos y la evidencia encontrada en la investigación. Se deben incluir las fuentes utilizadas, las técnicas y herramientas empleadas en el análisis de la evidencia, así como los resultados obtenidos.

Además, se debe tomar en cuenta la privacidad y seguridad de la información en el informe, y se debe evitar divulgar información confidencial o protegida por ley sin el debido consentimiento o autorización.

Revisión del informe: En esta etapa se revisa el informe para asegurarse de que cumpla con los estándares de calidad necesarios, se hayan incluido todos los hallazgos relevantes y se hayan seguido las pautas de presentación establecidas. En esta etapa, se debe revisar y verificar que el informe sea claro, conciso, preciso y completo. Además, se debe asegurar que la información presentada sea objetiva y que las conclusiones y

recomendaciones estén respaldadas por la evidencia digital encontrada durante la investigación.

Para llevar a cabo una revisión del informe adecuada, se pueden seguir los siguientes pasos:

1. Leer el informe completo para tener una comprensión general del contenido.
2. Revisar la estructura y el formato del informe para asegurarse de que sea coherente y fácil de seguir.
3. Verificar la precisión de los detalles técnicos y los datos presentados en el informe.
4. Asegurarse de que todas las fuentes de información sean citadas adecuadamente.
5. Revisar las conclusiones y recomendaciones para asegurarse de que sean lógicas y estén respaldadas por la evidencia encontrada.
6. Corregir cualquier error gramatical o de ortografía en el informe.

Una revisión cuidadosa del informe puede ayudar a garantizar que se presente información precisa y relevante y que las conclusiones y recomendaciones sean útiles para el cliente o la institución que solicitó la investigación.

Presentación del informe: En esta etapa se presenta el informe al cliente o a la institución solicitante, y se explica claramente los hallazgos y conclusiones obtenidas durante la investigación. Para esta etapa, es importante tener en cuenta la audiencia del informe y presentar los resultados de manera clara y concisa. Algunas consideraciones importantes para la presentación del informe pueden incluir:

1. Identificar al destinatario del informe y adaptar el contenido en consecuencia.
2. Presentar los resultados de manera clara y objetiva.
3. Incluir conclusiones y recomendaciones basadas en los hallazgos.
4. Resumir los principales resultados y conclusiones en un resumen ejecutivo.
5. Presentar el informe en un formato adecuado y legible, incluyendo gráficos y tablas cuando sea necesario.

6. Considerar la privacidad y la confidencialidad de la información y asegurar que el informe se entregue de manera segura a los interesados.

En el contexto del peritaje informático en telecomunicaciones, la presentación del informe es una etapa crítica para garantizar que los resultados sean comprensibles y útiles para las partes involucradas en la investigación.

Comentarios y aclaraciones: En esta etapa se responden a cualquier comentario o pregunta que pueda tener el cliente o la institución solicitante sobre el informe presentado. Es importante que el perito esté preparado para responder a estas solicitudes y proporcionar explicaciones adicionales si es necesario. Esto puede implicar la revisión y actualización del informe original en función de los comentarios recibidos.

Por ejemplo, si el informe concluye que se ha producido una violación de datos en una empresa y se han identificado ciertos riesgos de seguridad, los destinatarios pueden solicitar más información sobre la naturaleza de la vulnerabilidad y las medidas recomendadas para abordarla. El perito informático debe estar preparado para proporcionar una explicación detallada y actualizaciones al informe según sea necesario.

Archivado del informe: En esta etapa se archiva el informe de manera segura y accesible para futuras consultas o referencias. Esto incluye el registro detallado de todas las acciones tomadas durante la investigación, la documentación de los hallazgos y las conclusiones, y la preservación de la evidencia digital recolectada.

Es importante que los datos recopilados y el informe generado sean almacenados de manera segura y confidencial, para evitar posibles alteraciones, pérdida o daño. Además, es importante que se definan claramente las políticas y procedimientos para el manejo de la información confidencial y la protección de los datos personales, para garantizar la privacidad de los afectados.

En el ámbito de las telecomunicaciones, el archivado del informe de la investigación debe cumplir con la normativa vigente en materia de protección de datos personales y de seguridad de la información. Además, es importante que se consideren las políticas internas de la empresa o institución involucrada en la investigación, para garantizar la confidencialidad y privacidad de la información recolectada.

Tabla 24:
Etapas de la fase 5.

Etapa	Detalle	Aplicación práctica en Telecomunicaciones
1. Identificación de los destinatarios del informe	Identificar a quiénes va dirigido el informe y sus necesidades específicas de información.	Identificar si el informe será entregado a un juez, un abogado, un cliente, una entidad gubernamental, etc.
2. Descripción de la metodología utilizada	Describir los procedimientos, técnicas y herramientas utilizadas en la investigación.	Detallar la metodología utilizada para adquirir, autenticar, analizar y evaluar la evidencia digital.
3. Presentación de los hallazgos	Presentar los hallazgos de la investigación de manera clara, concisa y objetiva.	Mostrar los resultados de la investigación en relación con la identificación de los problemas, las causas y las posibles soluciones.
4. Análisis de la evidencia	Presentar el análisis detallado de la evidencia digital recolectada.	Mostrar cómo se llegó a las conclusiones y recomendaciones, basadas en el análisis de la evidencia digital.
5. Conclusiones y recomendaciones	Presentar las conclusiones y las recomendaciones basadas en los hallazgos y el análisis de la evidencia digital.	Indicar las medidas correctivas necesarias para evitar futuros incidentes, recomendaciones para mejorar la seguridad y las prácticas en el manejo de la información.
6. Presentación de anexos	Incluir anexos relevantes al informe, tales como copias de la evidencia digital, documentación adicional y otros recursos.	Adjuntar la evidencia digital recolectada, junto con cualquier otra documentación relevante que sustente los hallazgos y recomendaciones.

Nota: En la tabla 25 se detalla cada etapa de la fase 5 de la metodología con un ejemplo de aplicación en cada etapa, adaptado de (Internacional Organization for Standardization, 2018).

4.3.8 Técnicas y herramientas de investigación

Las técnicas y herramientas de investigación en el ámbito de la informática forense son muy diversas y están en constante evolución debido a los avances tecnológicos. A continuación, se presentan algunas de las técnicas y herramientas más utilizadas en la investigación forense de telecomunicaciones:

Análisis de registro de llamadas: permite obtener información sobre las llamadas realizadas y recibidas desde un dispositivo de telecomunicaciones, como teléfonos móviles o fijos.

Análisis de registro de mensajes: permite obtener información sobre los mensajes enviados y recibidos desde un dispositivo de telecomunicaciones, como SMS o mensajes de chat.

Análisis de registro de datos de tráfico: permite obtener información sobre el tráfico de datos en una red de telecomunicaciones, incluyendo la información de la sesión, la duración y el volumen de datos transferidos.

Análisis de registros de ubicación: permite obtener información sobre la ubicación de un dispositivo de telecomunicaciones en un momento determinado, utilizando técnicas como el GPS o la triangulación de antenas.

Análisis de registro de actividades en línea: permite obtener información sobre las actividades en línea realizadas desde un dispositivo de telecomunicaciones, como el historial de navegación y la actividad en redes sociales.

Análisis de registro de transacciones financieras: permite obtener información sobre las transacciones financieras realizadas desde un dispositivo de telecomunicaciones, como las transferencias bancarias y las compras en línea.

