República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

Facultad de Estudio de Postgrado e Investigación

Tesis en Opción al Título de Magister en:

Ciberseguridad

Tema de Tesis:

Brechas del Peritaje Informático Forense: Impacto para Juristas y Peritos

Autor:

Ing. Jaime Eduardo Perdomo Córdova, Msc.

Director de Tesis:

Ing. Mayra Lorena Mahecha Guzmán, Msc.

Abril 2024

Guayaquil – Ecuador

DEDICATORIA

A mi amada familia y a mi querida esposa, dedico este logro a ustedes, mis pilares inquebrantables, cuyo amor y apoyo han sido mi fuente de inspiración y fortaleza a lo largo de este viaje académico. Vuestra paciencia, comprensión y sacrificio han sido fundamentales en mi camino hacia la culminación de esta maestría en Ciberseguridad. Este logro no solo es mío, sino que también les pertenece a ustedes, quienes han estado a mi lado en cada paso del camino, brindándome su amor y aliento incondicional.

A mis hijos, que son la luz de mi vida, a mi madre, cuyo amor y guía han sido un faro en mi camino, y a mi padre y hermano que ya no están entre nosotros físicamente, pero cuyo amor y sabiduría continúan guiándome desde lo más profundo de mi corazón, les dedico este logro con gratitud y amor eterno. Vuestras enseñanzas y recuerdos siguen vivos en mí, inspirándome a alcanzar nuevas alturas y a nunca renunciar a mis sueños.

AGRADECIMIENTO

Quiero expresar mi sincero agradecimiento a mis profesores y a mi tutora por su continuo apoyo y orientación durante la realización de este trabajo de titulación en el marco de la maestría en Ciberseguridad. Su contribución ha sido fundamental para alcanzar los objetivos establecidos y asegurar el éxito de este proyecto. Reconozco plenamente la valiosa contribución de su experiencia y compromiso, y valoro sinceramente su dedicación hacia el ámbito de la ciberseguridad.

RESUMEN

Este estudio se enfoca en examinar la situación actual del peritaje informático forense en Quito D.M., Ecuador, con un énfasis en las deficiencias y desafíos que enfrentan las prácticas locales de recolección, preservación y análisis de evidencia digital. Se destacan las discrepancias entre estas prácticas y los estándares internacionales reconocidos en el ámbito del peritaje informático forense, subrayando la necesidad de una mayor alineación para fortalecer el peritaje informático forense en Ecuador y abordar los desafíos actuales en la investigación y persecución de delitos cibernéticos. Además, se enfatiza la importancia de comprender las implicaciones de las deficiencias identificadas en el peritaje informático forense local, que van más allá de la efectividad de las investigaciones digitales y afectan la confianza en el sistema judicial, pudiendo resultar en decisiones judiciales erróneas. La falta de alineación con los estándares internacionales deja a la región vulnerable frente a los delitos cibernéticos, los cuales están en constante evolución y requieren respuestas ágiles y efectivas para proteger a los ciudadanos en un entorno digitalizado. Por lo tanto, este estudio aboga por una mayor conciencia y acción para mejorar las prácticas de peritaje informático forense en Ecuador, a fin de fortalecer la capacidad de investigación y persecución de delitos cibernéticos.

Palabras claves: Peritaje informático forense, Investigación digital, Protección de evidencia digital, Delitos cibernéticos, Vulnerabilidad digital.

ABSTRACT

This study focuses on examining the current situation of computer forensic expertise in Quito D.M., Ecuador, with an emphasis on the deficiencies and challenges faced by local practices of collection, preservation and analysis of digital evidence. Discrepancies between these practices and recognized international standards in the field of computer forensic expertise are highlighted, underlining the need for greater alignment to strengthen computer forensic expertise in Ecuador and address current challenges in the investigation and prosecution of cybercrimes. Furthermore, the importance of understanding the implications of the deficiencies identified in local computer forensic expertise is emphasized, which go beyond the effectiveness of digital investigations and affect confidence in the judicial system, potentially resulting in erroneous judicial decisions. The lack of alignment with international standards leaves the region vulnerable to cybercrimes, which are constantly evolving and require agile and effective responses to protect citizens in a digitalized environment. Therefore, this study advocates for greater awareness and action to improve computer forensics practices in Ecuador, in order to strengthen the capacity to investigate and prosecute cybercrimes.

Keywords: Computer forensic expertise, Digital investigation, Protection of digital evidence, Cybercrimes, Digital vulnerability.

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesis de Maestria me corresponde exclusivamente, y el patrimonio intelectual de la misma a la UNIVERSIDAD TECNOLOGICA EMPRESARIAL DE GUAYAQUIL – UTEG”.

Ing. Jaime Eduardo Perdomo Córdova, Msc.

0920971033

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La pericia informática emerge como un componente fundamental en el contexto jurídico contemporáneo, siendo un instrumento clave para la resolución de casos que involucran evidencia digital. En este sentido, la presente investigación se enfoca en el análisis de la eficacia del peritaje informático en el sistema legal ecuatoriano, explorando su contribución a la resolución de casos y su alineación con estándares nacionales e internacionales.

La evolución de la tecnología ha transformado profundamente la naturaleza de los delitos y las disputas legales, incorporando elementos digitales que requieren una comprensión especializada. El peritaje informático, como disciplina, se ha desarrollado para abordar estos desafíos, proporcionando a los tribunales una herramienta valiosa para la interpretación y evaluación de pruebas digitales. En la capital del Ecuador, donde el sistema legal enfrenta una creciente complejidad, la eficacia del peritaje informático adquiere una relevancia crucial.

La falta de regulaciones claras y la necesidad de adaptarse a un entorno tecnológico en constante cambio presentan desafíos significativos para los peritos informáticos en la capital del Ecuador. Esta investigación busca analizar en profundidad cómo la adhesión a protocolos nacionales e internacionales impacta en la efectividad del peritaje informático. Además, se explorará la percepción de la comunidad legal y judicial sobre la contribución de esta disciplina a la resolución de casos.

La importancia de esta investigación radica en proporcionar una comprensión integral de la situación actual del peritaje informático en el Distrito Metropolitano de Quito, identificando áreas de mejora y brindando recomendaciones para fortalecer su rol en el sistema legal. A través de un enfoque mixto que combina métodos cuantitativos y cualitativos, se pretende obtener una visión holística y contextualizada que enriquezca el conocimiento existente en este campo.

El siguiente documento se estructura en varios capítulos que abordan aspectos específicos de la investigación. En el primer capítulo, se revisará el estado del arte existente sobre peritaje informático, destacando tendencias globales y perspectivas relevantes para el contexto ecuatoriano. El segundo capítulo detalla la metodología utilizada, incluyendo la descripción de las variables de investigación, la población y muestra, y las técnicas de recolección de datos.

El capítulo tres se divide en dos secciones esenciales que respaldan la ejecución eficiente de la investigación. En la primera sección, se presenta un detallado cronograma de actividades para la presente investigación. La segunda sección aborda el Presupuesto de Inversión, proporcionando una visión financiera detallada de los recursos necesarios para llevarla a cabo la investigación.

Esta investigación pretende aportar conocimientos significativos a la comunidad académica, jurídica y pericial, ofreciendo una perspectiva integral sobre el estado actual y las perspectivas futuras del peritaje informático en el contexto legal ecuatoriano.

CAPITULO I

MARCO TEÓRICO CONCEPTUAL

1.1. Antecedentes de la investigación

El desarrollo y la creciente complejidad de las tecnologías de la información han generado un aumento significativo en la incidencia de delitos cibernéticos y casos relacionados con la informática forense en la capital de los ecuatorianos. A medida que la sociedad se vuelve más dependiente de la tecnología, también aumenta la necesidad de una investigación eficiente y precisa en este campo.

(Mairata De Anduiza, 2019) en su artículo historias de un perito informático forense describe al perito judicial, también conocido como perito forense, como un experto con conocimientos especializados y reconocidos, adquiridos a través de su educación superior. Su función principal es proporcionar información o emitir opiniones fundamentadas ante los tribunales de justicia en relación con los puntos litigiosos que son objeto de su peritaje.

Según (Icaza, 2010) el perito Informático Forense debe recibir capacitación tanto en tecnologías de la información y comunicación como en disciplinas legales. En este sentido, es esencial que sea un profesional versátil, que integre de manera integral la formación tecnológica y los conocimientos en ciencias jurídicas en su área de formación.

(Ochoa Arévalo, 2018) describe que el peritaje informático forense, como disciplina, se encarga de la recopilación, análisis y presentación de evidencia digital en contextos legales. A pesar de la importancia crítica de esta práctica, existen brechas y desafíos notables en su implementación en el contexto ecuatoriano.

El presente estudio busca explorar y analizar las brechas que dificultan el debido proceso del peritaje informático, identificando sus causas y evaluando su impacto tanto para los juristas que confían en la evidencia digital en los tribunales

como para los peritos encargados de llevar a cabo el peritaje informático. Este análisis no solo considerará aspectos técnicos y tecnológicos, sino también cuestiones legales, éticas y de capacitación, además, se abordarán aspectos adicionales relacionados con la calidad, buenas prácticas y el alineamiento a estándares internacionales.

En los aspectos técnicos y tecnológicos se analizarán los desafíos que enfrentan los peritos informáticos en áreas como la adquisición, preservación, análisis y presentación de evidencia digital. Se examinarán las herramientas y técnicas disponibles y se identificarán posibles deficiencias o áreas de mejora.

En tema de formación y capacitación se evaluarán los programas de formación y capacitación disponibles para los peritos informáticos, identificando áreas de mejora y recomendando recursos educativos adicionales. Se destacará la importancia de la formación continua en un campo tecnológico en constante evolución.

En el campo del peritaje informático forense un factor de gran relevancia es el alineamiento a estándares internacionales con lo cual se podrá evaluar el grado de conformidad del proceso de investigación digital con estándares internacionales relevantes, como ISO/IEC 27037 para la adquisición y preservación de evidencia digital. Se propondrán estrategias para mejorar dicho alineamiento y garantizar la calidad y confiabilidad de los resultados del peritaje.

Se pretende indagar en los desafíos específicos que enfrenta el peritaje informático forense en la ciudad de Quito, tales como la falta de estándares unificados, la escasez de capacitación especializada para los profesionales, las limitaciones legales en la admisión de evidencia digital, entre otros. Además, se explorarán casos emblemáticos que han evidenciado estas brechas y han influido en la toma de decisiones judiciales.

El aspecto crítico que ha emergido como un desafío sustancial es el desconocimiento del debido proceso para llevar a cabo las investigaciones digitales

forenses, tanto por parte de los peritos encargados de la recopilación y análisis de evidencia digital como por los juristas involucrados en la presentación y evaluación de esta evidencia en los tribunales, la falta de una comprensión clara del debido proceso ha generado consecuencias significativas.

Los peritos informáticos, en muchos casos, pueden encontrarse trabajando en condiciones poco definidas en cuanto a los procedimientos adecuados. La ausencia de protocolos estandarizados y la falta de directrices claras en el manejo de la evidencia digital pueden dar lugar a prácticas que comprometen la integridad de la información recopilada, esto no solo debilita la solidez de la evidencia, sino que también puede abrir la puerta a cuestionamientos legales sobre la legalidad y validez del proceso de recolección.

Por otro lado, los juristas, al no tener un entendimiento profundo de los métodos y desafíos asociados con el peritaje informático, pueden no tener la aptitud adecuada para cuestionar de manera efectiva los procedimientos utilizados por los peritos. La falta de conocimiento sobre cómo se obtiene y maneja la evidencia digital puede resultar en interrogatorios ineficaces y decisiones judiciales que no reflejan una comprensión completa de las implicaciones tecnológicas involucradas.

En última instancia, este estudio aspira a proporcionar recomendaciones concretas para mejorar la práctica del peritaje informático forense en la capital del Ecuador, con el objetivo de fortalecer la integridad del proceso legal y apuntar a una administración de justicia más eficiente y precisa en la era digital.

1.2. Planteamiento del problema

El peritaje informático forense ha emergido como una disciplina crucial en el ámbito legal y de seguridad en Ecuador. En vista del constante aumento de los delitos cibernéticos y la imperiosa necesidad de resguardar la integridad digital, la demanda de servicios proporcionados por peritos informáticos forenses ha experimentado un incremento significativo en investigaciones tanto judiciales como corporativas.

Según (Alcívar et al., 2018) en el Ecuador el Consejo de la Judicatura (CJ), acredita a los peritos que no solo requieren de conocimientos en informática, sino también en leyes o viceversa. Deben buscar evidencias de un delito y redactar informes técnicos forenses sin establecer responsables, sin juicios de valor, es decir, manteniendo una postura objetiva y neutral de cara a las obtenciones de la pericia, sin embargo, existe déficit de este tipo de profesionales algunas provincias del Ecuador y según estadísticas del CJ a nivel nacional son pocos los peritos registrados.

En este contexto, el papel crucial del peritaje informático forense se destaca como un elemento fundamental para la investigación y resolución de casos digitales. No obstante, a pesar de su importancia crítica, la eficacia y confiabilidad del peritaje informático forense en el país se ven amenazadas por diversas brechas y desafíos.

Una de las brechas con la que se enfrenta el proceso de peritaje informático es la no aplicación de estándares unificados en el peritaje informático forense lo cual genera un panorama de incertidumbre en cuanto a los procedimientos y prácticas aceptadas. Esta carencia compromete la consistencia y calidad de las investigaciones, dando lugar a enfoques procedimentales que afectan la integridad de la evidencia digital presentada en los tribunales y con ello al debido proceso.

Como referencia a lo establecido en el párrafo anterior, podemos mencionar el caso del perito condenado por fraude procesal en una audiencia de juicio en Quito en mayo de 2018, lo cual destaca la grave consecuencia de la falta de aplicación de estándares unificados en el peritaje informático forense. La ausencia de procedimientos y prácticas estandarizadas genera incertidumbre en el proceso, comprometiendo la consistencia y calidad de las investigaciones. (Físcalia General del Estado, 2018).

En este contexto, el perito transgredió principios básicos de integridad al manipular evidencia digital en un caso de corrupción. Al sustituir nombres, ocultar

información y emplear una notación no convencional en la transcripción de audios, faltó a los principios de objetividad y exactitud que los estándares unificados buscan salvaguardar. Su accionar, evidenciado en la alteración de pruebas periciales, ilustra cómo la falta de procedimientos uniformes puede llevar a enfoques subjetivos y poco fiables en el manejo de la evidencia digital.

La presentación de aproximadamente 20 pruebas por parte del fiscal, incluyendo informes periciales y la reproducción de los audios, subraya la necesidad de contar con estándares unificados que respalden la integridad y credibilidad de las investigaciones forenses. La utilización de estos estándares habría proporcionado un marco claro para la realización del peritaje, reduciendo la posibilidad de manipulación o errores en el proceso.

La judicialización del caso bajo el artículo 272 inciso 2 del Código Orgánico Integral Penal (COIP) pone de relieve la gravedad de las acciones del perito informático y la importancia de aplicar estándares unificados para asegurar la justicia y la transparencia en los procesos legales relacionados con la evidencia digital.

Figura 1. Alteración Informe Caso Odebrecht

Fuente: Fiscalía General del Estado

Otro caso relevante donde se evidencia la falta de aplicación del debido proceso y cumplimiento de normativa del peritaje informático forense es el que se refleja en el escrito del 25 de septiembre respecto al Informe pericial de informática forense NO. 01-OCM-1833506-2023-STN.

El escrito firmado por el Coordinador General de Asesoría Jurídica del Consejo de Participación Ciudadana y Control Social (Nuñez, 2023), hace mención a un informe pericial de informática forense presentado en septiembre del 2023 el cual plantea preocupaciones sobre la objetividad y la imparcialidad en el peritaje informático forense en Ecuador. En el escrito presentado se cuestiona la designación del perito y la posible manipulación de pruebas para apoyar intereses particulares en detrimento de la legalidad y la imparcialidad.

La falta de transparencia en la selección del perito y la aparente manipulación del archivo de video generan dudas sobre la integridad del proceso pericial. Además, se señala que el perito optó por seleccionar solo ciertos fragmentos del video para su análisis, lo que podría distorsionar la interpretación de los hechos.

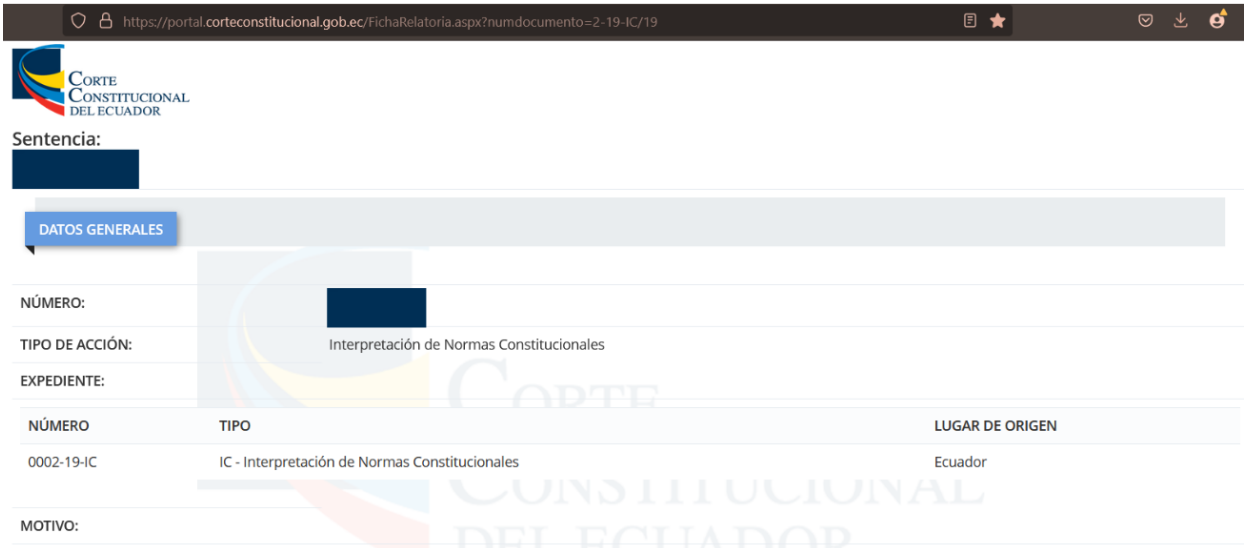
Este caso destaca la necesidad de fortalecer los mecanismos de control y regulación en el ámbito del peritaje informático forense en Ecuador, asegurando la imparcialidad, la ética y el cumplimiento del debido proceso en todas las etapas de la investigación. La falta de integridad y objetividad en los informes periciales puede socavar la confianza en el sistema judicial y comprometer la administración de justicia, subrayando la importancia de abordar estas deficiencias de manera efectiva y oportuna.

Asimismo, la discrepancia entre las normas que regulan la carrera pericial y las conclusiones emitidas en el informe pericial plantea interrogantes sobre la calidad y la claridad de las conclusiones periciales. Aunque se mencionan algunas evidencias y análisis realizados, la ausencia de conclusiones precisas y claras contribuye a la incertidumbre sobre la validez y la objetividad del informe presentado.

Esta discrepancia entre lo esperado según las normativas establecidas y lo realmente manifestado en el informe refleja una posible deficiencia en el proceso de peritaje, lo que podría comprometer la integridad y la credibilidad del resultado pericial. La falta de claridad en las conclusiones dificulta la interpretación adecuada de los hallazgos presentados, generando dudas sobre la fundamentación y la imparcialidad del informe.

Esta situación subraya la importancia de que los peritos actúen en concordancia con los estándares éticos y legales establecidos, garantizando la transparencia y fiabilidad de sus conclusiones en el ámbito del peritaje informático forense.

Figura 2. Búsqueda Informe Pericial

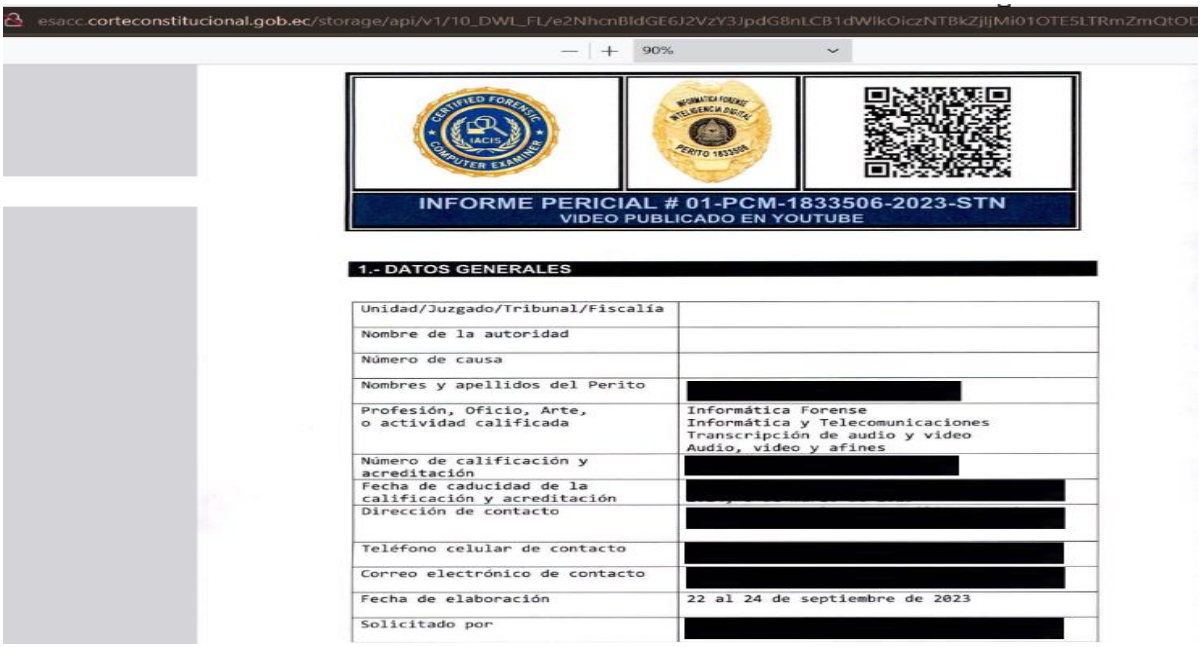


Fuente: Corte Constitucional

Figura 3. Consulta Informe Pericial

Fuente: Corte Constitucional

Figura 4. Informe Pericial



Fuente: Corte Constitucional

Otro de los casos mediáticos donde interviene el peritaje informático es el caso Ola Bini en el que (Cazar, 2022), menciona en su libro Colateral, el papel

desempeñado por el perito informático Fabián Hurtado en el análisis del "pantallazo" como evidencia de acceso a un sistema de la Empresa Pública de Telecomunicaciones (CNT) en el caso de Ola Bini, el cual subraya la importancia de una evaluación imparcial y objetiva de las pruebas presentadas en un caso judicial.

El papel desempeñado por el perito informático Fabián Hurtado en el caso de Ola Bini destaca su competencia y objetividad al analizar la evidencia presentada. Hurtado realizó un exhaustivo análisis técnico de la captura de pantalla en cuestión, identificando y clasificando las palabras relevantes para determinar su significado en el contexto del caso. Su informe concluyó que las palabras indicaban la falta de acceso y el cierre automático de la conexión, lo que sugiere que no se produjo ninguna intrusión.

Esta conclusión sugiere un análisis profesional y riguroso de la evidencia presentada por la Fiscalía. El perito demostró un entendimiento adecuado de los conceptos técnicos involucrados y aplicó un enfoque objetivo al evaluar la naturaleza del "pantallazo" en cuestión. Al destacar que la simple presencia de una pantalla de inicio de sesión no implica necesariamente un acceso no autorizado, el perito proporcionó una perspectiva crítica y fundamentada que ayuda a contextualizar la evidencia presentada en el caso de Ola Bini.

Los peritos, como Fabián Hurtado, trabajan en base a normativas y códigos de ética que exigen imparcialidad en su labor. Sin embargo, a pesar de la claridad y la solidez de su informe, el trabajo de Hurtado fue objeto de represalias y cuestionamientos por parte de otras personas involucradas en el caso. Estas acciones revelan una falta hacia el debido proceso y la imparcialidad que debería prevalecer en el sistema judicial. La presentación de una queja disciplinaria en su contra y la apertura de una investigación muestran un intento de desacreditar su trabajo y socavar su credibilidad como experto forense.

Estos acontecimientos ponen de manifiesto la importancia de garantizar un proceso judicial justo y equitativo, en el que se respete el trabajo de los expertos y se valore su independencia y objetividad. Además, subrayan la necesidad de proteger a los profesionales que desempeñan un papel crucial en la búsqueda de la verdad y la justicia, asegurando que puedan llevar a cabo su labor sin temor a represalias o interferencias indebidas.

En resumen, el análisis técnico riguroso proporcionado por Fabián Hurtado resalta la necesidad de contar con expertos imparciales en el proceso judicial, quienes puedan evaluar la evidencia de manera objetiva y profesional, en conformidad con los estándares éticos y normativos de la profesión.

Sin embargo, a lo largo de la evolución de este caso, se contó con la participación de varios peritos informáticos forenses, quienes realizaron una serie de análisis exhaustivos que pusieron de manifiesto aspectos inquietantes.

Dichos análisis, llevados a cabo por expertos en la materia, han generado un considerable debate y han levantado señalamientos de posibles irregularidades, lo cual arroja serias dudas sobre la integridad y la imparcialidad del proceso judicial en su conjunto. Esta situación ha alimentado una creciente preocupación en la opinión pública y ha puesto en entredicho la confianza en el sistema judicial.

Durante los peritajes informáticos, se observó una falta de profundidad en el análisis de la evidencia digital por parte de los peritos designados. Las respuestas vagas y la ausencia de un examen detallado de los dispositivos electrónicos incautados han generado interrogantes sobre la calidad y la validez de las conclusiones presentadas ante el tribunal. Esta falta de rigor técnico socava la credibilidad del proceso judicial y sus resultados.

Otro punto crítico que se evidenció durante los peritajes fue la violación de la cadena de custodia de las pruebas. La falta de un registro adecuado de la manipulación y el almacenamiento de la evidencia digital compromete la integridad y la autenticidad de la misma. Esta irregularidad plantea serias dudas sobre la

fiabilidad de la evidencia presentada y sus implicaciones en la toma de decisiones judiciales.

Además, se han registrado casos de presentación de pruebas inconsistentes y no relacionadas directamente con las acusaciones contra Ola Bini. La inclusión de evidencia irrelevante, como un video sobre Assange, genera dudas sobre la veracidad de las afirmaciones y la legitimidad del proceso judicial en su conjunto. Esta falta de coherencia en la presentación de pruebas mina la confianza en la imparcialidad del sistema judicial.

Por último, se ha observado un intento por parte de la Fiscalía de incluir pruebas no anunciadas durante la audiencia, lo que constituye una transgresión del debido proceso y afecta los derechos de defensa del acusado. Esta falta de transparencia debilita la credibilidad del proceso judicial y sus garantías fundamentales.

En conclusión, los fallos y las irregularidades detectadas durante los peritajes informáticos en el caso de Ola Bini plantean serias preocupaciones sobre la integridad y la validez del proceso judicial. Estos aspectos erosionan la confianza en el sistema judicial y sus garantías fundamentales, lo que podría tener serias repercusiones en el respeto de los derechos individuales y la garantía del debido proceso en casos similares en el futuro.

Otra de las brechas del peritaje informático radica en la falta de programas de capacitación especializados para peritos informáticos forenses en el país, lo cual crea una brecha crítica.

Según (Lara, 2022) en la RESOLUCIÓN 147-2022 DEL PLENO DEL CONSEJO DE LA JUDICATURA, EN EL CAPÍTULO IV CURSO BÁSICO PARA PERITOS en el **Artículo 40: Alcance de la capacitación.-** Las y los peritos calificados deberán aprobar un Curso Básico para Peritos organizado por la Escuela de la Función Judicial, que consistirá en la profundización de temas contenidos en el presente Reglamento, sobre las obligaciones integrales y los deberes de las y los

peritos, de la normativa pertinente constante en el Código Orgánico de la Función Judicial y demás leyes aplicables, así como en el análisis y comprensión del formato a utilizarse para la emisión de los informes periciales y respecto al cumplimiento de sus requisitos.

Sin embargo, la falta de una formación continua en tecnologías emergentes y aspectos legales puede conducir a procedimientos inadecuados por parte de los peritos en el ámbito de la ciberseguridad, lo cual afecta su capacidad para abordar eficazmente los desafíos en este campo.

Esta deficiencia de conocimientos actualizados se ve agravada por las restricciones legales en la admisión de evidencia digital en los tribunales ecuatorianos, que constituyen otro desafío significativo. La ausencia de normativas claras y actualizadas sobre la aceptación de pruebas digitales crea un ambiente propicio para disputas legales que socavan la solidez de los casos y minan la confianza en la evidencia presentada.

(Martins, 2022) en la publicación realizada sobre la Problemática jurídica de la prueba digital y sus implicaciones en los principios penales, señala que: en la lucha contra los delitos digitales, es crucial el uso de medidas de investigación tecnológica y la obtención de pruebas digitales. Sin embargo, este proceso presenta desafíos legales para investigadores, abogados, fiscales y jueces, quienes deben enfrentar obstáculos para asegurar la autenticidad y la validez de la evidencia digital presentada.

La extracción de pruebas digitales y la identificación de los responsables del delito plantean problemas legales que deben abordarse dentro del marco jurídico existente en el Derecho Penal. Dada estas circunstancias La falta de un entendimiento claro del debido proceso en las investigaciones digitales forenses, tanto por parte de los peritos como de los juristas, representa una brecha fundamental en la seguridad digital. La ausencia de protocolos estandarizados y

directrices claras puede dar lugar a prácticas que comprometen la integridad de la información recopilada, debilitando la robustez de la evidencia digital.

La falta de comprensión profunda por parte de los juristas sobre los métodos y desafíos asociados con el peritaje informático dificulta su capacidad para cuestionar eficazmente los procedimientos utilizados por los peritos. Esto no solo afecta la calidad de los interrogatorios, sino que también influye en la toma de decisiones judiciales, poniendo en riesgo la validez de los juicios en el ámbito digital.

Según lo indicado por (Salazar Méndez et al., n.d.) en su publicación en la Revista Científica de Ciencias Jurídicas, Criminología y Seguridad de la FISCALÍA GENERAL DEL ESTADO, en relación con las medidas o actividades que permitan la investigación criminal, se destacan varias deficiencias importantes que deben ser corregidas por los ordenamientos procesales. Estas incluyen:

A. “El desconocimiento de los agentes de la policía judicial o de la fiscalía en cuanto a la obtención o recuperación estándar, aducción, aseguramiento y exhibición con cumplimiento de la cadena de custodia de aquella evidencia digital o medio probatorio en formato informático o digital que puede ser reconocido (auditada y trazable como prueba en los juicios, en relación con los delitos realizados en entornos o con medios virtuales. Al margen de lo anterior, debe existir amplia regulación de los mensajes de datos almacenados en dispositivos tecnológicos y lógicos que puedan ser declarados admisibles como medios de prueba en la legislación interna, conforme a los estándares ISO internacionales.

   Por lo demás, ello exige que la autoridad competente regule de forma clara y precisa, a través de protocolos, las técnicas digitales forenses específicamente admitidas para enfrentar las diferentes características de la evidencia digital (volátil, eliminable, duplicable, anónima, alterable y modificable). Esto, además, para garantizar que

las actividades de investigación respetan y cumplen con los diferentes requisitos legales para considerarla legal, lícita, creíble, admisible, auténtica, completa y confiable. No basta con una somera mención de dichas características en la ley, es necesario desarrollarlas para que todos puedan entender sus alcances y las limitaciones que se desprenden de ellas.

B. La falta de programas metodológicos serios que permitan planificar adecuadamente el diseño de la búsqueda, recolección, obtención, preservación, embalaje, etc. de la prueba digital necesaria para demostrar los cibercrímenes en el juicio. En otras palabras, para garantizar la práctica adecuada de la prueba y su análisis técnico científico. Ello es particularmente importante cuando se trata de casos que afectan la seguridad o la defensa nacional.

   Naturalmente, para que la planificación de la investigación judicial pueda ser exitosa es primordial que las actividades judiciales estén precedidas por aproximaciones interdisciplinarias y colaborativas, que utilicen de manera correcta los diferentes términos técnicos y jurídicos en las diferentes etapas de una investigación digital forense. En dichas actividades de colaboración se deben seguir de manera estricta los diferentes deberes de actuación para no producir inconvenientes innecesarios. Así, por ejemplo, los líderes técnicos de la investigación deben ser principalmente ingenieros, mientras que los líderes que impulsan la imputación de cargos y la acusación de los posibles autores deberán ser abogados especializados.

C. También es importante anotar que las entidades del Estado encuentran importantes obstáculos en la falta de iniciativas y desarrollo en legal tech, especialmente, de equipos y software

especializados, licenciados y autorizados con código abierto para adelantar toda clase de investigaciones o pesquisas judiciales efectivas. La carencia de estos medios implica que, en muchos casos, la actividad de investigación no se ajuste a los estándares legales o internacionales en materia de identidad y seguridad de la evidencia digital, además de hacer muy dispendiosa (y costosa) la obtención y disposición de múltiples versiones de software licenciado que le permitan realizar las correspondientes comparaciones y averiguaciones técnicas de la evidencia, a partir del software empleado efectivamente por los cibercriminales.

D. Las malas prácticas al momento de producir la prueba en el proceso. Uno de los fenómenos más comunes en el ámbito de las investigaciones digitales es la falta de selección de la evidencia obtenida, exhibida y solicitada como prueba en el juicio oral (o en las audiencias públicas correspondientes), que luego no se practica en su totalidad por la renuncia expresa de alguna de las partes procesales. Así mismo, el solo hecho de que las contrapartes tengan que revisar grandes volúmenes de evidencia e información que se descubre de manera innecesaria en los procedimientos judiciales, sin ninguna clase de control previo de material, produce una quiebra del plazo razonable del proceso judicial y afecta de manera tangible los derechos de defensa y contradicción, así como en la eficacia del juicio y en la inmediación del juez.

E. Para terminar este aparte, es necesario evitar la alta rotación de funcionarios judiciales o de investigación entre las diferentes entidades del Estado. Rotación que no solo permite una dispersión injustificada de las distintas investigaciones judiciales, sino también que se desperdicien las capacitaciones especializadas a funcionarios

judiciales y agentes fiscales y, con ello, la oportunidad de hacer investigaciones realmente eficaces. Es inconcebible que dichos funcionarios sean reemplazados por personas que desconocen las técnicas de investigación o el lenguaje técnico aplicado".

Las brechas y desafíos identificados en el peritaje informático forense representan una amenaza palpable para la integridad de las investigaciones y la administración de justicia en el ámbito digital.

Estas deficiencias pueden resultar en la manipulación o pérdida de evidencia, la falta de capacidad para realizar un análisis forense adecuado o la presentación de pruebas inadmisibles en los procesos legales. Ante este escenario, el presente trabajo de investigación se propone no solo identificar y comprender estas brechas, sino también analizar sus causas subyacentes y proponer soluciones prácticas y efectivas para abordarlas.

Al hacerlo, se busca fortalecer la seguridad digital y garantizar la integridad del proceso de peritaje informático forense en el contexto específico del Ecuador. Este enfoque no solo beneficiará a los profesionales involucrados en la investigación y persecución de delitos cibernéticos, sino que también contribuirá a la protección de los derechos individuales y la confianza en el sistema judicial en la era digital.

1.2.1. Formulación del problema

¿Cuáles son las brechas y desafíos que enfrenta el peritaje informático forense, afectando su eficacia y confiabilidad en el ámbito legal y tecnológico?

1.2.2. Sistematización del problema

1. ¿De qué manera la falta de comprensión del debido proceso en las investigaciones digitales forenses impacta la integridad y validez de la evidencia digital?

2. ¿Cuáles son los desafíos tecnológicos específicos que enfrentan los peritos informáticos forenses en la adquisición, preservación, análisis y presentación de evidencia digital?
3. ¿Cuáles son las implicaciones de la falta de capacitación técnica especializada en metodologías forenses digitales y cómo afecta la confiabilidad de los resultados periciales en el peritaje informático forense?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Analizar las brechas existentes en el peritaje informático forense, centrándose en aspectos técnicos, tecnológicos y de capacitación, para fortalecer la integridad del proceso de la investigación digital forense.