Herramientas de recuperación de datos: permiten recuperar datos eliminados o dañados en dispositivos de almacenamiento de telecomunicaciones, como discos duros o tarjetas de memoria.

Herramientas de análisis de metadatos: permiten analizar los metadatos de archivos y mensajes, como la fecha y hora de creación, la ubicación y los datos del dispositivo de origen.

Herramientas de análisis de redes: permiten analizar el tráfico de red para identificar patrones y anomalías que puedan ser indicativas de actividad maliciosa.

4.3.8.1 Técnicas de recolección de evidencia digital

Las técnicas de recolección de evidencia digital son los métodos utilizados para adquirir y preservar información digital que puede ser utilizada como evidencia en una investigación. Algunas técnicas comunes incluyen:

Imágenes de disco: esta técnica se utiliza para hacer una copia exacta del disco duro o dispositivo de almacenamiento que se está investigando. Las imágenes de disco pueden ser utilizadas para preservar la integridad de la información original y pueden ser examinadas y analizadas en un entorno seguro.

Captura de red: esta técnica se utiliza para recopilar información de tráfico de red, como paquetes de datos y protocolos. Puede ser útil en investigaciones de delitos cibernéticos y en la identificación de actividad maliciosa en la red.

Extracción de archivos: esta técnica se utiliza para extraer archivos específicos de un sistema de almacenamiento. Es útil en investigaciones que requieren información específica de archivos, como correos electrónicos, documentos y archivos de registro.

Análisis de memoria: esta técnica se utiliza para adquirir y analizar la información almacenada en la memoria volátil de un sistema. Puede proporcionar información valiosa sobre actividades recientes en el sistema, incluyendo la presencia de malware o intrusiones.

Recuperación de datos borrados: esta técnica se utiliza para recuperar información que ha sido eliminada del sistema de almacenamiento. Puede ser útil en investigaciones que requieren acceso a información que ha sido borrada intencionalmente.

4.3.8.2 Herramientas para la adquisición y análisis de la evidencia digital

Existen diversas herramientas que pueden ser utilizadas por el perito informático en la adquisición y análisis de la evidencia digital. A continuación, se detallan algunas de ellas

Tabla 25:
Herramientas de adquisición y análisis.

Nombre de la herramienta	Descripción	Campo de aplicación
FTK Imager	Herramienta de adquisición de imágenes de discos y archivos	Adquisición de evidencia digital en discos duros y medios de almacenamiento similares
Autopsy	Plataforma de análisis forense digital	Análisis de evidencia digital en discos duros y medios de almacenamiento similares
Wireshark	Analizador de protocolos de red	Análisis de tráfico de red en la investigación de delitos informáticos
Xplico	Herramienta de análisis de tráfico de red	Análisis de contenido de paquetes de red para la recuperación de información en casos de delitos informáticos
Foremost	Herramienta de recuperación de datos	Recuperación de archivos eliminados o dañados en discos duros y otros medios de almacenamiento

Scalpel	Herramienta de recuperación de archivos	Recuperación de archivos eliminados o dañados en discos duros y otros medios de almacenamiento
PhotoRec	Herramienta de recuperación de datos	Recuperación de archivos eliminados o dañados en discos duros y otros medios de almacenamiento
OSForensics	Suite de análisis forense digital	Análisis de evidencia digital en discos duros y otros medios de almacenamiento
EnCase	Suite de análisis forense digital	Análisis de evidencia digital en discos duros y otros medios de almacenamiento
Volatility	Herramienta de análisis de memoria	Análisis de la memoria RAM de un sistema para identificar procesos, conexiones de red y otros detalles relevantes en la investigación de delitos informáticos
Registry Viewer	Herramienta de análisis de registro de Windows	Análisis del registro de Windows en la investigación de delitos informáticos
RegRipper	Herramienta de análisis de registro de Windows	Análisis del registro de Windows en la investigación de delitos informáticos
Bulk Extractor	Herramienta de análisis de archivos y medios digitales	Búsqueda de información confidencial en archivos y medios digitales
Guymager	Herramienta de clonación de discos	Copia de discos duros y otros medios de almacenamiento para su análisis forense
Sleuth Kit	Suite de herramientas forenses digitales	Análisis de evidencia digital en discos duros y otros medios de almacenamiento

Nota: en la tabla 25 se puede observar diferentes herramientas que son las más utilizadas existen muchas otras herramientas disponibles en el mercado para la adquisición y análisis de evidencia digital.

Es importante destacar que el perito informático debe seleccionar las herramientas adecuadas en función de la naturaleza del caso y la evidencia a analizar, y además, contar con los conocimientos y habilidades necesarias para su correcta utilización.

4.3.8.3 Análisis de la cadena de custodia

El análisis de la cadena de custodia es una técnica utilizada en la investigación forense para garantizar la integridad y autenticidad de la evidencia digital. La cadena de custodia se refiere a la documentación detallada y controlada de todas las acciones que se han realizado en relación con la evidencia, desde su recolección hasta su presentación en el tribunal.

El análisis de la cadena de custodia implica la revisión exhaustiva de los registros de la cadena de custodia para asegurarse de que no haya irregularidades o violaciones en el manejo de la evidencia. Esta técnica puede incluir la revisión de los registros de control de acceso, la documentación de transferencias y la revisión de los procedimientos de almacenamiento.

La importancia del análisis de la cadena de custodia radica en que ayuda a garantizar que la evidencia digital sea admisible en el tribunal y que se pueda confiar en su autenticidad e integridad. Además, el análisis de la cadena de custodia también puede ayudar a identificar cualquier problema en el proceso de recolección y manejo de la evidencia, lo que puede ser útil para mejorar los procedimientos en el futuro.

El procedimiento para realizar el análisis de la cadena de custodia consta de los siguientes pasos:

Identificación del origen de la evidencia es importante documentar y registrar detalladamente el lugar y momento en que se obtuvo la evidencia digital, así como la persona que la recolectó y el método utilizado.

Sellado de la evidencia la evidencia debe ser sellada en el momento de la recolección para evitar cualquier alteración o contaminación.

Registro de la evidencia se debe hacer un registro detallado de la evidencia digital recolectada, incluyendo información sobre el dispositivo de origen, la ubicación del archivo o datos, la fecha y hora de la recolección, y la persona que la recolectó.

Transporte y almacenamiento la evidencia debe ser transportada y almacenada de forma segura para garantizar su integridad y evitar cualquier manipulación no autorizada.

Análisis de la cadena de custodia se debe realizar un análisis detallado de toda la cadena de custodia, incluyendo la documentación y registro de cada paso del proceso.

Presentación en el tribunal la evidencia digital recolectada debe ser presentada en el tribunal de manera clara y concisa, con la debida documentación y registro de la cadena de custodia.

Es importante tener en cuenta que el análisis de la cadena de custodia debe ser realizado por personal capacitado y experimentado en la investigación forense digital para garantizar su validez y fiabilidad. Para un mayor control y detalle se ha generado una lista de control que se encuentra en el Anexo 1 de esta investigación

4.3.9 Consideraciones sobre Aspectos éticos y legales

4.3.9.1 Ética profesional en el trabajo del perito informático

La ética profesional es fundamental en cualquier campo de trabajo, y en el caso del perito informático no es la excepción. Al lidiar con información confidencial y sensible, el perito informático debe ser muy cuidadoso en el manejo de la evidencia digital y en su trato con las partes involucradas. A continuación, se presentan algunas consideraciones éticas relevantes para el trabajo del perito informático:

- Integridad el perito informático debe ser honesto y transparente en todo momento, y no debe manipular o alterar la evidencia digital de ninguna manera. Debe asegurarse de que toda la información sea presentada de manera objetiva y sin sesgos.