1.3.2. Objetivo específicos

- Identificar los factores que contribuyen a la falta de comprensión del proceso en investigaciones digitales, incluyendo la carencia de protocolos, y su impacto en la validez de la evidencia.
- Determinar los desafíos tecnológicos de peritos informáticos en la adquisición, preservación, análisis y presentación de evidencia digital.
- Investigar cómo la falta de capacitación en metodologías forenses digitales afecta la fiabilidad de los resultados periciales, proponiendo recomendaciones para mejorar la formación de los peritos.

1.4. Justificación de la investigación

La investigación sobre las brechas y desafíos en el peritaje informático forense se erige de forma necesaria en consonancia con la evolución constante de la tecnología en la sociedad actual. El vertiginoso avance tecnológico ha otorgado beneficios invaluables a la sociedad ecuatoriana, pero conlleva un aumento proporcional en la comisión de delitos cibernéticos. La creciente conectividad digital

y la dependencia de la tecnología en diversas esferas de la vida cotidiana han generado un escenario en el cual la protección y la interpretación adecuada de la evidencia digital se tornan cruciales para la administración de la justicia.

La investigación se fundamenta en la premisa de que la adaptación del sistema judicial a estas realidades tecnológicas es esencial para mantener la integridad y la confianza en el proceso legal. El peritaje informático forense, como disciplina especializada, se sitúa en el epicentro de esta dinámica, enfrentando el desafío de evolucionar a la par de las tecnologías emergentes y los patrones cambiantes de los delitos cibernéticos.

La sociedad ecuatoriana, al incorporar rápidamente la tecnología en su tejido social, se ha vuelto más vulnerable a amenazas digitales, desde fraudes electrónicos hasta ciberataques de mayor envergadura. Esta vulnerabilidad resalta la necesidad crítica de contar con peritos informáticos forenses altamente capacitados, capaces de abordar con eficacia las complejidades de la evidencia digital y de contribuir al esclarecimiento de casos judiciales relacionados con el ámbito digital.

La justificación para esta investigación se basa en la necesidad urgente de mejorar y fortalecer el peritaje informático forense en el país, en respuesta a las demandas y desafíos actuales, dado que los peritajes son cada vez más frecuentes en los escenarios de gestión de incidentes en instituciones públicas y privadas. En este sentido, en un entorno cada vez más digitalizado, es fundamental adaptar las prácticas de peritaje informático para garantizar la integridad y fiabilidad del tratamiento de evidencia digital buscando asegurar que las investigaciones digitales se realicen con rigurosidad y precisión, lo que contribuye a la efectividad y legitimidad del proceso.

1.5. Marco de referencia de la investigación

El marco de referencia constituye el fundamento esencial tanto conceptual como contextual de la investigación, proporcionando una estructura integral que

aborda una variedad de dimensiones cruciales que afectan al peritaje informático forense. En este sentido, no solo se pretende explorar los principios teóricos que respaldan al peritaje forense informático como disciplina especializada relevante en los procesos de judicialización, sino también profundizar en las implicaciones legales, los conceptos clave y la metodología aplicada en la práctica del peritaje informático forense.

Este enfoque integral tiene como objetivo proporcionar una comprensión exhaustiva de todos los aspectos relevantes relacionados con el peritaje informático forense, permitiendo así una investigación rigurosa y completa que contribuya al avance y la mejora de esta importante área en el ámbito legal y tecnológico.

1.5.1. Marco Teórico

Según (Alberdi et al., 2017) el peritaje informático forense, siendo una disciplina en continua evolución, se basa en teorías fundamentales que engloban aspectos esenciales de la seguridad informática, la preservación de la integridad de la evidencia digital y la aplicación de métodos forenses en entornos digitales.

Este campo interdisciplinario se nutre de principios provenientes de diversas áreas como la informática, la criptografía, la ley y la ética, convergiendo para establecer un marco sólido que permita la adecuada identificación, recolección, análisis y presentación de pruebas digitales en el contexto judicial. Al comprender estas teorías fundamentales, se puede avanzar hacia una práctica más efectiva y confiable del peritaje informático forense, lo que a su vez fortalece la integridad y la credibilidad del proceso legal en la era digital.

Dentro del marco teórico, se adentra en las teorías relacionadas con la seguridad informática, centrándose especialmente en las estrategias y medidas específicas utilizadas para preservar la integridad, confidencialidad y disponibilidad de la información digital en el contexto del peritaje informático forense.

(Avenía, 2017) indica que la seguridad informática examina modelos teóricos que abordan la prevención de accesos no autorizados, la detección de vulnerabilidades y la mitigación de riesgos en sistemas informáticos.

Se examinan en profundidad conceptos clave como la autenticación, la encriptación, el control de acceso y la gestión de riesgos en el ámbito de la investigación forense digital.

Este análisis considera cómo estas teorías y prácticas de seguridad informática se aplican en el contexto del peritaje informático forense, donde la preservación y el análisis de la evidencia digital juegan un papel crucial en la resolución de disputas legales y la investigación de delitos cibernéticos. Se estudian en detalle los protocolos y estándares reconocidos internacionalmente, así como las mejores prácticas establecidas por organizaciones especializadas en ciberseguridad y forense digital.

Este enfoque integral proporciona un contexto esencial para comprender el papel crítico del peritaje informático forense en la preservación de la integridad y la seguridad de la información digital en un mundo cada vez más dependiente de la tecnología.

Según (María & Sosa, 2023) la Integridad de la Evidencia Digital **s**e profundiza en las teorías que respaldan la integridad de la evidencia digital, destacando la importancia de garantizar que la información recolectada sea precisa, no haya sido alterada y pueda ser presentada de manera confiable en un entorno judicial. Teorías relacionadas con la cadena de custodia digital, sellos temporales y técnicas de hash son examinadas para comprender cómo se preserva la integridad de la evidencia a lo largo del proceso forense.

Además, se analizan las teorías relacionadas con la cadena de custodia digital, que se centran en establecer y mantener un registro detallado de todos los pasos y personas involucradas en el manejo de la evidencia digital, desde su adquisición inicial hasta su presentación en el tribunal. Se estudian los

procedimientos para documentar y proteger la evidencia contra alteraciones no autorizadas, así como la utilización de sellos temporales y técnicas de hash para verificar la integridad de los datos en diferentes etapas del proceso forense.

Se examinan los estándares y prácticas recomendadas para la gestión de la cadena de custodia digital, incluyendo la autenticidad de las firmas digitales y el uso de herramientas de verificación de integridad. Todo esto con el fin de asegurar que la evidencia digital sea tratada de manera adecuada y que su integridad no sea comprometida en ningún momento. Este enfoque riguroso en la preservación de la integridad de la evidencia digital es esencial para garantizar su validez y fiabilidad en un entorno judicial, donde la evidencia debe ser presentada de manera confiable y veraz para respaldar los procesos legales.

De manera complementaria a la preservación de la evidencia digital, existen los métodos forenses en entornos digitales cuyo análisis se centra en teorías que sustentan los métodos forenses empleados en entornos digitales ~~Según~~ (Cajo et al., 2018), esto incluye la exploración de modelos teóricos que guían la identificación, adquisición y análisis de pruebas digitales. Se consideran teorías relacionadas con la adopción de enfoques sistemáticos y científicos para la recolección de evidencia, asegurando la confiabilidad y validez de los resultados.

Los métodos forenses en entornos digitales también involucran la aplicación de técnicas especializadas para preservar la integridad de la evidencia digital durante todo el proceso de análisis. Esto puede incluir la utilización de herramientas de software avanzadas para crear imágenes forenses de dispositivos, así como también técnicas de análisis de datos para identificar patrones y relaciones relevantes en la información recuperada.

Después de considerar los enfoques teóricos mencionados por (Cajo et al., 2018), es fundamental explorar las metodologías específicas empleadas en la investigación forense digital. Diversas metodologías han sido reconocidas y aplicadas en distintos contextos, ofreciendo herramientas y técnicas para llevar a

cabo este tipo de investigaciones. A continuación, se presentan algunas de estas metodologías.

RFC 3227 - Guidelines for Evidence Collection and Archiving – Directrices.

Según lo establece (Incibe, 2014), la RFC3227, denominada "Directrices para la recolección de evidencias y su almacenamiento", es un documento que establece pautas para la recopilación y preservación de evidencias en incidentes de seguridad. Este documento, parte de la serie "Request For Comments" (RFC), recopila propuestas de expertos en el área para establecer estándares y protocolos en diversas materias, incluyendo el manejo de evidencias digitales.

Las principales directrices de este documento incluyen principios durante la recolección de evidencias, como la captura detallada de imágenes del sistema, la toma de notas precisas y la minimización de cambios en la información recolectada. También establece un orden de volatilidad para la recolección de información, priorizando la obtención de datos más volátiles primero.

Asimismo, el RFC3227 señala acciones que deben evitarse para preservar la integridad de las evidencias, como no apagar el ordenador hasta completar la recolección de información y no confiar en los programas del sistema para recopilar datos. Se destaca la importancia de consideraciones sobre la privacidad y la necesidad de obtener autorizaciones por escrito para la recolección de evidencias.

En cuanto al procedimiento de recolección, se enfatiza en la transparencia de los métodos utilizados y se detallan pasos específicos, como la identificación de la evidencia relevante, la fijación del orden de volatilidad y la documentación detallada de cada paso. El almacenamiento de la evidencia debe seguir una cadena de custodia claramente documentada y emplear dispositivos de almacenamiento seguros.

Por lo tanto, el RFC3227 proporciona un marco sólido para la recolección y almacenamiento de evidencias en incidentes de seguridad, promoviendo la rigurosidad y la transparencia en todo el proceso. Es fundamental seguir estas directrices para garantizar la integridad y la validez de las evidencias digitales en investigaciones forenses y procesos legales.

ISO/IEC 27037:2012 - Information technology -- Security techniques - Guidelines for identification, collection, acquisition and preservation of digital Evidence.

Conforme a (Nessi, 2017), la norma ISO/IEC 27037:2012, es un marco crucial en el análisis forense de evidencias digitales, definiendo directrices para el manejo adecuado de dichas evidencias desde su identificación hasta su preservación. Esta normativa establece principios esenciales que guían al Perito Informático en cada etapa del proceso, asegurando la integridad y la confiabilidad de la evidencia presentada en un proceso judicial.

La ISO/IEC 27037:2012 se centra en cuatro principios fundamentales: metodología, auditoría del proceso, reproducción del proceso y defensa del proceso. Estos principios son esenciales para garantizar la autenticidad y la validez de la evidencia digital presentada en un tribunal.

La normativa establece pautas claras para la identificación, adquisición y conservación de la evidencia digital, así como para el mantenimiento de una cadena de custodia sólida y documentada. La Cadena de Custodia es crucial en el proceso, ya que traza el camino recorrido por la evidencia desde su descubrimiento hasta su presentación en el tribunal, asegurando su integridad y confiabilidad.

El incumplimiento de la normativa ISO/IEC 27037:2012 puede tener graves consecuencias legales, debilitando la credibilidad de la evidencia presentada y comprometiendo la posición legal en un proceso judicial. Es fundamental seguir rigurosamente las directrices de esta normativa para garantizar la solidez y la confiabilidad de la evidencia digital en un caso legal.

Tipología de los Dispositivos y Entornos en la ISO 27037

La norma aborda diferentes tipos de dispositivos y entornos, que incluyen:

- Computadoras y dispositivos de almacenamiento, así como periféricos.
- Sistemas críticos con una alta demanda de disponibilidad.
- Equipos informáticos y dispositivos conectados a redes.
- Dispositivos móviles.
- Sistemas de circuito cerrado de televisión digital.

Figura 5. La actuación pericial tipología de los dispositivos.

Fuente: La actuación pericial tipología de los dispositivos. (2012). Recuperado de https://www.informaticayderecho.com.ar.

Los fundamentos esenciales en los que se sustenta la norma ISO 27037 son los siguientes:

Aplicación de Métodos

La obtención de evidencia digital debe realizarse de la manera menos intrusiva posible, procurando preservar su integridad original y, siempre que sea factible, obteniendo copias de respaldo.

Proceso Auditable

Los procedimientos seguidos y la documentación generada deben ser validados y contrastados mediante buenas prácticas profesionales. Deben proporcionarse trazas y evidencias de las acciones realizadas y sus resultados.

Proceso Reproducible

Los métodos y procedimientos aplicados deben ser reproducibles, verificables y argumentables a un nivel comprensible por expertos en la materia, quienes puedan otorgar validez y respaldo a las acciones llevadas a cabo. Esto garantiza no solo la consistencia y la confiabilidad del proceso, sino también su transparencia y su capacidad de resistir el escrutinio y la evaluación crítica por parte de profesionales cualificados.

Proceso Defendible

Es fundamental que se mencionen las herramientas utilizadas, asegurando que hayan sido validadas y contrastadas en su uso para el propósito específico en el cual se emplean durante la actuación. Esto garantiza la transparencia y la fiabilidad del proceso, proporcionando una base sólida para la defensa de las actuaciones realizadas.

Figura 6. Fases/Procesos de actuación pericial ISO 27037

Fuente: La actuación pericial tipología de los dispositivos. (2012). Recuperado de https://www.informaticayderecho.com.ar.

Para cada tipo de dispositivo, la normativa divide el manejo de la evidencia en tres procesos distintos, estableciendo así un modelo genérico para su tratamiento:

Identificación

Este proceso implica la localización y la identificación de la evidencia, ya sea en su estado físico o lógico, según corresponda a cada caso particular.

Recolección y/o Adquisición

En este paso se procede a recolectar los dispositivos y la documentación relevantes, asegurándose de incautarlos o secuestrarlos apropiadamente, o bien a adquirir y copiar la información almacenada en dichos dispositivos.

Conservación/Preservación

Es crucial preservar la evidencia para garantizar su utilidad y su integridad. Esto implica mantener su originalidad para que pueda ser aceptada como prueba válida e íntegra en el futuro. Por lo tanto, las acciones en este proceso están orientadas hacia la conservación de la cadena de custodia, así como la integridad y originalidad de la evidencia.

La aplicación práctica de la Norma en las Actuaciones Periciales

Este estándar aborda la recopilación y captura de evidencia desde una perspectiva integral, centrándose principalmente en acciones derivadas de incidentes de seguridad y violaciones asociadas. Sin embargo, en escenarios cotidianos, no todos los principios establecidos son aplicables ni recomendables en su totalidad. Por lo tanto, es necesario adaptar la estrategia de actuación según las particularidades y condiciones específicas de cada caso.

Es esencial considerar las características clave de la información que se pretende recopilar, comprendiendo la naturaleza de la evidencia y determinando la mejor manera de proceder para garantizar su éxito. Esto implica desarrollar un protocolo de actuación personalizado y específico para cada situación particular.

La siguiente gráfica muestra los valores de las variables relevantes (Características de la Información y Estados de la Información) que deben ser considerados al capturar evidencia telemática.

Figura 7. La evidencia telemática.

Fuente: La actuación pericial tipología de los dispositivos. (2012). Recuperado de https://www.informaticayderecho.com.ar.

UNE: 71505-3:2013 - Sistema de Gestión de Evidencias Electrónicas

En un contexto donde la gran mayoría de organizaciones, tanto públicas como privadas, basan sus procesos y actividades en sistemas digitales, es crucial asegurar la disponibilidad de Evidencias Electrónicas válidas y legalmente reconocidas para proteger sus intereses y demostrar el cumplimiento de sus obligaciones. Para lograr esto, es esencial implementar un Sistema de Gestión de Evidencias Electrónicas.

Acorde a lo indicado por (Asociación Española de Normalización, 2020), La norma UNE 71505 establece requisitos para gestionar evidencias electrónicas a lo

largo de su ciclo de vida, abarcando actividades relacionadas con la generación, almacenamiento, transmisión, recuperación, tratamiento y comunicación de dichas evidencias.

Este sistema se encarga de varios aspectos fundamentales:

- Define y describe los conceptos de seguridad de la información relacionados con las evidencias electrónicas.
- Identifica las conexiones entre el Sistema de Gestión de Evidencias Electrónicas (SGEE) y el Sistema de Gestión de Seguridad de la Información.
- Especifica los controles de seguridad aplicables a la gestión de evidencias electrónicas.

La implementación de un SGEE garantiza la validez y disponibilidad de Evidencias Electrónicas. La norma UNE 71505 guía este proceso, definiendo buenas prácticas. El SGEE describe formatos y mecanismos para mantener la confiabilidad de las evidencias, cumpliendo con atributos esenciales.

Figura 8. Sistema de Gestión de Evidencias Electrónicas.

Fuente: Sistema de Gestión de Evidencias Electrónicas. (2012). Recuperado de https://www.govertis.com/une-71505-sistemas-de-gestion-de-evidencias-electronicas.

UNE: 71506-3:2013 - Metodología para el análisis forense de las evidencias electrónicas.

Según lo indicado por (Gervilla Rivas, 2014), la norma UNE 71506/2013 se ha creado con el propósito de establecer el procedimiento de análisis forense dentro del ciclo de gestión de evidencias electrónicas, en conjunto con los demás procesos que integran este sistema de gestión, tal como se detalla en la norma UNE 71505.

Esta norma no abarca la generación, gestión, seguridad, conservación o almacenamiento de la evidencia electrónica antes de su adquisición, ya que estos aspectos están cubiertos por las Normas UNE 71505.

Esta normativa no tiene como objetivo la validación o acreditación de laboratorios forenses, ni la homologación de software o equipos relacionados. Además, las normas son aplicables a cualquier organización, independientemente de su actividad o tamaño, así como a cualquier profesional competente en este campo.

La norma UNE 71506/2013 consta de diversas etapas:

Preservación

En esta fase se busca mantener la validez y fiabilidad de las evidencias originales. Los peritos informáticos deben almacenarlas correctamente, usar indumentaria adecuada para evitar descargas electrostáticas y guardar las evidencias de forma segura.

Adquisición

Durante esta etapa se realiza una copia a bajo nivel de los datos originales, tomando precauciones dependiendo del estado de los sistemas. Es crucial para no comprometer la integridad de las evidencias.

Documentación

Aquí se registra todo el procedimiento, desde el inicio del análisis hasta la entrega del informe pericial al solicitante. Se detallan los procesos y herramientas utilizadas, manteniendo una secuencia temporal definida.

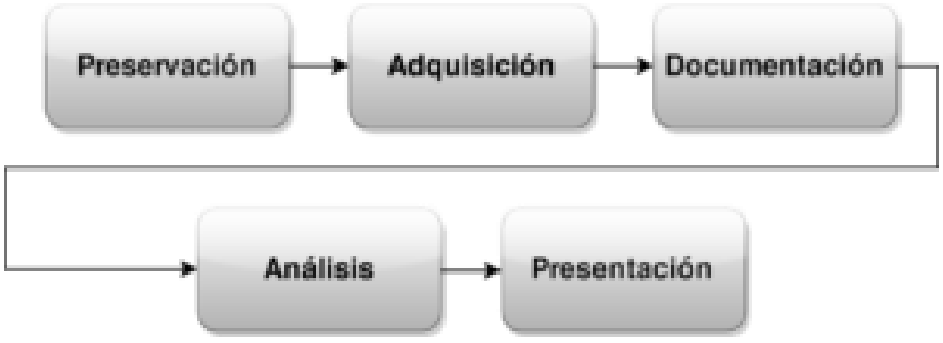
Análisis

Se llevan a cabo procesos para responder a preguntas relacionadas con el evento investigado, como la recuperación de archivos borrados, estudio de particiones y sistemas de archivos, análisis del sistema operativo y de la seguridad implementada.

Presentación

En la fase final se redacta un informe pericial comprensible para el público no técnico, que incluye toda la información obtenida durante el análisis. Este informe se envía al organismo solicitante junto con el documento de control de evidencias para garantizar una mayor trazabilidad del proceso.

Figura 9. Metodología para el análisis forense de las evidencias electrónicas.



Fuente: Sistema de Gestión de Evidencias Electrónicas. (2014). Recuperado de https://peritosinformaticos.es/iso-71506-2013-perito-informatico.

ISO 27042:2015

Según (ISO/IEC 27040, 2015), la norma ISO/IEC 27042:2015 se presenta como una guía integral para el análisis de evidencia digital, ofreciendo directrices claras sobre cómo los peritos informáticos deben abordar cada etapa del proceso, desde la identificación hasta la presentación en un juicio. Esta normativa aborda la complejidad inherente al proceso, donde los peritos deben justificar sus elecciones y demostrar su equivalencia a otros métodos utilizados por sus pares.

En detalle, la norma establece indicaciones específicas que el perito informático debe incluir en su informe pericial, siempre que no existan restricciones judiciales. Estas indicaciones incluyen información sobre las calificaciones del perito, los detalles iniciales del incidente, los objetivos de la investigación, los miembros del equipo de investigación, los hechos encontrados durante la investigación, los daños en la evidencia digital, las limitaciones de los análisis realizados, las herramientas utilizadas, la interpretación de la evidencia y las conclusiones, entre otros aspectos.

La normativa ISO/IEC 27042:2015 establece un conjunto de prácticas y procedimientos que deben seguir los peritos informáticos durante todo el proceso de análisis de evidencia digital. Al proporcionar un marco sólido y estandarizado, esta norma garantiza la coherencia y la calidad en cada etapa de la investigación forense digital. Desde la identificación inicial de la evidencia hasta su presentación ante un tribunal, los peritos pueden confiar en las directrices establecidas por esta normativa para asegurar la integridad y la validez de los datos recopilados.

Al seguir los estándares definidos en la ISO/IEC 27042:2015, los peritos informáticos pueden mejorar la eficiencia de sus procesos de trabajo, reducir errores y minimizar el riesgo de posibles desafíos legales o disputas relacionadas con la evidencia presentada. En resumen, esta normativa proporciona un marco sólido y confiable que ayuda a los profesionales en la investigación forense digital

a realizar su trabajo de manera efectiva y conforme a los más altos estándares de calidad y profesionalismo.

Figura 10. Etapas de la norma ISO 27042:2015

Fuente: ISO 27042:2015

Instituto Nacional de Estándares y Tecnología (Modelo Forense Digital Abstracto)

Según señala (OEA, 2019) el Instituto Nacional de Estándares y Tecnología (NIST) es una autoridad reconocida en el campo de la investigación forense digital, y ofrece una serie de pautas y procedimientos a través de sus publicaciones. Entre estas, destaca el "Guide to Integrating Forensic Techniques into Incident Response", que proporciona un marco detallado para la investigación y respuesta a incidentes en entornos digitales.

Esta metodología se basa en estándares reconocidos y enfoques científicos, asegurando la integridad y validez de los datos forenses obtenidos durante la investigación. Proporciona una estructura clara para la recolección, preservación,

análisis e interpretación de evidencia digital, lo que permite a los investigadores abordar de manera efectiva los incidentes y mantener la cadena de custodia de la evidencia.

El modelo desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) describe minuciosamente cada etapa y subproceso de la investigación forense digital, destacando la vital importancia de aspectos como la integridad, la autenticidad, la confidencialidad y la trazabilidad de la evidencia. Entre las características de este modelo se encuentran:

- Identificación de las evidencias
- Apoyo a conjeturas
- Aseguramiento físico de las evidencias
- Utilización de mecanismos lógicos
- Prevención de la pérdida de información

El enfoque del NIST se centra en la aplicación de prácticas forenses sólidas y rigurosas, garantizando la fiabilidad de los resultados y la adhesión a los principios éticos y legales en el manejo de la evidencia digital. Además, estas pautas son ampliamente reconocidas, lo que proporciona un estándar común para la investigación forense digital en diversos contextos y jurisdicciones.

Marco de investigación forense digital basado en eventos

(Fisher et al., 2006), señala que este enfoque de investigación se basa en la premisa fundamental de que los sistemas y redes informáticas registran una gran cantidad de eventos relacionados con la seguridad. Estos eventos pueden incluir actividades de usuarios, intentos de acceso no autorizado, cambios en la configuración del sistema, entre otros.

La recopilación y análisis de estos eventos permiten a los investigadores reconstruir y comprender los incidentes de seguridad que ocurrieron en un sistema o red en particular. Además, este enfoque se apoya en el uso de herramientas y

técnicas especializadas para extraer, analizar y correlacionar estos registros de eventos, lo que proporciona una visión más completa de la seguridad de la información y ayuda a identificar posibles amenazas y vulnerabilidades.

Modelo de Rodney McKemmish

Según (Mckemmish, 1999), este modelo, concebido en Australia como respuesta a la necesidad de profundizar en diversas capas binarias, lleva el nombre de su creador y se centra en la reconstrucción detallada de acciones y eventos pasados. Su enfoque se basa en la comprensión profunda de las diferentes capas binarias presentes en los sistemas informáticos, lo que facilita la reconstrucción de incidentes y actividades pasadas.

Una característica distintiva de este modelo es la inclusión de cuatro criterios clave: Significado (Meaning), Error, Transparencia y Experiencia (Experience), que se utilizan para evaluar la admisibilidad de las evidencias en un eventual proceso judicial. Estos criterios garantizan que las evidencias recopiladas y analizadas cumplan con estándares rigurosos de integridad, autenticidad y confiabilidad, lo que aumenta su valor probatorio ante un tribunal.

Además, el modelo se centra en la identificación exhaustiva de las evidencias relevantes, asegurando su integridad física y aplicando mecanismos lógicos para evitar la pérdida de información durante el proceso de análisis. Esto contribuye a la solidez y credibilidad de las conclusiones obtenidas a partir de la investigación forense digital.

En este contexto donde aplicar metodologías sólidas en el proceso de peritaje informático es de vital importancia, los profesionales forenses digitales deben estar al tanto de las últimas tendencias y desarrollos en el campo, lo que destaca la necesidad de una formación continua y la adaptación de los métodos forenses a medida que surgen nuevas tecnologías y técnicas de ataque. Esto garantiza la eficacia y relevancia de las investigaciones forenses en los entornos digitales en constante cambio.

Dada la naturaleza dinámica y cambiante de la tecnología, se examinan teorías que se adaptan a la evolución constante de las amenazas cibernéticas y las tecnologías emergentes. Esto implica la consideración de enfoques teóricos que permitan a los peritos informáticos forenses mantenerse actualizados con las últimas tendencias, adoptando estrategias que se ajusten a la rápida innovación en el ámbito digital.

Otro tema relevante dentro del marco teórico del peritaje informático forense, es la consideración de teorías relacionadas con la ética y la legalidad en el manejo de la evidencia digital.

Según (Javier, 2018) la ética profesional en este campo implica la adhesión a principios morales y normas de conducta que garantizan la imparcialidad, la objetividad y el respeto a la privacidad de los individuos involucrados. Asimismo, se consideran las implicaciones legales de la recolección y presentación de pruebas digitales en el contexto judicial, asegurando que el proceso cumpla con los requisitos legales y normativas establecidas.

De tal manera se puede establecer que la ética profesional en el campo del peritaje informático forense es fundamental para garantizar la integridad y la imparcialidad en el proceso. Esto implica adherirse a principios morales y normas de conducta que aseguren la imparcialidad, la objetividad y el respeto a la privacidad de las partes involucradas.

Asimismo, se debe tener en cuenta las implicaciones legales de la recolección y presentación de pruebas digitales en el contexto judicial, asegurando que el proceso cumpla con los requisitos legales y normativas establecidas.

1.5.2. Marco contextual

En Ecuador el progresivo avance tecnológico ha impulsado una escalada significativa de los delitos cibernéticos, desencadenando una demanda cada vez mayor de peritaje informático forense. El Ecuador inmerso en una era donde la

conectividad digital y la dependencia de la tecnología son omnipresentes, se encuentra en la encrucijada de enfrentar desafíos específicos que afectan directamente la eficacia del peritaje informático. La intersección de la legislación, la formación especializada, la seguridad digital y la colaboración a nivel gubernamental e internacional proporciona una visión integral de los factores que impactan directamente en la efectividad del peritaje informático forense en el contexto ecuatoriano, para fines de la presente investigación, particularmente en Quito D.M.

En Ecuador, el Código Orgánico Integral Penal (COIP) ha sido promulgado como una herramienta fundamental para abordar los delitos digitales y establecer las pautas legales en el ámbito de la ciberseguridad y el peritaje informático forense, de hecho, en 2014 fue todo un hito al conseguir tipificar por primera vez al ciberdelito. Sin embargo, la naturaleza dinámica y vertiginosa de la evolución tecnológica plantea otros desafíos significativos en términos de adaptación normativa.

Según (García Brito & Arciniegas Castro, 2023) la rapidez con la que surgen nuevas tecnologías y modalidades delictivas en el entorno digital exige que la legislación se mantenga al día para poder abordar eficazmente estas amenazas. Esto implica la necesidad de revisar y actualizar regularmente las leyes y regulaciones pertinentes para garantizar su relevancia y efectividad en la lucha contra los delitos cibernéticos.

Además, la alineación de la legislación nacional con los estándares internacionales en materia de ciberseguridad y peritaje informático forense es crucial para facilitar la cooperación internacional en la investigación y persecución de delitos digitales.

(MINTEL, 2022) establece que la armonización de las leyes y regulaciones con los convenios y tratados internacionales fortalece la capacidad de los países para enfrentar los desafíos transnacionales en el ámbito digital.

En este sentido, es fundamental que el marco normativo ecuatoriano sea flexible y adaptable para responder de manera efectiva a los cambios en el panorama tecnológico y las nuevas amenazas que puedan surgir. Esto puede implicar la incorporación de disposiciones específicas que aborden aspectos como la protección de datos, la ciberseguridad empresarial, la responsabilidad de los proveedores de servicios en línea y la cooperación internacional en la lucha contra el cibercrimen.

En tal sentido, la actualización y adaptación constante de la legislación en materia de ciberseguridad y peritaje informático forense son fundamentales para garantizar la eficacia y la relevancia del marco legal en la protección de los ciudadanos, las empresas y las instituciones frente a las amenazas digitales en un entorno cada vez más interconectado y tecnológicamente avanzado.

Otro factor que impacta en la efectividad del peritaje informático forense es la formación de profesionales en el campo del peritaje informático lo cual es esencial para abordar las complejidades cambiantes de los delitos cibernéticos. La capacitación especializada, especialmente en el contexto del COIP y las leyes aplicables, se presenta como una necesidad crítica para garantizar que los peritos estén debidamente preparados para enfrentar los desafíos específicos del panorama digital ecuatoriano.

La Seguridad Digital y Delitos Cibernéticos es otro de los factores que impactan al peritaje informático forense, el aumento de la conectividad digital ha propiciado un incremento en los delitos cibernéticos en Ecuador; por lo que la seguridad digital se convierte en una preocupación prioritaria, y el marco contextual explorará las amenazas específicas que enfrenta el país, así como las consecuencias económicas y sociales de estos delitos.

Por otra parte la Colaboración Gubernamental y Acuerdos Internacionales es un factor que impacta directamente a la efectividad del peritaje informático forense, de tal manera que la colaboración entre el gobierno ecuatoriano y organismos

internacionales en materia de seguridad digital desempeña un papel crucial en la lucha contra las amenazas cibernéticas. Ecuador, al igual que otros países, reconoce la importancia de trabajar en conjunto con organismos internacionales, como la Interpol, la Organización de las Naciones Unidas (ONU) y la Organización de Estados Americanos (OEA), así como también de participar en acuerdos específicos, como el Convenio de Budapest sobre Ciberdelincuencia.

Según (Na & Hipertensiva, 2022) el Convenio de Budapest, es un tratado internacional que tiene como objetivo abordar los delitos cibernéticos y promover la cooperación internacional en la investigación y persecución de estos delitos. Este convenio establece un marco legal común para combatir el cibercrimen, incluyendo disposiciones relacionadas con la recolección de pruebas digitales, la protección de datos y la cooperación entre países en la extradición de sospechosos y la asistencia judicial mutua.

La adhesión al Convenio de Budapest brinda a Ecuador acceso a recursos y herramientas internacionales que pueden fortalecer su capacidad para investigar y prevenir delitos cibernéticos. Además, este convenio proporciona pautas y estrategias para el desarrollo de políticas y marcos legales nacionales en materia de seguridad digital y peritaje informático forense.

La colaboración con otros países y organismos internacionales también permite a Ecuador intercambiar información y mejores prácticas en el ámbito de la ciberseguridad y el peritaje informático forense. Esto puede incluir la capacitación de personal especializado, el intercambio de tecnologías y herramientas forenses, y la participación en ejercicios conjuntos de respuesta a incidentes cibernéticos.

De tal manera, la colaboración con organismos internacionales, en particular a través de acuerdos como el Convenio de Budapest, es fundamental para fortalecer la capacidad de Ecuador en la lucha contra los delitos cibernéticos y garantizar la eficacia del peritaje informático forense en un entorno digital cada vez más complejo y globalizado.

Otro de los factores que afectan directamente a la efectividad del peritaje informático forense es el acceso a la Tecnología y Brecha Digital, la disponibilidad y el acceso equitativo a la tecnología son consideraciones importantes en el contexto ecuatoriano. La brecha digital puede afectar la uniformidad en la práctica del peritaje informático forense a lo largo del territorio Ecuatoriano.

El acceso equitativo a la tecnología es un factor crucial que influye directamente en la efectividad del peritaje informático forense en Ecuador. Aunque el país ha experimentado avances significativos en términos de conectividad y acceso a internet en los últimos años, aún persisten disparidades importantes en cuanto a la disponibilidad y el uso de tecnologías digitales en diferentes regiones y sectores de la población.

Una de las brechas digitales más significativas en Ecuador es la disparidad rural-urbana. Mientras que las áreas urbanas suelen tener una infraestructura tecnológica más desarrollada y un acceso más fácil a internet de alta velocidad y dispositivos digitales, las zonas rurales pueden enfrentar mayores desafíos en términos de conectividad y acceso a tecnología. Esto puede dificultar el acceso de las comunidades rurales a servicios de peritaje informático forense, limitando así su capacidad para investigar y resolver delitos digitales en estas áreas.

Además, la brecha generacional en el uso de la tecnología también puede influir en la efectividad del peritaje informático forense. Mientras que las generaciones más jóvenes suelen estar más familiarizadas con el uso de dispositivos digitales y herramientas tecnológicas, las personas mayores pueden enfrentar mayores dificultades para adaptarse a los avances tecnológicos y utilizar herramientas de peritaje informático forense de manera efectiva. Esto puede afectar la calidad y la uniformidad de las investigaciones digitales forenses, especialmente cuando se trata de casos que involucran a personas de diferentes grupos de edad.

En tal sentido, la brecha digital en Ecuador presenta desafíos importantes para la efectividad del peritaje informático forense, especialmente en términos de

acceso equitativo a la tecnología y habilidades digitales. Abordar estas disparidades y promover un acceso más amplio y equitativo a la tecnología son pasos fundamentales para fortalecer la capacidad del país en la investigación y prevención de delitos digitales mediante el uso de técnicas forenses digitales, por lo que se examinará cómo estas disparidades influyen en la capacidad de llevar a cabo investigaciones digitales forenses de manera efectiva.

1.5.3. Marco Legal

En el marco legal, se lleva a cabo un análisis exhaustivo del contexto jurídico ecuatoriano, poniendo especial énfasis en el Código Orgánico Integral Penal (COIP) y otras normativas vinculadas. Este componente busca no solo comprender cómo estas leyes rigen la adquisición, tratamiento y presentación de evidencia digital en procedimientos judiciales, sino también evaluar su eficacia y coherencia con estándares internacionales.

El eje central del análisis legal se concentra en el COIP, identificando las disposiciones específicas que regulan el peritaje informático forense. Se examinan los procedimientos establecidos para la obtención de evidencia digital, la cadena de custodia, y las garantías procesales asociadas a la pericia informática. Este análisis proporciona una visión detallada de cómo la legislación ecuatoriana aborda los desafíos del peritaje informático en el ámbito legal.

Además del COIP, se exploran otras legislaciones pertinentes que puedan tener implicaciones directas o indirectas en el peritaje informático forense. Esto puede incluir leyes relacionadas con la protección de datos, privacidad electrónica y delitos informáticos. La comprensión de este marco legal amplio con base en el derecho comparado es esencial para contextualizar la práctica del peritaje informático dentro de un marco normativo integral.

Como una guía fundamental para el tratamiento de la evidencia digital en el contexto de esta investigación, se menciona la "RFC 3227: Guía Para Recolectar y Archivar Evidencia". Esta guía, redactada en febrero de 2002 por Dominique

Brezinski y Tom Killalea, ingenieros del Network Working Group, proporciona un marco de alto nivel para la recolección y archivado de evidencia digital. Este documento es de particular importancia debido a su enfoque detallado en los procedimientos y mejores prácticas para preservar la integridad y autenticidad de la evidencia a lo largo del proceso forense.