- Confidencialidad el perito informático debe mantener la confidencialidad de la información obtenida durante la investigación, y solo debe divulgarla a las partes involucradas o a terceros de confianza cuando sea necesario y permitido por la ley.
- Imparcialidad el perito informático no debe tener ningún interés personal en el resultado de la investigación, y debe realizar su trabajo de manera objetiva e imparcial. Debe basar sus conclusiones y recomendaciones en hechos y pruebas objetivas, y no en suposiciones o prejuicios personales.
- Competencia el perito informático debe contar con la capacitación y experiencia necesarias para realizar su trabajo de manera efectiva. Además, debe mantenerse actualizado en cuanto a las nuevas tecnologías y técnicas de investigación para brindar un servicio de calidad.
- Responsabilidad el perito informático debe asumir la responsabilidad de sus acciones y decisiones durante la investigación, y debe ser capaz de justificar y respaldar sus conclusiones y recomendaciones. También debe cumplir con todas las leyes y regulaciones aplicables durante el proceso.

4.3.9.2 Protección de datos personales y privacidad

La protección de datos personales y privacidad es una cuestión cada vez más importante en la sociedad actual, debido al creciente uso de las tecnologías de la información y la comunicación. La privacidad se refiere al derecho de las personas a controlar el acceso y la utilización de su información personal, mientras que la protección de datos personales se refiere a las medidas técnicas y organizativas para proteger los datos personales de su pérdida, alteración, acceso no autorizado y divulgación.

En la era digital, cada vez se recopila más información personal de las personas, ya sea a través de redes sociales, compras en línea, registros de salud o de actividades en línea, entre otros. Esta información puede incluir datos personales sensibles, como la información médica, la orientación sexual, la religión y las opiniones políticas. Por lo tanto, la protección

de datos personales y la privacidad son fundamentales para garantizar la dignidad humana, la libertad y la autonomía.

La protección de datos personales también es importante para prevenir el uso indebido de la información personal, como la identidad robada o la suplantación de identidad. Además, es importante proteger la información personal de los niños y los jóvenes, quienes pueden ser especialmente vulnerables a la manipulación y el acoso en línea.

La protección de datos personales y la privacidad son fundamentales para garantizar el respeto de los derechos humanos, la privacidad y la seguridad de las personas. Los peritos informáticos deben asegurarse de cumplir con los estándares éticos y legales de protección de datos personales y privacidad en el curso de su trabajo.

4.3.9.3 Consideraciones legales en la investigación de delitos informáticos

La investigación de delitos informáticos está sujeta a diversas consideraciones legales y normativas que deben ser tomadas en cuenta por el perito informático. En muchos países, la investigación de delitos informáticos se rige por leyes específicas que establecen los procedimientos y requisitos que deben seguirse para la recolección, preservación y presentación de evidencia digital en un juicio.

Algunas de las principales consideraciones legales en la investigación de delitos informáticos incluyen:

La necesidad de contar con una orden judicial En muchos casos, los peritos informáticos necesitan una orden judicial para poder investigar y recolectar evidencia digital. Esto se debe a que la recolección de información personal y privada sin una orden judicial puede violar las leyes de protección de datos y privacidad.

Las leyes de protección de datos y privacidad: Los peritos informáticos deben tener en cuenta las leyes y regulaciones que protegen la privacidad y los datos personales de los

individuos. Esto significa que la recolección, almacenamiento y uso de información personal debe hacerse de acuerdo con estas leyes y regulaciones.

Las leyes de propiedad intelectual La investigación de delitos informáticos a menudo implica la recolección y análisis de información protegida por leyes de propiedad intelectual, como patentes, derechos de autor y marcas registradas. Los peritos informáticos deben asegurarse de que la recolección y uso de esta información se haga de acuerdo con las leyes de propiedad intelectual.

Las leyes de interceptación de comunicaciones En muchos países, la interceptación de comunicaciones está prohibida sin una orden judicial. Los peritos informáticos deben asegurarse de que cualquier interceptación de comunicaciones se haga de acuerdo con las leyes y regulaciones pertinentes.

El cumplimiento de las normas y estándares de la industria Los peritos informáticos deben seguir las mejores prácticas de la industria y cumplir con los estándares y normas aplicables. Esto puede incluir la adhesión a las normas ISO para la recolección y preservación de evidencia digital.

4.4 Validación de la metodología

La validación de la metodología propuesta se llevará a cabo mediante el análisis de las respuestas obtenidas del cuestionario tipo Likert de 5 puntos diseñado para expertos peritos informáticos. Para ello, se aplicará un análisis estadístico descriptivo de las respuestas obtenidas, con el fin de determinar el grado de acuerdo de los expertos con respecto a los diferentes aspectos de la metodología propuesta.

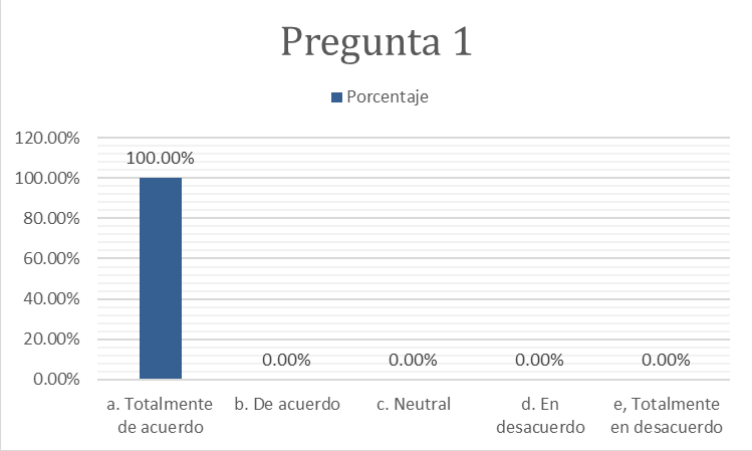
Pregunta 1: ¿La metodología propuesta es clara y fácil de entender?

Tabla 26:
Resultados pregunta 1 cuestionario de validación.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	8	100.00%
b. De acuerdo	0	0.00%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 26 se aprecian los resultados de la pregunta 1 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Figura 22: Resultados pregunta 1 cuestionario de validación.



Nota: En la figura 22 se aprecian los resultados de la pregunta 1 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Análisis

La respuesta a la pregunta 1 del cuestionario de validación indica que el 100% de los expertos peritos informáticos encuestados están totalmente de acuerdo en que la metodología

propuesta es clara y fácil de entender. Este resultado sugiere que la metodología desarrollada es fácilmente comprensible para los expertos y cumple con el objetivo de ser una guía clara y accesible para la realización de buenas prácticas en la investigación de evidencia digital en el ámbito de las telecomunicaciones. Este resultado es muy positivo, ya que demuestra que la metodología ha sido diseñada de forma clara y efectiva, y que puede ser utilizada por los expertos en la materia sin dificultades.