En el mismo contexto, se analizan las disposiciones específicas que buscan de establecer una estandarización, una buena práctica para la adquisición, tratamiento y presentación de la evidencia digital. Esto implica una revisión exhaustiva de cómo se define y reconoce la evidencia digital dentro del marco legal, así como los protocolos establecidos para su obtención y manejo. Se presta especial atención a la garantía de la integridad y autenticidad de la evidencia a lo largo de este proceso, asegurando que se cumplan los estándares establecidos tanto a nivel nacional como internacional.

La estandarización es esencial para garantizar la fiabilidad y la validez de la evidencia digital presentada en los procedimientos judiciales, lo que contribuye a la integridad del proceso. Además, se lleva a cabo una comparación con estándares internacionales reconocidos en el ámbito del peritaje informático forense. Este análisis va más allá de las fronteras nacionales, permitiendo identificar posibles brechas o divergencias entre las disposiciones legales ecuatorianas y los estándares internacionales.

La referencia a estos estándares internacionales no solo sirve para evaluar la consistencia y efectividad de la legislación nacional en este campo, sino que también contribuye a la formulación de recomendaciones alineadas con las mejores prácticas a nivel global. Esta comparación facilita el intercambio de conocimientos y experiencias entre jurisdicciones, promoviendo así una mayor armonización y eficacia en la regulación del peritaje informático forense tanto a nivel nacional como internacional.

La evaluación del marco legal se enfoca en identificar posibles brechas o áreas de mejora que puedan obstaculizar la eficacia del peritaje informático forense. Esto puede incluir aspectos relacionados con la claridad de las normativas, la adaptabilidad a avances tecnológicos y la congruencia con estándares internacionales.

Al identificar estas brechas y áreas de mejora, se pueden desarrollar recomendaciones específicas para mejorar la práctica del peritaje informático forense, garantizando así su alineación con los más altos estándares internacionales y su capacidad para abordar eficazmente los desafíos del entorno digital actual**.**

Este análisis detallado del marco legal proporciona una base sólida para comprender cómo la legislación ecuatoriana aborda el peritaje informático forense, permitiendo identificar puntos de mejora para el fortalecimiento que contribuyan a un entorno más eficaz y confiable en el ámbito jurídico digital.

CAPÍTULO II

MARCO METODOLÓGICO

2.1. Métodos de investigación

En este capítulo se detalla la metodología empleada para llevar a cabo la investigación sobre el peritaje informático forense en el contexto del Distrito Metropolitano de Quito. Se describen tanto el método lógico como los métodos empíricos utilizados, en relación con los objetivos formulados.

El método lógico, según (Blanqueto, 2019), se fundamenta en la revisión crítica y analítica de la literatura existente, teorías, conceptos y principios relevantes para comprender un fenómeno o problema de estudio. Este enfoque busca construir un marco teórico sólido que oriente el análisis y la interpretación de los hallazgos empíricos, proporcionando así una base conceptual para la investigación.

Siguiendo este enfoque, el método lógico constituye el fundamento teórico y conceptual de la presente investigación sobre peritaje informático forense. Se apoya en la revisión crítica y analítica de la literatura existente en esta área, así como en la exploración de teorías, conceptos y principios relevantes para una comprensión clara del tema de estudio.

Este método se erige como el pilar sobre el cual se construye un marco teórico robusto que guía tanto el análisis como la interpretación de los hallazgos empíricos obtenidos. En consecuencia, la investigación se apoya en fuentes académicas, literatura especializada, normativas legales y documentos técnicos relacionados con el peritaje informático forense. Se lleva a cabo una revisión exhaustiva de estudios previos, artículos científicos, libros y guías de buenas prácticas en el campo de la informática forense.

Esta revisión permite identificar las tendencias, los desafíos y las brechas existentes en el ámbito del peritaje informático, proporcionando así una base sólida para el diseño y la implementación de la investigación empírica.

Para complementar el enfoque lógico, se emplean métodos empíricos que permitan recopilar datos concretos y verificables sobre la aplicación del peritaje informático forense en Ecuador, particularmente, en la ciudad de Quito.

Según (Nur, 2020), el método empírico se refiere a la recopilación de datos a través de la observación directa o la experiencia práctica. En el contexto de la investigación, implica la utilización de técnicas que involucran la recolección de datos del mundo real, ya sea a través de experimentos, encuestas, entrevistas, observaciones u otras formas de interacción con el objeto de estudio.

Después de considerar el método empírico mencionado por (Nur, 2020), es importante destacar que en el proceso de investigación se utilizó el método Delphi. El método Delphi según (Torrado-fonseca, 2016), es una técnica de recopilación de datos que involucra a un panel de expertos que participan en rondas sucesivas de preguntas e intercambios de opiniones de forma anónima.

Este enfoque permite obtener información y opiniones de manera sistemática y estructurada, facilitando la identificación de tendencias, consensos y discrepancias en el campo de estudio. En el contexto de esta investigación, el método Delphi complementó el enfoque empírico al proporcionar una perspectiva adicional y una validación de los hallazgos obtenidos a través de otras técnicas de recolección de datos del mundo real.

Siguiendo este enfoque, las estrategias empíricas empleadas en esta investigación comprenden encuestas exhaustivas y análisis documental. Estas metodologías posibilitan la obtención de datos directamente del terreno de estudio, lo que conlleva a una comprensión minuciosa y detallada de los aspectos relacionados con el peritaje informático forense.

Se llevó a cabo encuestas estructuradas con peritos informáticos, juristas y otros profesionales relevantes en el campo del peritaje informático forense en Quito D.M.

Se seleccionaron seis peritos informáticos exclusivamente de la ciudad de Quito, quienes cumplían con los siguientes requisitos: estar acreditados como peritos informáticos forenses por el Consejo de la Judicatura, haber participado en análisis forense digital, contar con al menos un año de experiencia. En cuanto a la selección de los cuatro juristas, se basó en su experiencia en casos relacionados con peritaje informático forense, así como en su conocimiento y manejo de la legislación pertinente en esta área.

Estas encuestas proporcionaron información detallada sobre las experiencias, percepciones y desafíos enfrentados en la práctica del peritaje informático en el contexto local. Se prestó especial atención a la identificación de brechas en las prácticas y recursos disponibles para los peritos informáticos en la región.

Se examinaron minuciosamente diversos documentos relacionados con el peritaje informático forense, tales como guías, protocolos de actuación, informes técnicos, publicaciones académicas y científicas sobre temas relacionados con la informática forense, así como documentos técnicos y de investigación, incluyendo estudios de casos y análisis de tendencias.

Este análisis exhaustivo permitió recabar datos concretos y objetivos que respaldan y enriquecen los hallazgos obtenidos a través de las encuestas en profundidad. Esta revisión documental es esencial para cimentar la investigación, proporcionando un contexto sólido y una comprensión profunda del tema abordado.

2.2. Enfoque de la investigación, tipo de diseño de investigación y alcance.

2.2.1. Enfoque de la investigación

La investigación adopta una estrategia metodológica que integra métodos cualitativos y la realización de una investigación documental. Este enfoque se selecciona para obtener una comprensión profunda y multifacética del peritaje informático forense en su aplicación práctica.

En cuanto a la recopilación cualitativa de datos, se realizó mediante encuestas en profundidad con actores claves, incluidos peritos informáticos, y juristas con experiencia relevante en el campo. Estas encuestas sirven para obtener perspectivas detalladas sobre sus experiencias, desafíos y percepciones en el ámbito del peritaje informático forense. A través de estas interacciones, se capta no solo los aspectos técnicos y legales del peritaje informático, sino también las implicaciones prácticas y éticas que enfrentan los profesionales en su trabajo diario.

Simultáneamente, se realiza una investigación documental exhaustiva que abarca la revisión de normativas, leyes, reglamentos, guías y literatura relevante relacionada con el peritaje informático forense, casuística inclusive. Este análisis documental proporciona una base sólida para contextualizar el marco legal y regulatorio que influye en el ámbito investigado. Además, permite identificar las mejores prácticas, tendencias emergentes y debates actuales en el campo, enriqueciendo así la comprensión global de la problemática estudiada.

Se ha optado por un enfoque de investigación mixto con el fin de recopilar datos que proporcionen una visión completa y enriquecedora de los desafíos del peritaje informático forense. Esta combinación de métodos cualitativos y de investigación documental permite obtener una comprensión profunda y exhaustiva de las brechas identificadas.

La integración de métodos cualitativos, mediante encuestas en profundidad, junto con la investigación documental, proporciona una perspectiva integral del

peritaje informático forense en el contexto ecuatoriano. Esta combinación metodológica permite no solo una descripción detallada, sino también una comprensión enriquecida de la situación actual, sentando así una base sólida para el ejercicio del perito informático forense.

Al obtener una perspectiva amplia y complementaria que aborda la complejidad del tema desde diversos ángulos, facilita la identificación de patrones, discrepancias y áreas de mejora. Esta estrategia no solo ofrece un análisis exhaustivo, sino que también contribuye significativamente a la generación de conocimientos aplicables, guiando el desarrollo de políticas, prácticas y futuras investigaciones en este ámbito crucial para la intersección entre el ámbito legal y tecnológico.

2.2.2. Tipo de diseño de investigación

El diseño de la investigación se estructura como exploratorio-descriptivo, este diseño se selecciona para permitir una comprensión profunda y detallada de las brechas y desafíos en el peritaje informático forense. La elección de un diseño mixto posibilita la recopilación de datos que facilitan una visión completa y enriquecedora de la problemática.

2.2.2.1. Diseño de Investigación Exploratorio

Según (Meza, 2017) el diseño de investigación exploratorio tiene como objetivo explorar y comprender fenómenos que son poco conocidos o comprendidos, sin estar limitado por hipótesis preconcebidas. Su finalidad es generar nuevas ideas, comprensiones o teorías sobre un tema específico.

En el contexto del peritaje informático forense, este enfoque permite abordar las brechas y desafíos desde diversas perspectivas, sin imponer suposiciones previas, lo que facilita una comprensión más completa considerando el carácter práctico que tiene en los procesos de judicialización.

2.2.2.2. Diseño de Investigación Descriptivo

(Martinez, 2018) señala que el diseño de investigación descriptivo se centra en la descripción detallada y sistemática de un fenómeno, situación o problema, sin la intención de establecer relaciones causales entre variables. Su objetivo principal es proporcionar una representación precisa y completa de las características, comportamientos o condiciones presentes en un contexto específico.

En el caso del peritaje informático forense, un enfoque descriptivo permitiría identificar y analizar de manera detallada las brechas y desafíos en esta área, proporcionando una visión clara y objetiva de la situación actual. Este diseño de investigación es fundamental para comprender en profundidad las características y complejidades del peritaje informático forense, lo que a su vez sirve como base para el desarrollo de estrategias de mejora y optimización.

2.2.3. Alcance de la Investigación

El alcance de la investigación se centra en examinar las deficiencias en la aplicación de estándares y protocolos en el peritaje informático forense en la ciudad de Quito, Distrito Metropolitano. Se investigarán específicamente las prácticas y herramientas utilizadas para la adquisición, preservación y análisis de evidencia digital por parte de los peritos informáticos. El estudio también analizará cómo estas deficiencias pueden afectar la validez y confiabilidad de la evidencia presentada en los tribunales, así como las implicaciones legales de su falta de aplicación.

Además, se explorarán las necesidades de formación y capacitación de los peritos informáticos y la comprensión de los profesionales del derecho sobre los principios y procedimientos de la informática forense. Se investigará cómo se abordan los dilemas éticos en la práctica pericial y se propondrán recomendaciones para mejorar la formación y actualización profesional en el campo.

En tal sentido, la investigación proporciona una evaluación detallada de las deficiencias en la aplicación de estándares en el peritaje informático forense en

Quito, así como recomendaciones concretas para fortalecer su validez y confiabilidad en el proceso pericial.

2.3. Unidad de Análisis, población y muestra

La investigación se enfoca en la aplicación del método Delphi para analizar el proceso de peritaje informático en el Distrito Metropolitano de Quito. En lugar de una población y muestra tradicionales, el método Delphi se basa en la selección de expertos en el campo del peritaje informático, así como otros profesionales involucrados en los procesos de forensia digital, por ejemplo abogados. Estos expertos son elegidos por su experiencia y conocimiento relevante en el tema en cuestión.

La unidad de análisis se centra en las opiniones y percepciones de estos expertos, recopiladas a través de múltiples rondas de cuestionarios estructurados y retroalimentación. El objetivo es obtener una comprensión profunda del proceso de peritaje informático en Quito D.M., identificar áreas de consenso y discrepancia entre los expertos, y desarrollar recomendaciones para mejorar la práctica del peritaje informático en la región.

2.3.1. Población

Para el método Delphi, el término "población" se refiere a la selección inicial de expertos que participarán en el proceso. En este caso, la población estaría compuesta por profesionales altamente calificados y con experiencia en el campo del peritaje informático en el Distrito Metropolitano de Quito. Estos expertos incluyen peritos informáticos, y abogados con experiencia en casos relacionados con evidencia digital.

La población se seleccionó cuidadosamente para garantizar una representación adecuada de diferentes áreas de especialización y perspectivas dentro del campo del peritaje informático. La inclusión de una variedad de expertos

permitirá obtener una gama más amplia de opiniones y perspectivas durante el proceso.

La selección de la población es un paso crucial en el método aplicado, ya que la calidad y la relevancia de los resultados dependen en gran medida de la experiencia y diversidad de los participantes. Una vez seleccionada la población inicial, estos expertos fueron invitados a participar en las rondas de cuestionarios y retroalimentación del proceso para recopilar y analizar sus opiniones y percepciones sobre el peritaje informático en Quito D.M.

2.3.2. Muestra

En el método aplicado, el concepto de "muestra" se interpreta de manera diferente en comparación con otros enfoques de investigación. En lugar de seleccionar una muestra representativa de una población más amplia, como se haría en métodos cuantitativos, en el método Delphi se trabaja con una muestra de expertos que han sido cuidadosamente seleccionados para participar en el proceso.

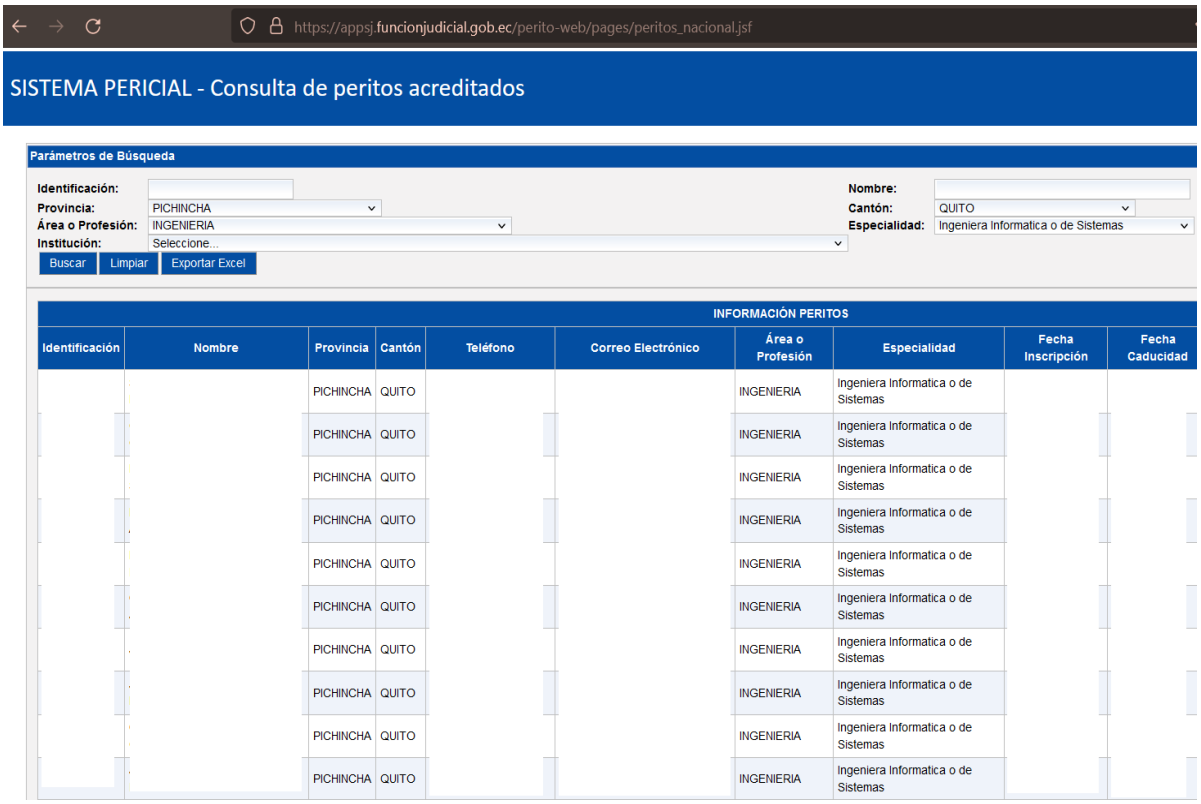
La muestra en el método Delphi consiste en el grupo de expertos que se ha elegido para proporcionar sus opiniones y conocimientos sobre el tema en cuestión. Estos expertos constituyen la muestra de este método, y su experiencia y perspectivas son fundamentales para el éxito del proceso.

Es importante seleccionar una muestra diversa y representativa de expertos en el campo del peritaje informático en el Distrito Metropolitano de Quito. La muestra debe incluir a profesionales con una amplia gama de experiencias, conocimientos y perspectivas relevantes para el tema de investigación. Esto garantizará que se capturen diferentes puntos de vista y se obtengan resultados más robustos y completos durante las rondas de retroalimentación del método Delphi.

La selección de la muestra será mediante un muestreo intencional, priorizando la representatividad de peritos informáticos forenses y profesionales del derecho en el contexto de Quito- Ecuador.

En consideración a la presencia de los 21 peritos acreditados por el Consejo de la Judicatura en la especialidad de Ingeniería Informática o de Sistemas en la Provincia de Pichincha Cantón Quito, se tomó como muestra 6 peritos acreditados en esta jurisdicción y 4 profesionales de derecho lo cual permitirá obtener una muestra que obtenga las distintas perspectivas y prácticas laborales de los profesionales especializados en investigaciones digitales dentro de la localidad, asegurando la obtención de información completa y representativa para los objetivos específicos de la investigación.

Figura 11. *Consulta Sistema Pericial - Consulta Peritos Acreditados*



Fuente: Tomada del sitio Web: https://appsj.funcionjudicial.gob.ec/perito-web/pages/peritos_nacional.jsf

2.4. Variables de la investigación

En esta investigación, se abordan diversos temas relacionados con el proceso de peritaje informático en el Distrito Metropolitano de Quito. Estos temas

incluyen, entre otros, la preservación de la integridad de la evidencia digital, los protocolos y prácticas utilizados en la recolección y análisis de evidencia digital, los desafíos y oportunidades en la aplicación de técnicas forenses digitales, así como la legislación y regulación vigente en el ámbito del peritaje informático forense.

Dado que el enfoque metodológico de esta investigación se basa en el método Delphi, no se utilizan variables de investigación en el sentido tradicional, es decir, no se basará en una cuantificación basada en métodos estadísticos sino en reconocer un consenso en las respuestas y opiniones del panel de expertos. Para ello, se identifican y exploran estos temas clave para comprender mejor el proceso de peritaje informático en Quito D.M. Cada uno de estos temas será abordado a través del método Delphi, utilizando la participación de expertos seleccionados cuidadosamente en el campo del peritaje informático.

Este método permite una exploración más amplia y flexible de los aspectos esenciales del tema de investigación, así como la recopilación de opiniones y percepciones de expertos para enriquecer el análisis y las conclusiones de la investigación.

2.5. Tabla de categorización

En esta investigación cualitativa, la tabla de categorización desempeña un papel fundamental en la organización y el análisis de los datos recopilados a través de las entrevistas realizadas a los peritos informáticos forenses y juristas. Esta herramienta proporciona una estructura clara y sistemática para identificar, clasificar y comprender los temas y patrones emergentes en las respuestas de los participantes.

La construcción de la tabla de categorización se basa en las variables de investigación y los objetivos específicos del estudio. Esto garantiza que las categorías y subcategorías incluidas en la tabla estén directamente relacionadas con los aspectos clave que se pretenden explorar y comprender en el contexto del peritaje informático forense en Quito D.M.

Cada categoría y subcategoría en la tabla representa un aspecto relevante del fenómeno investigado, como las experiencias laborales de los peritos, sus competencias técnicas, las percepciones sobre el proceso de peritaje y otros temas pertinentes. Al organizar los datos en estas categorías, se facilita la identificación de patrones, tendencias y diferencias significativas en las respuestas de los participantes.

La tabla de categorización proporciona una estructura analítica que guía el proceso de análisis de datos, permitiendo una comprensión más profunda y detallada de las perspectivas y experiencias de los participantes en relación con el peritaje informático forense en Quito D.M.

Tabla 1. Tabla de Categorización

Categoría Principal	Subcategorías/dimensiones
Experiencias Laborales	Tipo de casos atendidos
	Desafíos enfrentados
	Estrategias utilizadas
Competencias Técnicas	Conocimientos informáticos
	Experiencia en herramientas forenses
	Capacitación recibida
	Certificaciones y acreditaciones
Desafíos	Importancia del peritaje informático
	Confianza en los resultados periciales
	Percepción de la calidad del trabajo
Mejores prácticas	Opiniones sobre protocolos recomendados en la adquisición de evidencia
Percepciones	Actitudes hacia la aceptación de evidencia digital en juicios

2.6. Fuentes, técnicas e instrumentos para la recolección de información

2.6.1. Fuentes de Información:

Documental: Se revisaron leyes, normativas y protocolos tanto nacionales como internacionales vinculados al peritaje informático forense en Quito D.M. Esto incluirá el análisis de informes periciales previos y casos judiciales relevantes para obtener una perspectiva con base, inclusive, en la jurisprudencia asociada.

Encuestas Complementarias: Además, para enriquecer la comprensión del contexto local y complementar la recolección de datos, se llevarán a cabo encuestas a peritos informáticos forenses en Quito D.M, así como con profesionales del ámbito legal y judicial. Estas encuestas tienen como objetivo recoger experiencias y percepciones específicas del contexto local, abordando temas relacionados con los desafíos, prácticas y enfoques en el peritaje informático forense en la región.

2.6.2. Técnicas de Recolección de Datos:

Revisión Bibliográfica:

La revisión exhaustiva de literatura especializada permitirá comprender la evolución del peritaje informático forense en el país y su alineación con estándares internacionales. Este proceso de revisión bibliográfica servirá como base de conocimientos para contextualizar las rondas del método Delphi, proporcionando información relevante sobre las prácticas actuales y los desafíos en el campo del peritaje informático forense en Quito D.M.

Ronda de preguntas:

Las rondas de preguntas seguirán un formato estructurado, asegurando la uniformidad en la obtención de datos y facilitando la comparación entre respuestas de distintos participantes en las rondas sucesivas del método. Este enfoque permite la recopilación sistemática de opiniones y percepciones de expertos en el campo

del peritaje informático forense en el contexto ecuatoriano, contribuyendo así a la comprensión profunda de la práctica del peritaje informático en el país.

Análisis Documental:

Además de las encuestas Delphi, se llevará a cabo un análisis minucioso de documentos legales, informes periciales y cualquier material relevante. Este análisis documental complementará las respuestas de los participantes en las encuestas Delphi, proporcionando una visión más completa de la práctica del peritaje informático forense en el contexto ecuatoriano.

2.6.3. Instrumentos de Recolección de Datos:

Para facilitar el proceso de recopilación de datos en el método Delphi, se elaboraron cuestionarios estructurados. Estos cuestionarios, diseñados con preguntas clave, sirvieron como guía para los participantes en cada ronda del estudio.

Estas preguntas están formuladas para abordar aspectos específicos relacionados con el peritaje informático forense en el contexto de Quito D.M. La estructura del cuestionario aseguró la uniformidad en la obtención de datos y facilitó la comparación entre las respuestas de los distintos participantes en las rondas sucesivas del método Delphi.

Además de los cuestionarios, se implementó una matriz de preguntas versus dimensiones para la evaluación de la comprensión y desafíos en las brechas del peritaje informático forense.

Esta matriz se diseñó para organizar sistemáticamente las preguntas de los cuestionarios en función de las dimensiones o categorías relevantes del estudio. Con esta matriz, fue posible relacionar las respuestas de los participantes con aspectos específicos del peritaje informático, como experiencias laborales, competencias técnicas, desafíos enfrentados, entre otros. La creación de esta

matriz permitió una mejor comprensión y análisis de los datos recopilados, facilitando la identificación de patrones y tendencias a lo largo de las rondas del método Delphi.

CUESTIONARIOS

RONDA 1: IDENTIFICAR FACTORES DE LA FALTA DE COMPRENSIÓN DEL PROCESO EN INVESTIGACIONES DIGITALES.

1. **¿Cuáles considera que son los principales factores que contribuyen a la falta de comprensión del proceso en investigaciones digitales en el contexto de Quito D.M.?**
    a) Falta de capacitación en metodologías forenses digitales
    b) Ausencia de protocolos claros y definidos
    c) Limitaciones tecnológicas en la adquisición y análisis de evidencia digital
    d) Otros (especificar)

2. **¿Qué carencias de procedimientos específicos cree que impactan en la validez de la evidencia digital en el ámbito forense?**
    a) La no aplicación de protocolos de preservación de la evidencia
    b) Ausencia de directrices para la autenticación de la evidencia digital
    c) Limitaciones en la cadena de custodia digital
    d) Otros (especificar)

3. **¿Cómo afecta la ausencia de ciertos procedimientos al desarrollo de investigaciones digitales en el contexto local?**
    a) Dificulta la preservación adecuada de la evidencia digital
    b) Compromete la integridad de la cadena de custodia digital
    c) Impacta la fiabilidad de los resultados periciales

d) Otros (especificar)

4. **¿Como percibe el nivel de comprensión del proceso en investigaciones digitales por parte de los profesionales del ámbito legal y judicial en Quito D.M.?**
    a) Insuficiente
    b) Moderado
    c) Suficiente
    d) Excelente

5. **¿Qué recomendaciones sugeriría para mejorar la comprensión del proceso en investigaciones digitales en la ciudad?**
    a) Implementar programas de capacitación en metodologías forenses digitales
    b) Establecer protocolos claros y actualizados para la recolección y preservación de evidencia digital
    c) Fomentar la colaboración entre peritos informáticos y profesionales del ámbito legal
    d) Otros (especificar)

RONDA 2: DETERMINAR LOS DESAFÍOS TECNOLÓGICOS DE PERITOS INFORMÁTICOS.

1. **Basado en las respuestas de la primera ronda, ¿está de acuerdo con los factores identificados como contribuyentes a la falta de comprensión del proceso en investigaciones digitales?**
    a. Sí
    b. No
    c. Parcialmente

2. **¿Cuáles son los principales desafíos tecnológicos que enfrentan los peritos informáticos forenses en Quito D.M.?**
    a. Escasez de herramientas especializadas para análisis forense
    b. Dificultades en la adquisición de evidencia de dispositivos protegidos
    c. Limitaciones en la interpretación de datos complejos
    d. Otros (especificar)

3. **¿Qué tecnologías específicas o herramientas considera que son necesarias para abordar estos desafíos tecnológicos?**
    a. Software de análisis forense de última generación
    b. Herramientas de recuperación de datos avanzadas
    c. Dispositivos de almacenamiento seguros y compatibles con estándares forenses
    d. Otros (especificar)

4. **¿Cómo crees que la falta de acceso o capacitación en tecnologías específicas afecta el trabajo de los peritos informáticos en la ciudad?**
    a. Limita la capacidad de llevar a cabo investigaciones digitales efectivas

b. Dificulta la identificación y preservación adecuada de la evidencia digital
c. Impacta la credibilidad de los resultados periciales
d. Otros (especificar)

5. **¿Qué recomendaciones propondrías para superar los desafíos tecnológicos identificados en el peritaje informático forense en Quito D.M.?**
    a. Establecer programas de capacitación en herramientas forenses específicas
    b. Facilitar el acceso a tecnologías forenses de última generación
    c. Promover la colaboración con expertos en tecnología y ciberseguridad
    d. Otros (especificar)

RONDA 3: INVESTIGAR LA FALTA DE CAPACITACIÓN EN METODOLOGÍAS FORENSES DIGITALES.

1. **¿Estás de acuerdo con los desafíos tecnológicos identificados en la segunda ronda?**
    a) Sí
    b) No
    c) Parcialmente

2. **¿Cómo crees que la falta de capacitación en metodologías forenses digitales impacta la fiabilidad de los resultados periciales en Quito D.M.?**
    a) Compromete la calidad del análisis forense
    b) Aumenta el riesgo de errores en la interpretación de datos
    c) Impacta la objetividad y neutralidad de los peritajes
    d) Otros (especificar)

3. **¿Qué aspectos específicos de las metodologías forenses digitales considera que son necesarios mejorar en la capacitación de los peritos informáticos?**
    a) Técnicas de adquisición y preservación de evidencia digital
    b) Análisis de malware y vulnerabilidades de seguridad
    c) Interpretación de resultados y elaboración de informes periciales
    d) Otros (especificar)

4. **¿Qué acciones específicas podrían implementarse para mejorar la formación y capacitación de los peritos informáticos forenses en la ciudad?**
    a) Desarrollar programas de formación especializados en metodologías forenses digitales

b) Promover la certificación y acreditación de peritos informáticos
c) Establecer convenios de colaboración con instituciones académicas y centros de investigación
d) Otros (especificar)

5. **¿Qué papel deberían desempeñar las instituciones académicas, las organizaciones profesionales y el Consejo de la Judicatura en la mejora de la capacitación de metodologías forenses digitales?**
    a) Desarrollar programas académicos especializados en peritaje informático forense
    b) Ofrecer oportunidades de formación continua y actualización profesional
    c) Fomentar la investigación y el desarrollo de nuevas metodologías forenses
    d) Otros (especificar)

En cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPD) del Ecuador, se ha tomado la decisión de no incluir el nombre de los expertos en el formulario de la ronda de preguntas. Esta medida se adopta con el fin de garantizar el cumplimiento de los principios fundamentales de protección de datos, como la privacidad, la confidencialidad y la seguridad de la información personal.

La LOPD establece que los datos personales deben ser tratados de manera lícita, leal y transparente, y que se deben adoptar medidas adecuadas para garantizar su seguridad y protección. En este sentido, la omisión del nombre de los expertos en el formulario de preguntas contribuye a respetar el derecho a la privacidad de los participantes, al evitar la divulgación de información personal que no sea estrictamente necesaria para el propósito del estudio.

Asimismo, la LOPD establece que el tratamiento de datos personales debe limitarse a lo necesario y relevante para el cumplimiento de los fines específicos del

tratamiento. En el contexto de este estudio, la identificación de los participantes por su nombre no es esencial para el análisis de las respuestas y la obtención de conclusiones pertinentes sobre las brechas del peritaje informático forense en el contexto de Quito D.M. Por lo tanto, la exclusión de esta información contribuye a minimizar el procesamiento de datos personales y a cumplir con el principio de minimización de datos.

En conclusión, la decisión de no incluir el nombre de los expertos en el formulario de la ronda de preguntas se fundamenta en el respeto a la privacidad y la protección de datos personales de acuerdo con los principios y disposiciones establecidos en la Ley Orgánica de Protección de Datos Personales del Ecuador. Esta medida asegura que el estudio se realice de manera ética y legalmente conforme, sin comprometer la integridad ni la confidencialidad de la información de los participantes.

Tabla 2. Matriz de Preguntas vs Dimensiones para la Evaluación de la Comprensión de las Brechas del Peritaje Informático Forense.

Ronda	Pregunta	Categoría Principal	Subcategoría/Dimensión
Ronda 1	1. ¿Cuáles considera que son los principales factores que contribuyen a la falta de comprensión del proceso en investigaciones digitales en el contexto de Quito D.M.?	Desafíos	Importancia del peritaje informático
Ronda 1	2. ¿Qué carencias de procedimientos específicos cree que impactan en la validez de la evidencia digital en el ámbito forense?	Desafíos	Percepción de la calidad del trabajo
Ronda 1	3. ¿Cómo afecta la ausencia de ciertos procedimientos al desarrollo de investigaciones digitales en el contexto local?	Desafíos	Confianza en los resultados periciales
Ronda 1	4. ¿Cuál es su percepción sobre como percibe el nivel de comprensión del proceso en investigaciones digitales por	Percepciones	Actitudes hacia la aceptación de evidencia digital en juicios

	parte de los profesionales del ámbito legal y judicial en Quito D.M.?		
Ronda 1	5. ¿Qué recomendaciones sugeriría para mejorar la comprensión del proceso en investigaciones digitales en la ciudad?	Mejores Prácticas	Opiniones sobre protocolos recomendados en la adquisición de evidencia
Ronda 2	1. Basado en las respuestas de la primera ronda, ¿está de acuerdo con los factores identificados como contribuyentes a la falta de comprensión del proceso en investigaciones digitales?	-	-
Ronda 2	2. ¿Cuáles son los principales desafíos tecnológicos que enfrentan los peritos informáticos forenses en Quito D.M.?	Desafíos	Importancia del peritaje informático
Ronda 2	3. ¿Qué tecnologías específicas o herramientas considera que son necesarias para abordar estos desafíos tecnológicos?	Competencias Técnicas	Experiencia en herramientas forenses
Ronda 2	4. ¿Cómo crees que la falta de acceso o capacitación en tecnologías específicas afecta el trabajo de los peritos informáticos en la ciudad?	Competencias Técnicas	Capacitación recibida
Ronda 2	5. ¿Qué recomendaciones propondrías para superar los desafíos tecnológicos identificados en el peritaje informático forense en Quito D.M.?	Mejores Prácticas	Opiniones sobre protocolos recomendados en la adquisición de evidencia
Ronda 3	1. ¿Estás de acuerdo con los desafíos tecnológicos identificados en la segunda ronda?	-	-
Ronda 3	2. ¿Cómo crees que la falta de capacitación en metodologías forenses digitales impacta la fiabilidad de los resultados periciales en Quito D.M.?	Competencias Técnicas	Capacitación recibida

Ronda 3	3. ¿Qué aspectos específicos de las metodologías forenses digitales considera que son necesarios mejorar en la capacitación de los peritos informáticos?	Competencias Técnicas	Capacitación recibida
Ronda 3	4. ¿Qué acciones específicas podrían implementarse para mejorar la formación y capacitación de los peritos informáticos forenses en la ciudad?	Competencias Técnicas	Capacitación recibida
Ronda 3	5. ¿Qué papel deberían desempeñar las instituciones académicas, las organizaciones profesionales y el Consejo de la Judicatura en la mejora de la capacitación de metodologías forenses digitales?	Competencias Técnicas	Capacitación recibida

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1. Análisis

Se realizó un análisis exhaustivo de los resultados obtenidos a partir de una ronda de preguntas dirigida tanto a expertos en peritaje informático forense como a juristas bajo el método Delphi. El objetivo fue explorar en profundidad los temas definidos en los objetivos de la investigación. Esto implicó examinar la comprensión del debido proceso en investigaciones digitales, así como los desafíos tecnológicos específicos y el posible impacto derivado de la falta de capacitación técnica especializada.

Caracterización de los expertos que participaron en la consulta.

La tabla proporciona una visión detallada de los expertos que participaron en la consulta en la ciudad de Quito. En ella, se destaca una distribución equilibrada entre dos áreas clave: ingeniería informática o de sistemas y derecho. La mayoría de los participantes son ingenieros informáticos o de sistemas, con una notable experiencia acumulada de entre 5 y 10 años en el campo.

Este grupo se destaca por su sólida base de conocimientos técnicos en investigaciones digitales, respaldada por una experiencia considerable en ingeniería informática.

Además, la inclusión de expertos en derecho con experiencia relevante en la disciplina enriquece aún más el proceso de consulta, aportando una comprensión legal profunda que complementa las habilidades técnicas.

Esta combinación diversa y equilibrada de perfiles garantiza una perspectiva integral y efectiva en la identificación y resolución de desafíos en el ámbito de las investigaciones digitales.