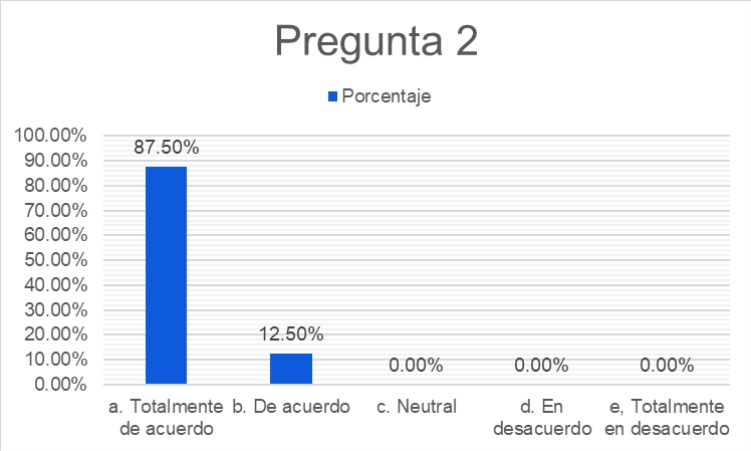
Pregunta 2: La metodología propuesta es completa y abarca todos los aspectos relevantes para la investigación de delitos informáticos en el ámbito de las telecomunicaciones.

Tabla 27:
Resultados pregunta 2 cuestionario de validación.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	7	87.50%
b. De acuerdo	1	12.50%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 27 se aprecian los resultados de la pregunta 2 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Figura 23: Resultados pregunta 2 cuestionario de validación.



Nota: En la figura 23 se aprecian los resultados de la pregunta 2 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Análisis

La respuesta a la pregunta 1 del cuestionario de validación indica que el 100% de los expertos peritos informáticos encuestados están totalmente de acuerdo en que la metodología propuesta es clara y fácil de entender. Este resultado sugiere que la metodología desarrollada es fácilmente comprensible para los expertos y cumple con el objetivo de ser una guía clara y accesible para la realización de buenas prácticas en la investigación de evidencia digital en el ámbito de las telecomunicaciones. Este resultado es muy positivo, ya que demuestra que la metodología ha sido diseñada de forma clara y efectiva, y que puede ser utilizada por los expertos en la materia sin dificultades.

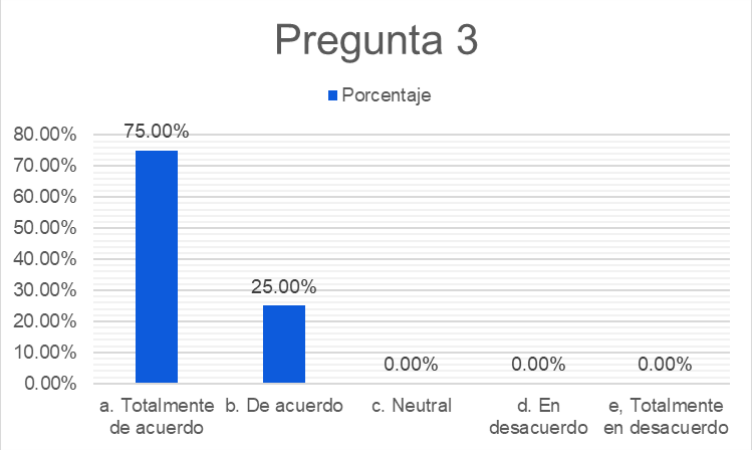
Pregunta 3: La metodología propuesta incluye las mejores prácticas de la norma ISO 27037 y su aplicación en el contexto ecuatoriano.

Tabla 28:
Resultados pregunta 3 cuestionario de validación.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	6	75.00%
b. De acuerdo	2	25.00%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 28 se aprecian los resultados de la pregunta 3 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Figura 24: Resultados pregunta 3 cuestionario de validación.



Nota: En la figura 24 se aprecian los resultados de la pregunta 3 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Análisis

Según la tabla de resultados, la pregunta 3 obtuvo una calificación promedio de 4.75 puntos, lo que indica que la mayoría de los expertos peritos informáticos están de acuerdo en que la metodología propuesta incluye las mejores prácticas de la norma ISO 27037 y su aplicación en el contexto ecuatoriano. El 75% de los encuestados están totalmente de acuerdo

y el 25% están de acuerdo, lo que sugiere que la metodología propuesta es relevante y se adapta adecuadamente a la normativa y el contexto local. Sin embargo, se debe tener en cuenta que se trata de una muestra limitada de expertos y que la validación de la metodología debería incluir la opinión de un conjunto más amplio de expertos en el campo de la investigación de delitos informáticos en el ámbito de las telecomunicaciones.

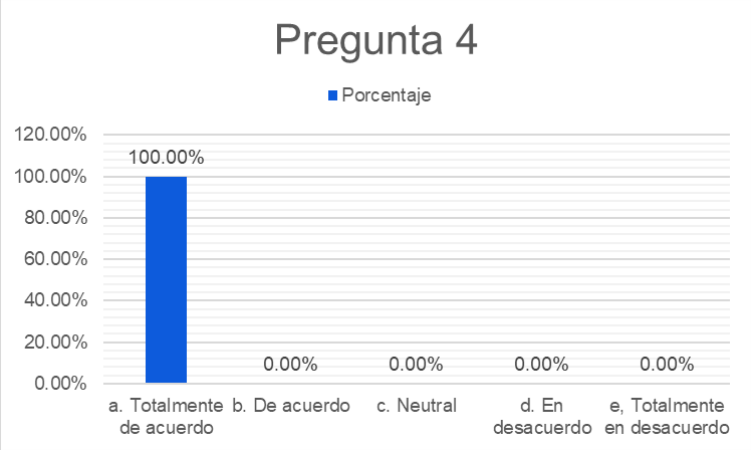
Pregunta 4: La metodología propuesta es aplicable en la práctica y en el campo de trabajo de un perito informático en el ámbito de las telecomunicaciones.

Tabla 29:
Resultados pregunta 4 cuestionario de validación.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	8	100.00%
b. De acuerdo	0	0.00%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 29 se aprecian los resultados de la pregunta 4 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Figura 25: Resultados pregunta 4 cuestionario de validación.



Nota: En la figura 25 se aprecian los resultados de la pregunta 4 del cuestionario de validación de la metodología , fuente Cuestionario de validación Metodología (2022)

Análisis

La pregunta 4 del cuestionario de validación obtuvo una frecuencia de 8 respuestas "Totalmente de acuerdo", lo que representa un porcentaje del 100%. Esto indica que los expertos peritos informáticos consideran que la metodología propuesta es aplicable en la práctica y en el campo de trabajo de un perito informático en el ámbito de las telecomunicaciones. Estos resultados sugieren que la metodología es considerada efectiva y útil por parte de los expertos, lo que fortalece la validez y confiabilidad de la misma.