Tabla 3. Caracterización de los expertos que participaron en la consulta.

Ciudad	Área o profesión	Experiencia	Especialización
Quito	Ingeniería	10 años	Ingeniera Informatica o de Sistemas
Quito	Ingeniería	5 años	Ingeniera Informatica o de Sistemas
Quito	Ingeniería	7 años	Ingeniera Informatica o de Sistemas
Quito	Ingeniería	6 años	Ingeniera Informatica o de Sistemas
Quito	Ingeniería	8 años	Ingeniera Informatica o de Sistemas
Quito	Ingeniería	5 años	Ingeniera Informatica o de Sistemas
Quito	Derecho	5 años	Derecho
Quito	Derecho	7 años	Derecho
Quito	Derecho	6 años	Derecho
Quito	Derecho	8 años	Derecho

3.1.1. Análisis de la primera ronda de preguntas: identificar factores de la falta de comprensión del proceso en investigaciones digitales.

Pregunta 1:

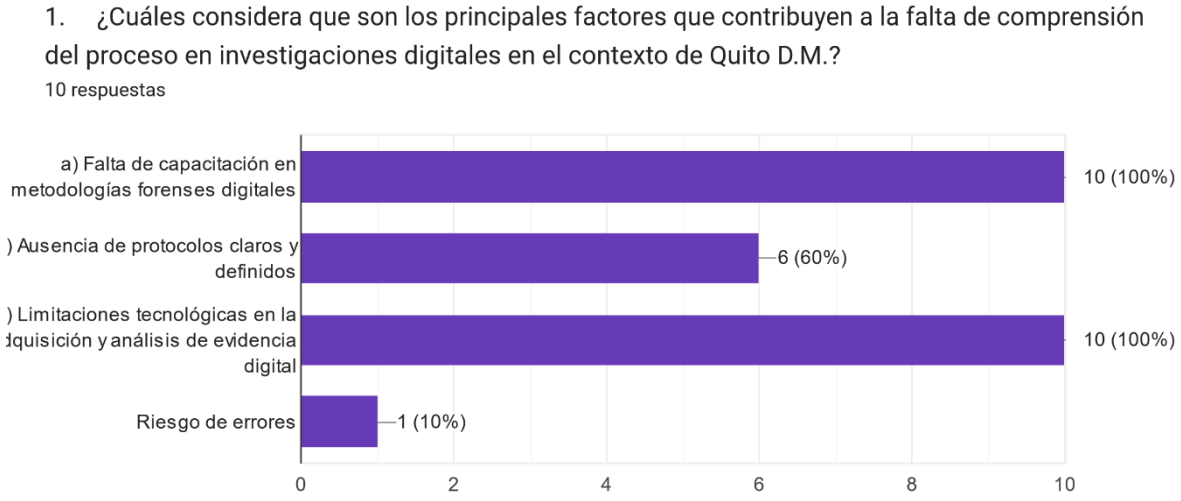
¿Cuáles considera que son los principales factores que contribuyen a la falta de comprensión del proceso en investigaciones digitales en el contexto de Quito D.M.?

En esta pregunta se exploraron los principales factores que se consideran responsables de la falta de comprensión del proceso en investigaciones digitales en el contexto de Quito D.M. Las opciones proporcionadas permiten identificar las áreas clave de preocupación y establecer prioridades para abordar las deficiencias en el campo del peritaje informático forense.

El análisis refleja que la falta de capacitación en metodologías forenses digitales y las limitaciones tecnológicas en la adquisición y análisis de evidencia digital son identificadas como los factores más significativos, con un porcentaje del 100% de los encuestados seleccionando estas opciones. La ausencia de protocolos claros y definidos también es reconocida como un problema importante, con el 60% de los encuestados identificándola como un factor contribuyente. Además, se

señala el riesgo de errores como otro factor relevante, aunque solo el 10% de los encuestados lo considera como una preocupación.

Figura 12. Análisis pregunta 1 Primera Ronda



Pregunta 2:

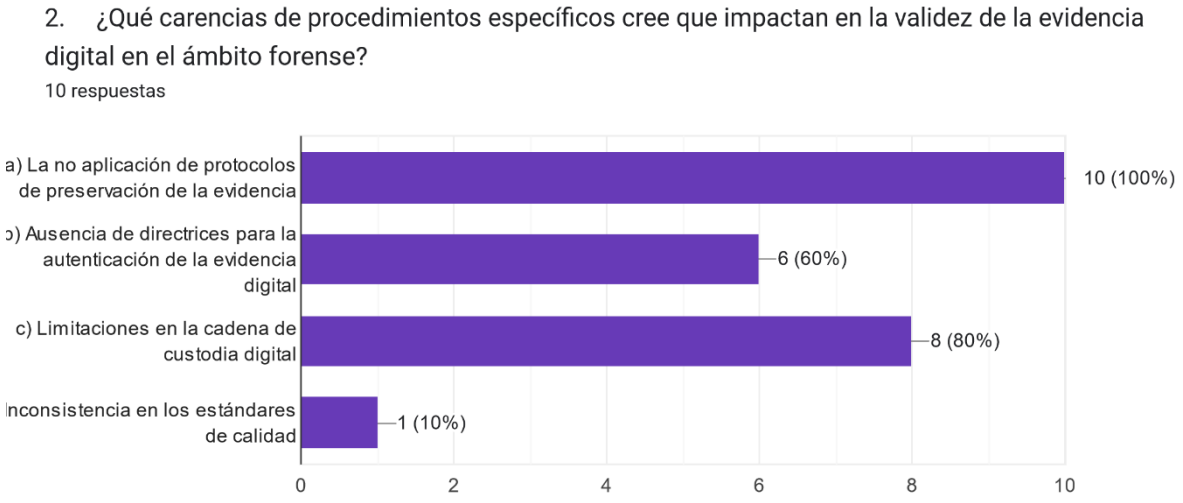
¿Qué carencias de procedimientos específicos cree que impactan en la validez de la evidencia digital en el ámbito forense?

Se observa que en el ámbito forense digital, las carencias de procedimientos específicos pueden tener un impacto significativo en la validez de la evidencia presentada. En esta pregunta, se buscó identificar cuáles de estas deficiencias son consideradas más relevantes por los participantes.

Los resultados muestran que la falta de aplicación de protocolos de preservación de la evidencia fue señalada como el factor más crítico, con el 100% de los encuestados seleccionándolo. La ausencia de directrices para la autenticación de la evidencia digital y las limitaciones en la cadena de custodia digital también fueron identificadas como preocupaciones importantes, con el 60% y el 80% de los participantes respectivamente. Además, se destacó la

inconsistencia en los estándares de calidad como otro aspecto relevante, aunque solo el 10% de los encuestados lo consideró como una preocupación significativa.

Figura 13. Análisis pregunta 2 Primera Ronda



Pregunta 3:

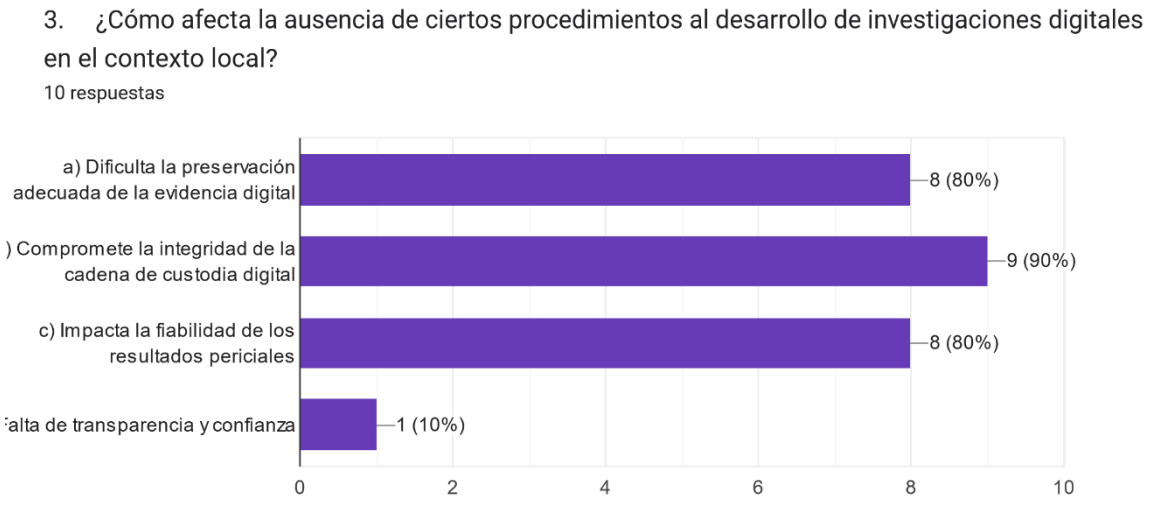
¿Cómo afecta la ausencia de ciertos procedimientos al desarrollo de investigaciones digitales en el contexto local?

Al examinar los porcentajes de las respuestas, destaca que la mayoría de los participantes identificaron la carencia de protocolos claros para la preservación de la evidencia digital como un factor significativo, con un 80% de acuerdo en que esto dificulta adecuadamente dicha preservación. Asimismo, un alto porcentaje del 90% señaló que la falta de directrices para autenticar la evidencia compromete la integridad de la cadena de custodia digital, lo que indica una preocupación destacada en este aspecto.

Por otro lado, El 80% reconoció que la ausencia de ciertos procedimientos impacta en la fiabilidad de los resultados periciales, lo que sugiere que algunos participantes pueden tener percepciones divergentes sobre este tema. Finalmente, se mencionó un factor adicional, la falta de transparencia y confianza, aunque solo

un 10% de los participantes lo consideró relevante, indicando que este aspecto podría ser menos prioritario en comparación con otros desafíos identificados.

Figura 14. Análisis pregunta 3 Primera Ronda



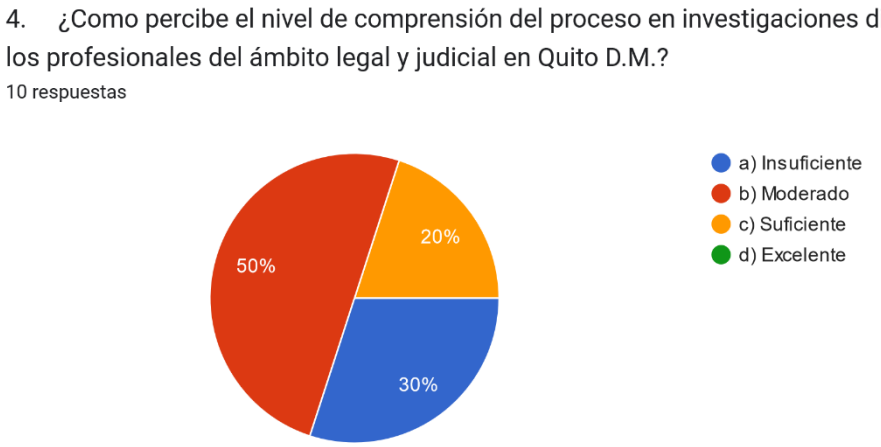
Pregunta 4:

¿Como percibe el nivel de comprensión del proceso en investigaciones digitales por parte de los profesionales del ámbito legal y judicial en Quito D.M.?

Al evaluar el nivel de comprensión del proceso en investigaciones digitales por parte de los profesionales del ámbito legal y judicial en Quito D.M., se observa que el 50% de los participantes considera que este nivel es moderado, seguido por un 30% que lo percibe como insuficiente. Además, un 20% lo califica como suficiente, mientras que ningún participante lo evaluó como excelente.

Esta distribución de respuestas sugiere una percepción variada sobre el nivel de comprensión del proceso en investigaciones digitales entre los profesionales del ámbito legal y judicial en la ciudad de Quito.

Figura 15. Análisis pregunta 4 Primera Ronda



Pregunta 5:

¿Qué recomendaciones sugeriría para mejorar la comprensión del proceso en investigaciones digitales en la ciudad?

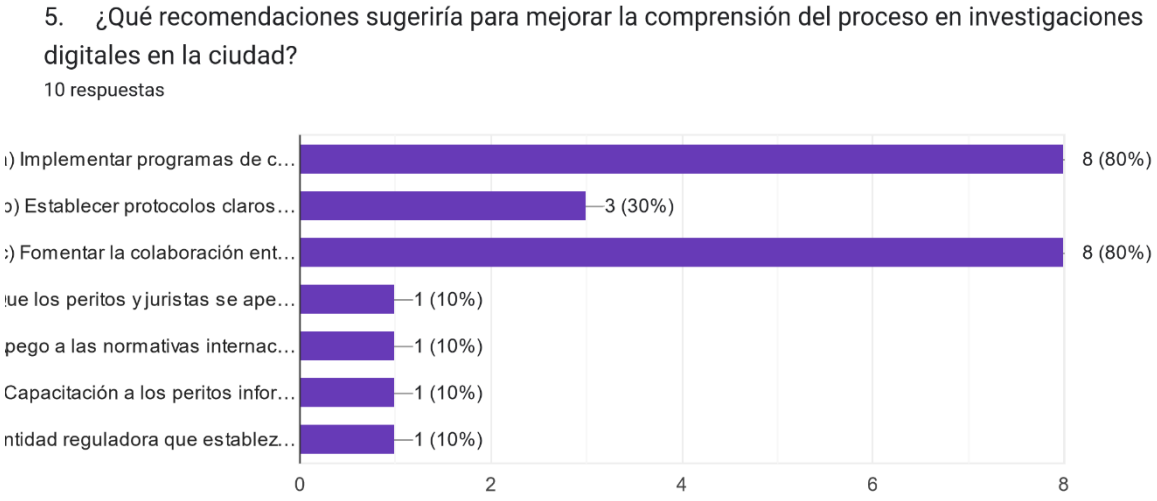
Al analizar las recomendaciones sugeridas para mejorar la comprensión del proceso en investigaciones digitales en la ciudad, se observa que dos recomendaciones tienen un alto porcentaje de acuerdo entre los participantes, con un 80% de acuerdo en cada una. Estas recomendaciones son la implementación de programas de capacitación en metodologías forenses digitales y el fomento de la colaboración entre peritos informáticos y profesionales del ámbito legal.

Por otro lado, las recomendaciones relacionadas con el establecimiento de protocolos claros y actualizados para la recolección y preservación de evidencia digital tuvieron un porcentaje menor de acuerdo, con solo el 30%.

Además, se mencionaron algunas recomendaciones adicionales en la opción "d", como el apego a guías internacionales para el peritaje informático, la capacitación a los peritos informáticos forenses y la creación de una entidad reguladora que establezca un ranking de peritos basados en sus logros y experiencias en casos previos, cada una con un 10% de acuerdo. Estas sugerencias adicionales reflejan una variedad de enfoques y preocupaciones entre

los participantes sobre cómo mejorar la comprensión del proceso en investigaciones digitales en la ciudad de Quito.

Figura 16. Análisis pregunta 5 Primera Ronda



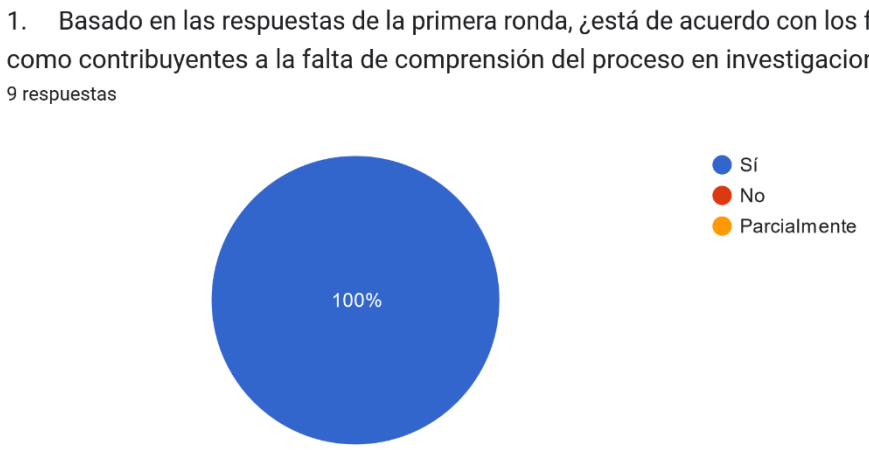
3.1.2. Análisis de la segunda ronda de preguntas: determinar los desafíos tecnológicos de peritos informáticos.

Pregunta 1:

Basado en las respuestas de la primera ronda, ¿está de acuerdo con los factores identificados como contribuyentes a la falta de comprensión del proceso en investigaciones digitales?

Según las respuestas de la primera ronda, se observa un acuerdo unánime entre los participantes con respecto a los factores identificados como contribuyentes a la falta de comprensión del proceso en investigaciones digitales. Todos los participantes (100%) están de acuerdo con los factores identificados. Esto sugiere una convergencia en la percepción de los desafíos y dificultades asociados con la comprensión del proceso en investigaciones digitales en el contexto estudiado.

Figura 17. Análisis pregunta 1 Segunda Ronda



Pregunta 2:

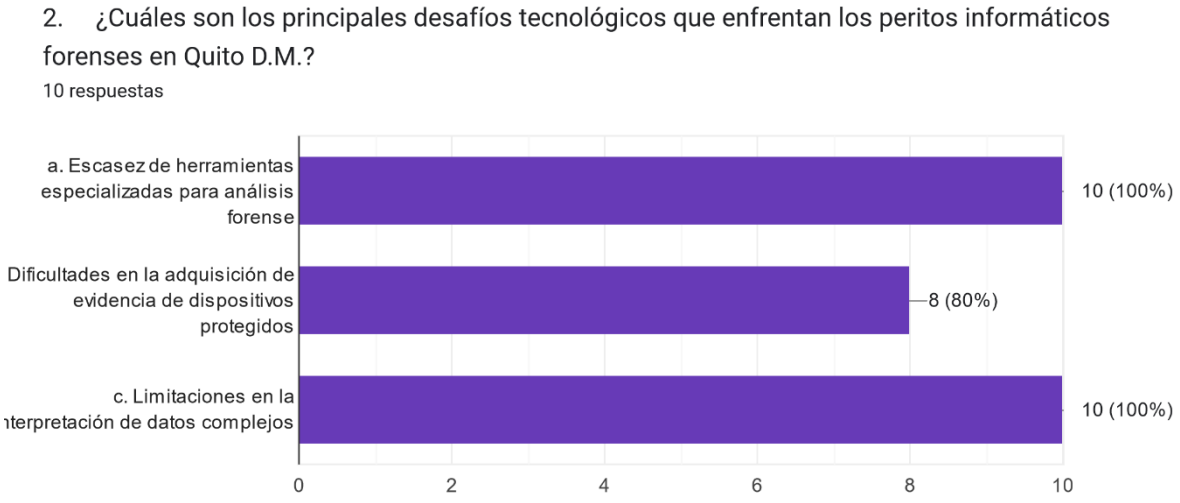
¿Cuáles son los principales desafíos tecnológicos que enfrentan los peritos informáticos forenses en Quito D.M.?