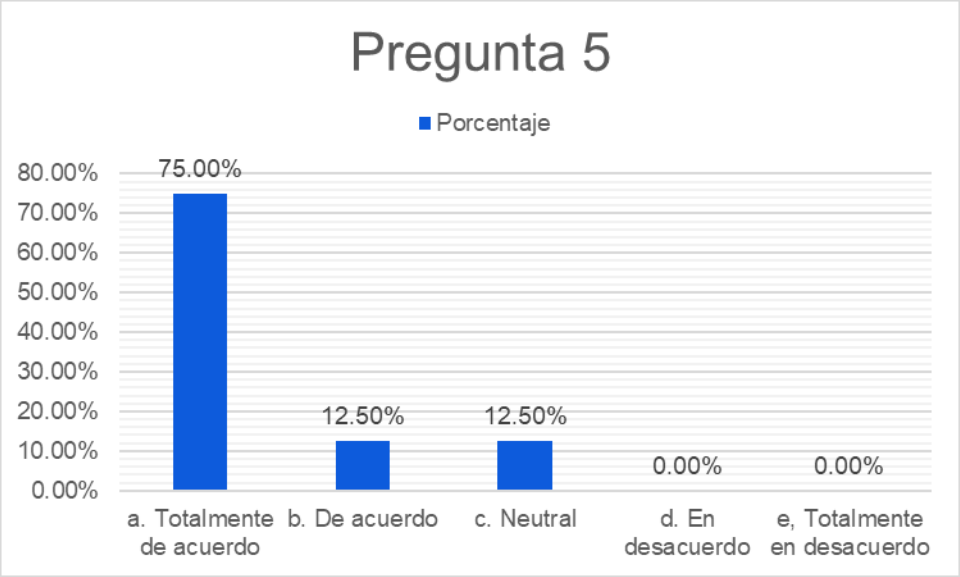
Pregunta 5: La metodología propuesta ayudará a mejorar la calidad de las investigaciones de delitos informáticos en el ámbito de las telecomunicaciones en Ecuador.

Tabla 30:
Resultados pregunta 5 cuestionario de validación.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	6	75.00%
b. De acuerdo	1	12.50%
c. Neutral	1	12.50%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 30 se aprecian los resultados de la pregunta 5 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Figura 26: Resultados pregunta 5 cuestionario de validación.



Nota: En la figura 26 se aprecian los resultados de la pregunta 5 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Análisis

En la pregunta 5 del cuestionario de validación, se obtuvo una respuesta mayoritaria de acuerdo y totalmente de acuerdo, representando el 87.5% de las respuestas. No obstante, se evidenció un 12.5% de respuestas neutrales, lo que indica que aún existen algunos peritos informáticos que no están seguros sobre el impacto de la metodología en la calidad de las investigaciones de delitos informáticos en el ámbito de las telecomunicaciones en Ecuador. Por lo tanto, se sugiere que se realicen más acciones de difusión y capacitación para que los peritos informáticos puedan entender de manera más clara y completa cómo la metodología propuesta puede contribuir a mejorar la calidad de sus investigaciones.

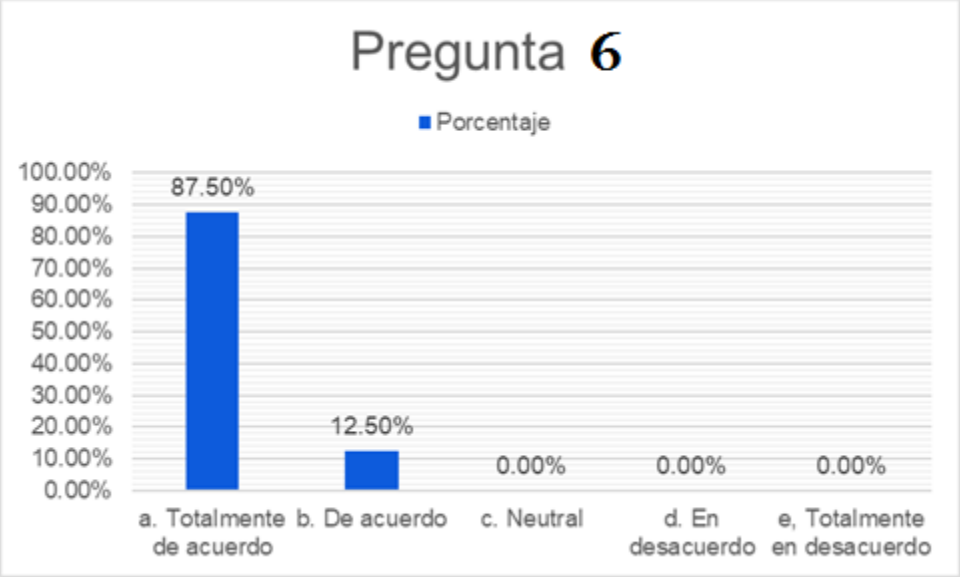
Pregunta 6: En general, ¿recomendaría la metodología propuesta a otros peritos informáticos en el ámbito de las telecomunicaciones en Ecuador?

Tabla 31:
Resultados pregunta 6 cuestionario de validación.

Respuesta	Frecuencia	Porcentaje
a. Totalmente de acuerdo	7	87.50%
b. De acuerdo	1	12.50%
c. Neutral	0	0.00%
d. En desacuerdo	0	0.00%
e, Totalmente en desacuerdo	0	0.00%
TOTAL	8	100.00%

Nota: En la tabla 31 se aprecian los resultados de la pregunta 6 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Figura 27: Resultados pregunta 6 cuestionario de validación.



Nota: En la figura 27 se aprecian los resultados de la pregunta 6 del cuestionario de validación de la metodología, fuente Cuestionario de validación Metodología (2022)

Análisis

Según los resultados presentados en la tabla 31, el 87.5% de los expertos peritos informáticos que participaron en la validación recomendarían la metodología propuesta a otros peritos informáticos en el ámbito de las telecomunicaciones en Ecuador, y el 12.5% restante estaría de acuerdo con hacerlo. Esto sugiere que la metodología diseñada y propuesta puede ser útil y relevante para los peritos informáticos en este contexto específico, lo que representa una importante contribución para el mejoramiento de las investigaciones de delitos informáticos en el país. Sin embargo, se debe tener en cuenta la opinión de otros expertos y la implementación práctica de la metodología para realizar una evaluación más completa de su efectividad y relevancia en el campo.

4.4.1 Análisis general de la encuesta de validación

El cuestionario de validación de la metodología diseñada para buenas prácticas del perito informático de telecomunicaciones en Ecuador, permitió recopilar información de expertos peritos informáticos en relación a la claridad, aplicabilidad y recomendación de la metodología propuesta.

En general, los resultados indicaron que los expertos peritos informáticos estuvieron de acuerdo en que la metodología propuesta es clara, completa y abarca todos los aspectos relevantes para la investigación de delitos informáticos en el ámbito de las telecomunicaciones. Asimismo, destacaron que la metodología incluye las mejores prácticas de la norma ISO 27037 y su aplicación en el contexto ecuatoriano.

En cuanto a la aplicabilidad, los resultados indicaron que la metodología propuesta es aplicable en la práctica y en el campo de trabajo de un perito informático en el ámbito de las telecomunicaciones. Esto sugiere que la metodología es una herramienta útil para los peritos informáticos y puede ayudarles en su trabajo diario en la investigación de delitos informáticos.

Los resultados también indican que la metodología propuesta ayudará a mejorar la calidad de las investigaciones de delitos informáticos en el ámbito de las telecomunicaciones en Ecuador. Esto sugiere que la metodología puede tener un impacto positivo en la calidad de las investigaciones de delitos informáticos en el país.

Por último, los resultados indicaron que la mayoría de los expertos peritos informáticos recomendarían la metodología propuesta a otros peritos informáticos en el ámbito de las telecomunicaciones en Ecuador. Esto sugiere que la metodología es vista como una herramienta útil y valiosa para la comunidad de peritos informáticos en el país.

Se puede indicar el análisis del cuestionario de validación de la metodología diseñada para buenas prácticas del perito informático de telecomunicaciones en Ecuador, permitió obtener información valiosa de expertos peritos informáticos sobre la claridad, aplicabilidad y recomendación de la metodología propuesta. Los resultados sugieren que la metodología es una herramienta útil y valiosa para los peritos informáticos en el país y puede ayudarles en su trabajo diario en la investigación de delitos informáticos en el ámbito de las telecomunicaciones.

5. CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Luego de realizar un análisis exhaustivo del marco legal vigente para el análisis y revisión de la normativa ISO 27037, se ha concluido que existe una necesidad imperante de incorporar estas normas y buenas prácticas en el ámbito de las investigaciones de delitos informáticos en el sector de las telecomunicaciones en Ecuador. La normativa ISO 27037 proporciona un marco de referencia sólido y completo para la recolección, preservación, análisis y presentación de la evidencia digital, lo que puede mejorar significativamente la calidad y eficacia de las investigaciones en este ámbito. Además, el análisis del marco legal vigente ha permitido identificar vacíos y lagunas en la normativa local, lo que sugiere la necesidad de actualizar y fortalecer la legislación para abordar de manera adecuada los desafíos que plantea la tecnología en la lucha contra el delito informático.
- La verificación del campo de acción, ámbito de aplicación, hardware, software y evidencias digitales fue un paso fundamental en este proyecto, ya que permitió tener un panorama claro y preciso de lo que implica la investigación de delitos informáticos en el ámbito de las telecomunicaciones en Ecuador. La identificación de los dispositivos y sistemas tecnológicos involucrados en estos delitos y la recopilación de las posibles fuentes de evidencia digital fueron fundamentales para poder diseñar una metodología que abarque todos los aspectos relevantes de esta práctica. La validación de esta verificación por parte de los expertos peritos informáticos a través del cuestionario de validación, en el cual se obtuvieron resultados positivos, ratifica la importancia de este paso para la investigación de delitos informáticos y la relevancia de una metodología adecuada para abordar este

tipo de casos. En conclusión, la verificación del campo de acción, ámbito de aplicación, hardware, software y evidencias digitales es un paso fundamental para el diseño de una metodología de investigación adecuada para delitos informáticos en el ámbito de las telecomunicaciones en Ecuador.

- Una de las conclusiones importantes que se puede obtener de la elaboración de la metodología para peritos informáticos en el ámbito de las telecomunicaciones en Ecuador bajo las normas de las buenas prácticas de la norma ISO 27037, es que se logró establecer un proceso estandarizado para la recolección, preservación, análisis y presentación de la evidencia digital en las investigaciones de delitos informáticos. La metodología ofrece una guía clara y precisa para los peritos informáticos, con instrucciones detalladas sobre cómo manejar la evidencia digital de manera adecuada, asegurando su integridad y autenticidad.
- La encuesta realizada a los expertos peritos informáticos permitió validar que la metodología propuesta es clara, fácil de entender y aplicable en la práctica y en el campo de trabajo de un perito informático en el ámbito de las telecomunicaciones. Además, se confirmó que la metodología propuesta incluye las mejores prácticas de la norma ISO 27037 y su aplicación en el contexto ecuatoriano. De esta manera, se puede concluir que se logró cumplir con el objetivo específico de elaborar la metodología para los peritos informáticos que se aplicaría bajo las normas de las buenas prácticas de la norma ISO 27037.
- Se logró cumplir con los objetivos específicos planteados y se diseñó una metodología para buenas prácticas del perito informático de Telecomunicaciones en Ecuador, con base en la norma ISO 27037. La metodología propuesta fue validada por expertos peritos informáticos, lo que permite asegurar que es una herramienta útil y aplicable en la práctica, por lo que se considera que el proyecto cumple con los objetivos planteados y que la metodología propuesta es una herramienta valiosa para la realización de

investigaciones de delitos informáticos en el ámbito de las telecomunicaciones en Ecuador, cumpliendo con los estándares internacionales de calidad y las mejores prácticas establecidas en la norma ISO 27037.

- La metodología también proporciona un enfoque sistemático para la investigación de delitos informáticos, que ayuda a garantizar que se cumplan los requisitos legales y éticos. Además, la metodología incorpora las mejores prácticas de la norma ISO 27037, lo que asegura que los peritos informáticos estén aplicando los estándares internacionales y manteniendo la calidad y precisión de las investigaciones.
- La elaboración de la metodología también permitió un análisis exhaustivo de los diferentes aspectos que involucra una investigación de delitos informáticos, como el campo de acción, ámbito de aplicación, hardware, software y evidencias digitales. Estos aspectos son críticos en cualquier investigación de delitos informáticos, y la metodología desarrollada garantiza que se consideren todos estos factores y se manejen de manera adecuada.

5.2 Recomendaciones

- Actualización periódica de la metodología: Debido a la constante evolución de las tecnologías y las amenazas informáticas, se recomienda una revisión y actualización periódica de la metodología propuesta para asegurar su relevancia y aplicabilidad en el contexto actual.
- Capacitación continua para peritos informáticos: Los peritos informáticos deben recibir capacitación continua para mantenerse actualizados sobre las últimas tecnologías, amenazas y técnicas de investigación para garantizar que estén en capacidad de aplicar correctamente la metodología propuesta.
- Aplicación de la metodología en casos reales: Es importante que la metodología sea aplicada en casos reales para evaluar su efectividad y hacer mejoras donde sea necesario. Se recomienda fomentar la colaboración con las autoridades encargadas de investigar delitos informáticos en el país para poder realizar estas aplicaciones.
- Investigación sobre el impacto de la metodología en la resolución de casos: Se recomienda llevar a cabo estudios sobre la efectividad de la metodología propuesta en la resolución de casos de delitos informáticos en el ámbito de las telecomunicaciones en Ecuador.
- Fortalecimiento del marco legal para delitos informáticos: Se sugiere un fortalecimiento del marco legal para delitos informáticos en el país para que las investigaciones puedan ser más efectivas y para que la aplicación de la metodología propuesta pueda ser más eficiente.
- Fomentar la investigación en el área de la ciberseguridad: Dado el constante aumento de las amenazas informáticas, es necesario fomentar la investigación en el área de la ciberseguridad, tanto a nivel académico como a nivel práctico, para poder mejorar las herramientas y técnicas de investigación disponibles para los peritos informáticos.

6. REFERENCIAS

Anahy, M., & Montes De Oca, P. (2021). Propuesta de investigación: Modelo de análisis forense digital para el sistema de negociación electrónico de la Bolsa Boliviana de Valores, basado en la Norma ISO/IEC 27037:2012. *INF-FCPN-PGI Revista PGI*, 128–130. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/68

Anampa, R., Dudu, B., Agüero, V., & Martin, J. (2021). *ISO 27037: 2012 en la mejora del análisis forense en la empresa DG Service, Lima 2021*. https://repositorio.ucv.edu.pe/handle/20.500.12692/70930

Asamblea Nacional. (2014). Ley de Propiedad Intelectual . *Registro Oficial* .

Asamblea nacional. (2021). Ley Orgánica de Protección de Datos Personales . *Registro Oficial* .

Asamblea Nacional del Ecuador. (2008). *CONSTITUCIÓN DEL ECUADOR*.

Asamblea Nacional del Ecuador. (2015). Ley Orgánica de Telecomunicaciones. *Idata.Ec*. https://idata.ec/wp-content/uploads/2023/01/telecomunicaciones.pdf

Astudillo, E. (2020). *Ciberdelitos aumentan durante la emergencia*.

Avila, E. (2019). *PRIMICIAS*.

Bahadur, P. (2015). *Computer Forensics – Digitized Science*. 1025–1031.

Bolaños-Burgos, F. (2016). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. *Estudio Cualitativo de La Relación de Las Leyes y La Pericia Informática En El Ecuador*, *4*(3).

Brocca, M. (2018). *¿Cómo adaptar tu negocio al nuevo RGPD europeo 2018?* El Blog de José Facchin. https://josefacchin.com/rgpd/

Cabero, J., Romero, R., & Palacios, A. (2020). Evaluation of teacher digital competence frameworks through expert judgement: The use of the expert competence coefficient. *Journal of New Approaches in Educational Research*, *9*(2), 275–283. https://doi.org/10.7821/NAER.2020.7.578

Cámara-Valencia. (2018). *La ciberseguridad en cifras: los datos muestran incremento en la preocupación empresarial*. https://ticnegocios.camaravalencia.com/servicios/tendencias/la-ciberseguridad-en-cifras-los-datos-muestran-incremento-en-la-preocupacion-empresarial/

Casey, E. (2019). The chequered past and risky future of digital forensics. *Https://Doi.Org/10.1080/00450618.2018.1554090*, *51*(6), 649–664. https://doi.org/10.1080/00450618.2018.1554090

Chávez, J. (2020). *Evidenciar el análisis forense en equipos y dispositivos móviles con sistema operativo android utilizando herramientas de peritaje informático para el Colegio Francisco Arizaga Luque ubicado en la Ciudad de Guayaquil*. http://repositorio.ug.edu.ec/handle/redug/48800

Choi, J., Yu, J., Hyun, S., & Kim, H. (2019). Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger. *Digital Investigation*, *28*, S50–S59. https://doi.org/10.1016/J.DIIN.2019.01.011

Codigo Organico Integral Penal, Noticias 268 (2018).

Congreso Nacional del Ecuador. (2002). Ley de Comercio Electrónico, Firmas Electrónicas y mensajes de datos. *Registro Oficial*. https://www.rmpplayas.gob.ec/wp-content/uploads/2023/04/LCEFEYMD-MARZO.pdf

Costa Carballo, C. (1998). Los orígenes de la informática. *Revista General de Información y Documentación*, *8*(1), 215–262. https://doi.org/10.5209/RGID.11668

Dirección Nacional de Registros Públicos. (2021). *Ley de Protección de Datos Personales* . Registro Oficial. https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Elaine, C. (2022). *Evaluación de herramientas para el proceso de generación de informes en el ámbito de la informática legal basado en la norma ISO 27037: 2012*. https://repositorio.pucese.edu.ec/handle/123456789/3034

Ferruzola Gomez, E. C., & Cuenca Espinoza, H. A. (2015). Cómo responder a un Delito Informático. *Ciencia Unemi*, *7*(11), 43. https://doi.org/10.29076/issn.2528-7737vol7iss11.2014pp43-50p

García, J. (2015). *Informe sobre el Peritaje Informático*. 1–65.

Gonzáles, J. A., & Gallardo, M. C. (2021). *Diseño y metodología de la investigación*. http://repositorio.concytec.gob.pe/handle/20.500.12390/2260

González, J., Bermeo, J., Villacreses, E., & Guerrero, J. (2018). *DELITOS INFORMÁTICOS: UNA REVISIÓN EN LATINOAMÉRICA*. MACHALA.

Google. (2022). *Requisitos para usar Google Meet - Ayuda de Google Meet*. https://support.google.com/meet/answer/7317473?hl=es-419#zippy=%2Cusa-un-sistema-operativo-compatible%2Crecomendaciones-de-hardware

Haque, M. M., & Hossain, S. A. (2018). National digital forensics framework for Bangladesh. *3rd International Conference on Electrical Information and Communication Technology, EICT 2017*, *2018-Janua*(December), 1–6. https://doi.org/10.1109/EICT.2017.8275133

Hernández-Sampieri, R., & Collado, C. F. (2018a). *Metodología de la investigación*. https://dspace.scz.ucb.edu.bo/dspace/bitstream/123456789/21401/1/11699.pdf

Hernández-Sampieri, R., & Collado, C. F. (2018b). *Metodología de la investigación*. https://dspace.scz.ucb.edu.bo/dspace/bitstream/123456789/21401/1/11699.pdf

Huichalaf, P. (2014). *Desarrollo de las Telecomunicaciones en Chile*.

International Organization for Standardization. (2018). *ISO - ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. https://www.iso.org/standard/44381.html

International Organization for Standardization. (2020). *ISO - ISO/IEC 27050-1:2019 - Information technology — Electronic discovery — Part 1: Overview and concepts*. https://www.iso.org/standard/78647.html

International Organization for Standardization. (2022). *ISO 27001:2022 Update*.

Ishtiaq, M. (2019). Book Review Creswell, JW (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches . Thousand Oaks, CA: Sage. *Academia.Edu*. https://www.academia.edu/download/72214301/Ishtiaq_2019.pdf

Majed, H., Noura, H. N., & Chehab, A. (2020). *Overview of Digital Forensics and Anti-Forensics Techniques*. 1–5. https://doi.org/10.1109/isdfs49300.2020.9116399

Marín, F., Pérez, J., Senior, A., & García, J. (2021). Validación del diseño de una red de cooperación científico-tecnológica utilizando el coeficiente K para la selección de expertos. *Información Tecnológica*, *32*(2), 79–88. https://doi.org/10.4067/S0718-07642021000200079

Navarro Clérigues, J. (2015). *Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico*. 148.

Overill, R. E., & Collie, J. (2021). Quantitative evaluation of the results of digital forensic investigations: a review of progress. *Forensic Sciences Research*, *6*(1), 13–18. https://doi.org/10.1080/20961790.2020.1837429

Pino, S. A. del. (2012). Delitos Informáticos: Generalidades. *Universidad Católica de Ecuador*, 1–67.

Pizarro, O. R. (2018). Peritaje forense y responsabilidad del perito. *Revista CONAMED*, *9*(4), 16–18.

Plan Nacional de Desarrollo. (2017). *Plan de Desarrollo*.

Poma, M. (2019). *Análisis de derecho comparado del perito informático*. https://reunir.unir.net/handle/123456789/10877

Real Academia Española. (2021). *Definición | Diccionario de la lengua española | RAE - ASALE*. https://dle.rae.es/principio

Rosero, D. S. (2019). *Diseño de una metodología de recolección de evidencia digital para análisis forense de unidades de disco duro, basada en la norma ISO/IEC 27037:2012*. http://localhost:8080/xmlui/handle/123456789/3609

Roy, S., Wu, Y., & LaVenia, K. N. (2019). Experience of incorporating NIST standards in a digital forensics curricula. *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, 1–6. https://doi.org/10.1109/ISDFS.2019.8757533

Sampaoli, J. (2018). *Peritaje informático: marco teórico-practico*.

Sampaoli, J. A., & Bender, C. (2018). *Peritaje informático : marco teórico-practico*. https://repositorio.uca.edu.ar/handle/123456789/523

Subijana, I. J., & Echeburúa, E. (2021). El Conflicto de Roles con respecto a la Prueba Pericial Psicológica en el Proceso Judicial. *Https://Journals.Copmadrid.Org/Apj*, *32*(1), 107–114. https://doi.org/10.5093/APJ2021A22

Toscano, F. (2018). *Metodología de la Investigación*. https://books.google.com.ec/books?hl=es&lr=&id=2RFaDwAAQBAJ&oi=fnd&pg=PA13&dq=Metodolog%C3%ADa+de+la+Investigaci%C3%B3n&ots=Lti7xsER_n&sig=47VpRB5R5N2F255uKRbFvcSeie4

Vaca, M. (2017). *EL HACKER COMO SUJETO ACTIVO EL DELITO: LIMITES Y EXCEPCIONES DE LA INTROMISION TECNOLÓGICA A LA RED DE INTERNET A LA LUZ DEL CÓDIGO ÓRGANICO INTEGRAL PENAL (COIP)"*. PUCE.

Veber, J., Smutný, Z., & Vyskočil, L. (2015). Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012. *Acta Informatica Pragensia*, *4*(3), 242–257. https://doi.org/10.18267/J.AIP.72

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*(2), 183–194. https://doi.org/10.1080/15614263.2015.1128163

Wen, L. (2017). Research on system design and implementation of computer forensics based on log. *Proceedings - 2017 International Conference on Computer Technology, Electronics and Communication, ICCTEC 2017*, *67*, 388–391. https://doi.org/10.1109/ICCTEC.2017.00090

7. ANEXOS

Anexo I Lista de chequeo para procedimiento de cadena de custodia

Etapa	Descripción	Realizado o No	Observaciones
1. Identificación de la evidencia y registro de la cadena de custodia inicial	1.1 Identificar la evidencia y su ubicación		
	1.2 Registrar el número de la evidencia		
	1.3 Registrar la fecha y hora de la adquisición		
	1.4 Registrar el nombre del adquiriente		
	1.5 Registrar las condiciones de la evidencia		
2. Protección de la evidencia	2.1 Asegurarse de que la evidencia esté en un lugar seguro		
	2.2 Asegurarse de que la evidencia no sufra daños físicos		
	2.3 Asegurarse de que la evidencia no sea alterada		
3. Transporte de la evidencia	3.1 Asegurarse de que la evidencia esté debidamente embalada		
	3.2 Asegurarse de que la cadena de custodia esté intacta durante el transporte		
	3.3 Asegurarse de que la evidencia llegue al destino final sin sufrir daños físicos		
4. Recepción de la evidencia	4.1 Verificar la integridad de la cadena de custodia		
	4.2 Registrar la fecha y hora de la recepción		
	4.3 Asegurarse de que la evidencia no haya sido alterada		
5. Almacenamiento de la evidencia	5.1 Asegurarse de que la evidencia esté en un lugar seguro y protegido		
	5.2 Asegurarse de que la evidencia no sufra daños físicos o ambientales		
	5.3 Asegurarse de que la evidencia no sea alterada		
6. Transferencia de la evidencia	6.1 Asegurarse de que la cadena de custodia esté intacta durante la transferencia		

	6.2 Registrar la fecha y hora de la transferencia		
	6.3 Registrar el nombre de la persona que recibe la evidencia		
	6.4 Asegurarse de que la evidencia no sufra daños físicos o ambientales durante la transferencia		
7. Devolución de la evidencia	7.1 Asegurarse de que la evidencia sea devuelta al propietario original o al destinatario adecuado		
	7.2 Registrar la fecha y hora de la devolución		
	7.3 Asegurarse de		

Anexo II Control de la fase 1

Etapa	Descripción	Realizado (Sí/No)	Observaciones
1	Identificar la necesidad de realizar una investigación		
2	Definir el objetivo de la investigación y los problemas a resolver		
3	Identificar las fuentes de información y los recursos necesarios para la investigación		
4	Identificar las restricciones legales y éticas aplicables a la investigación		
5	Evaluar la factibilidad de la investigación		
6	Documentar los resultados de esta etapa en un plan de investigación		

Anexo III: Control Fase 2

Etapa	Descripción	Realizado o No	Observaciones
Identificación del objeto de la investigación	Identificar el objetivo específico de la investigación.		
	Identificar la información necesaria para llevar a cabo la investigación.		
	Identificar los posibles riesgos que puedan afectar la investigación.		
Diseño de la investigación	Determinar la estrategia de la investigación.		
	Establecer el plan de recolección de datos.		
	Seleccionar la técnica de análisis de la evidencia digital.		
	Definir el calendario de la investigación.		
	Identificar los recursos necesarios para llevar a cabo la investigación.		
	Identificar los posibles riesgos que puedan afectar la investigación.		
Preparación de la investigación	Asegurarse de que se cuenta con las autorizaciones necesarias para llevar a cabo la investigación.		
	Designar al equipo responsable de la investigación.		
	Identificar el lugar de trabajo y los equipos necesarios para la investigación.		
	Asegurarse de que los equipos estén debidamente configurados y listos para su uso.		
	Realizar pruebas previas de los equipos y herramientas a utilizar en la investigación.		
	Realizar una evaluación previa de los posibles riesgos que puedan afectar la investigación.		

Anexo IV Control Fase 3

Etapa	Descripción	Realizado o no	Observaciones
Establecer los objetivos de la adquisición de la evidencia digital	Identificar los tipos de evidencia digital necesarios para el caso		
	Definir los dispositivos de almacenamiento de datos a examinar		
	Establecer los procedimientos de adquisición de la evidencia digital		
	Preparar los dispositivos para la adquisición de la evidencia digital		
Verificar la integridad de los dispositivos de almacenamiento de datos	Realizar una copia forense de los dispositivos de almacenamiento de datos		
	Verificar la integridad de las copias forenses		
Transportar y almacenar la evidencia digital adquirida	Realizar el traslado de la evidencia digital adquirida al lugar de almacenamiento		
	Almacenar la evidencia digital en un lugar seguro y controlado		
	Verificar que la cadena de custodia de la evidencia digital se mantiene en todo momento		

Anexo V Control Fase 4

Etapa	Descripción	Realizado (Sí/No)	Observaciones
Identificación de patrones y tendencias	Identificar patrones y tendencias significativas en la evidencia digital.		
Análisis de la autenticidad de la evidencia	Verificar la autenticidad de la evidencia digital.		
Análisis de la integridad de la evidencia	Verificar la integridad de la evidencia digital.		
Análisis de la confidencialidad de la evidencia	Verificar la confidencialidad de la evidencia digital.		
Análisis de la relevancia de la evidencia	Determinar la relevancia de la evidencia digital en relación a la investigación.		
Análisis de la suficiencia de la evidencia	Determinar si la evidencia digital es suficiente para apoyar la investigación.		

Anexo VI Control Fase 5

Etapa	Descripción	Realizado o no	Observaciones
Preparación del informe	Revisión y organización de los hallazgos y conclusiones en un informe		
Redacción del informe	Redacción clara y concisa del informe, incluyendo los hallazgos y conclusiones		
Revisión del informe	Revisión del informe para garantizar su exactitud y precisión		
Presentación del informe	Presentación del informe al cliente o partes interesadas		
Comentarios y aclaraciones	Proporcionar comentarios y aclaraciones adicionales según sea necesario		
Archivado del informe	Archivar el informe y cualquier evidencia digital en una ubicación segura y de fácil acceso		