Los resultados revelan que los peritos informáticos forenses en Quito D.M. enfrentan varios desafíos tecnológicos significativos. En primer lugar, el 100% de los participantes señaló la escasez de herramientas especializadas para el análisis forense como uno de los principales obstáculos. Esta carencia podría dificultar la recopilación, el procesamiento y la interpretación de la evidencia digital, lo que a su vez afecta la eficacia y la precisión de las investigaciones.

Además, el 100% de los encuestados identificó las limitaciones en la interpretación de datos complejos como otro desafío tecnológico importante. La naturaleza cada vez más sofisticada de la tecnología digital puede llevar a la aparición de datos altamente complejos, cuya interpretación adecuada puede resultar complicada incluso para expertos en el campo. Esta dificultad puede ralentizar el proceso de análisis forense y afectar la calidad de los resultados periciales.

Por último, el 80% de los participantes mencionó las dificultades en la adquisición de evidencia de dispositivos protegidos como un desafío relevante. La protección y el cifrado de datos en dispositivos digitales pueden dificultar la extracción de información relevante para la investigación forense, lo que puede obstaculizar el avance de la misma y afectar la capacidad de los peritos para obtener una imagen completa de los hechos en cuestión.

Figura 18. Análisis pregunta 2 Segunda Ronda



Pregunta 3:

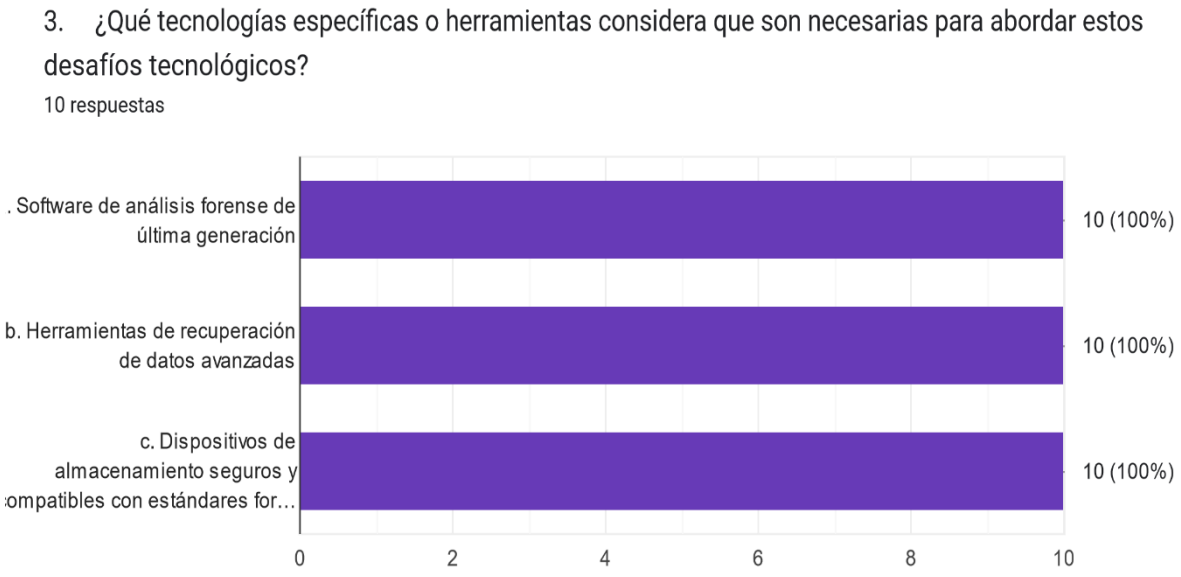
¿Qué tecnologías específicas o herramientas considera que son necesarias para abordar estos desafíos tecnológicos?

Basándonos en los resultados todos los participantes indicaron que consideran necesarias varias tecnologías específicas o herramientas para abordar los desafíos tecnológicos identificados. En primer lugar, el 100% de los encuestados mencionó el software de análisis forense de última generación como una herramienta esencial. Este tipo de software proporciona funcionalidades avanzadas para la recopilación, el procesamiento y la interpretación de evidencia digital, lo que puede mejorar significativamente la eficacia y la precisión de las investigaciones.

Además, el 100% de los participantes señaló que las herramientas de recuperación de datos avanzadas son necesarias para enfrentar los desafíos tecnológicos. Estas herramientas permiten recuperar información de dispositivos dañados o protegidos, lo que puede ser crucial para obtener evidencia relevante en casos forenses digitales.

Finalmente, el 100% de los encuestados consideró que los dispositivos de almacenamiento seguros y compatibles con estándares forenses son indispensables. Estos dispositivos garantizan la integridad y la preservación de la evidencia digital durante el proceso de recopilación y análisis, lo que contribuye a la validez y la fiabilidad de los resultados periciales.

Figura 19. Análisis pregunta 3 Segunda Ronda



Pregunta 4:

¿Cómo crees que la falta de acceso o capacitación en tecnologías específicas afecta el trabajo de los peritos informáticos en la ciudad?

Realizado el análisis de la pregunta 4 se evidencia que la falta de acceso a herramientas especializadas o la ausencia de capacitación en su uso puede limitar la capacidad de los peritos informáticos para llevar a cabo investigaciones digitales efectivas. Esto se traduce en dificultades para realizar un análisis exhaustivo de la evidencia digital, lo que podría resultar en la omisión de información crucial para resolver casos de delitos cibernéticos. Como consecuencia, la efectividad de las investigaciones se ve comprometida, ya que la carencia de recursos y habilidades necesarios podría obstaculizar el proceso de recolección y análisis de evidencia.

Además, la falta de acceso o capacitación en tecnologías específicas puede generar problemas en la identificación y preservación adecuada de la evidencia digital. Los peritos informáticos podrían enfrentar dificultades para recolectar y proteger la información digital relevante, lo que pone en riesgo su integridad y validez como prueba en un caso legal.

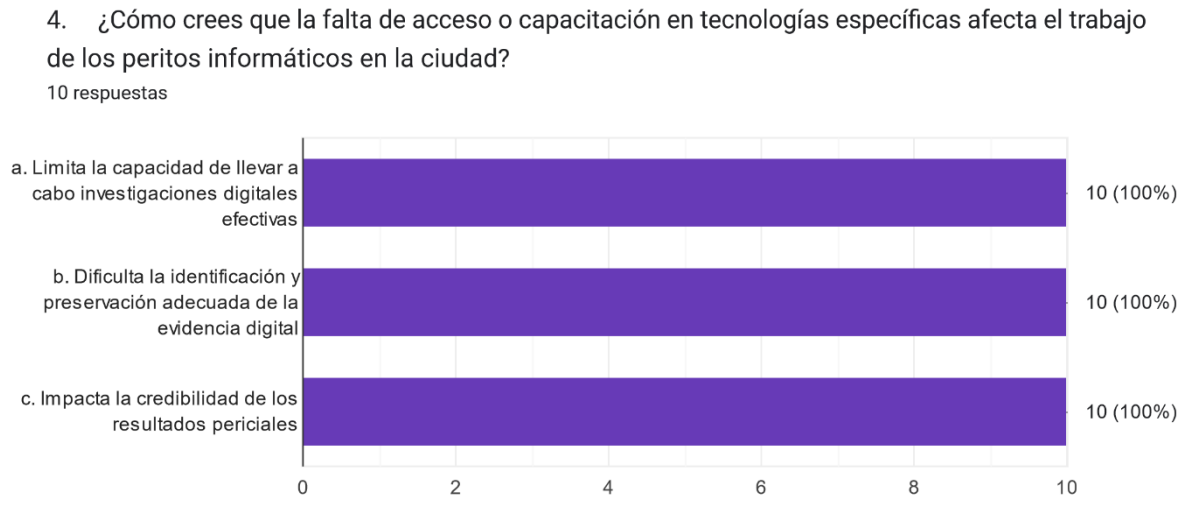
La identificación precisa y la preservación adecuada de la evidencia son fundamentales para garantizar la solidez de un caso, y la falta de recursos y conocimientos en esta área podría comprometer seriamente la capacidad de los peritos para cumplir con estas tareas de manera efectiva.

Por último, los errores en el análisis de la evidencia digital debido a la falta de acceso o capacitación en tecnologías específicas pueden tener un impacto significativo en la credibilidad de los resultados periciales. La confianza en la precisión y fiabilidad del trabajo de los peritos informáticos se ve debilitada cuando se cometen errores debido a la falta de recursos o conocimientos adecuados.

Dado que los resultados periciales desempeñan un papel crucial en la toma de decisiones judiciales, cualquier duda sobre su credibilidad puede afectar

negativamente al proceso legal en general, generando dudas sobre la justicia y la imparcialidad del sistema.

Figura 20. Análisis pregunta 4 Segunda Ronda



Pregunta 5:

¿Qué recomendaciones propondrías para superar los desafíos tecnológicos identificados en el peritaje informático forense en Quito D.M.?

Al considerar los porcentajes de las respuestas proporcionadas en la encuesta, se evidencia un alto acuerdo entre los participantes respecto a las recomendaciones propuestas para superar los desafíos tecnológicos en el peritaje informático forense en Quito D.M. Todas las opciones de respuesta obtuvieron un porcentaje del 100%, lo que sugiere un consenso generalizado entre los encuestados sobre la importancia de estas recomendaciones.

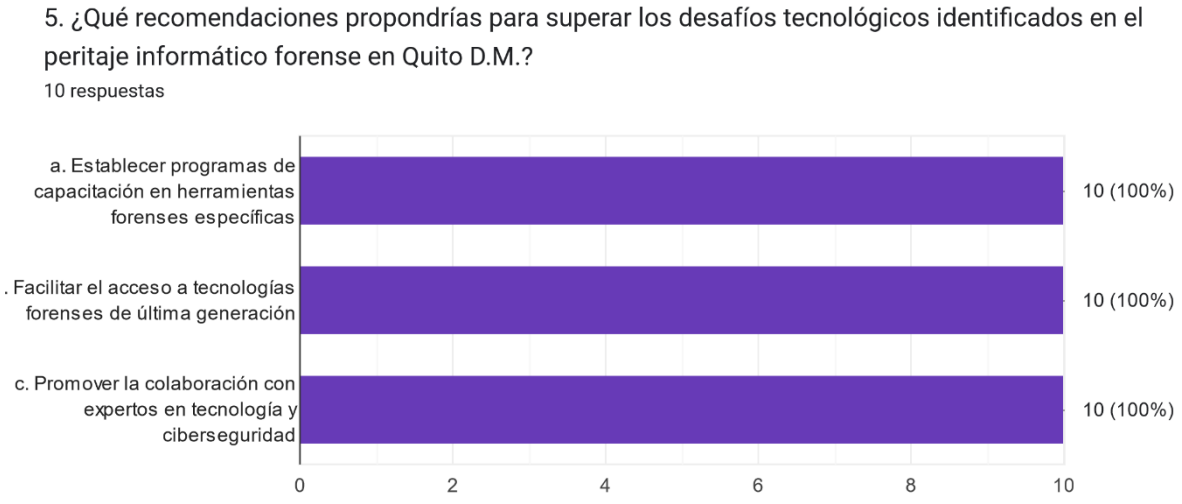
En primer lugar, el 100% de los participantes respaldó la idea de establecer programas de capacitación en herramientas forenses específicas. Esto indica un reconocimiento unánime de la necesidad de proporcionar a los peritos informáticos la formación necesaria para dominar las herramientas tecnológicas requeridas en su trabajo.

Asimismo, el 100% de los encuestados estuvo de acuerdo en la importancia de facilitar el acceso a tecnologías forenses de última generación. Esta unanimidad refleja una comprensión compartida de que el acceso a herramientas tecnológicas avanzadas es fundamental para realizar análisis eficaces y precisos de la evidencia digital.

Finalmente, el 100% de los participantes también respaldó la idea de promover la colaboración con expertos en tecnología y ciberseguridad. Este resultado sugiere un reconocimiento generalizado de la importancia de la colaboración interdisciplinaria para abordar los desafíos tecnológicos en el peritaje informático forense.

En resumen, los altos porcentajes de acuerdo en todas las recomendaciones indican un consenso sólido entre los encuestados sobre las acciones necesarias para superar los desafíos tecnológicos en el ámbito del peritaje informático forense en Quito D.M.

Figura 21. Análisis pregunta 5 Segunda Ronda

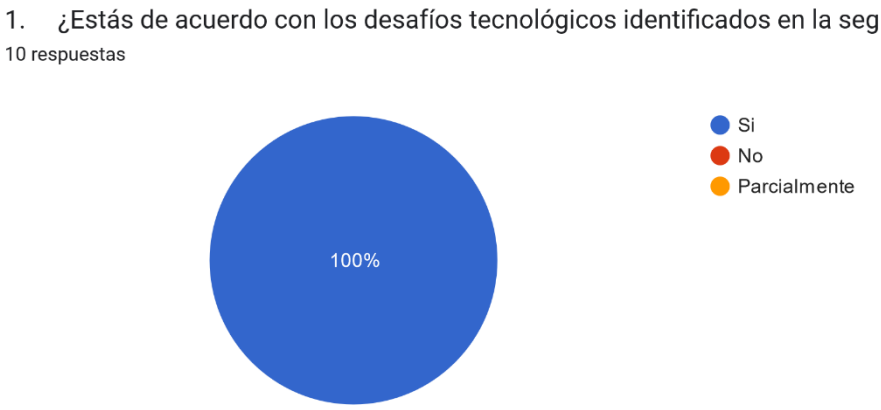


3.1.3. Análisis de la tercera ronda de preguntas: investigar la falta de capacitación en metodologías forenses digitales.

Pregunta 1:

Basándonos en los resultados obtenidos en la segunda ronda de la encuesta, todos los participantes estuvieron de acuerdo con los desafíos tecnológicos identificados. El 100% de los encuestados expresó conformidad con los desafíos presentados, lo que indica un consenso completo entre los participantes respecto a la relevancia y validez de los desafíos tecnológicos identificados en el ámbito del peritaje informático forense en Quito D.M.

Figura 22. Análisis pregunta 1 Tercera Ronda



Pregunta 2:

¿Cómo crees que la falta de capacitación en metodologías forenses digitales impacta la fiabilidad de los resultados periciales en Quito D.M.?

El análisis de la pregunta dos refleja que la falta de capacitación en metodologías forenses digitales puede tener un impacto significativo en la fiabilidad de los resultados periciales en Quito D.M., según lo indicado por los participantes de la encuesta.

En primer lugar, el 100% de los encuestados señaló que esta carencia compromete la calidad del análisis forense. Esta percepción resalta la importancia de contar con conocimientos sólidos en metodologías específicas para garantizar la precisión y exhaustividad del análisis en el contexto forense.

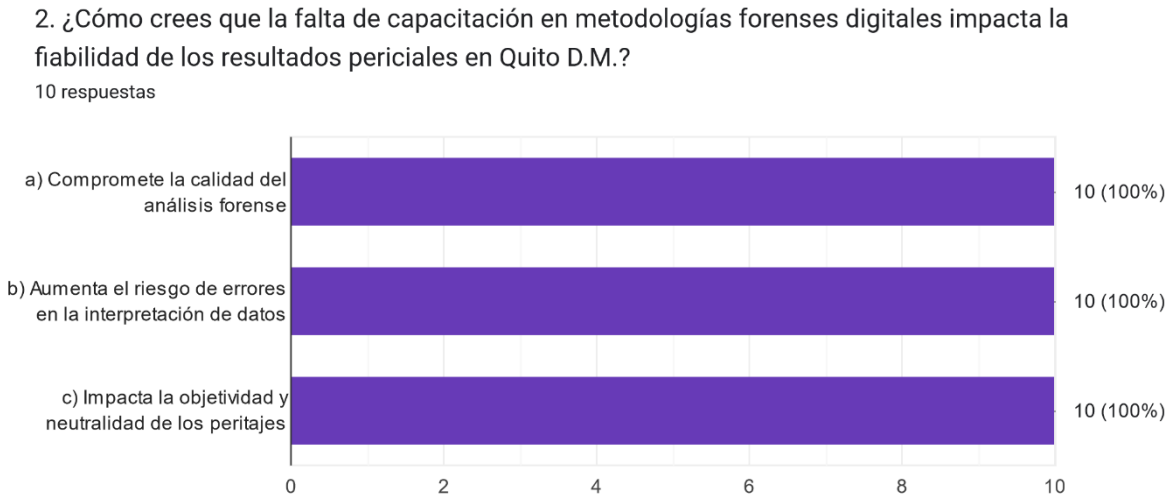
Además, el 100% de los participantes también expresó que la falta de capacitación aumenta el riesgo de errores en la interpretación de datos. Esta observación destaca cómo la carencia de conocimientos adecuados puede llevar a interpretaciones incorrectas o sesgadas de la evidencia digital, lo que socava la fiabilidad de los resultados periciales.

Por último, todos los encuestados, también el 100%, coincidieron en que la falta de capacitación en metodologías forenses digitales impacta la objetividad y neutralidad de los peritajes. Esta percepción sugiere que la falta de conocimientos específicos puede influir en la imparcialidad de los peritos informáticos, comprometiendo así la credibilidad de sus conclusiones en el ámbito legal.

Estos resultados subrayan la relevancia fundamental de la capacitación en metodologías forenses digitales para asegurar la confiabilidad y solidez de los resultados periciales en Quito D.M. La carencia de este tipo de capacitación puede no solo debilitar la calidad del análisis realizado por los peritos, sino también incrementar el peligro de cometer errores en la interpretación de los datos digitales recolectados.

Además, la falta de entrenamiento adecuado podría comprometer la imparcialidad y neutralidad de los peritajes, lo que podría poner en entredicho la validez de los resultados presentados en los procedimientos legales. En este contexto, resulta imperativo implementar programas de formación especializados que doten a los peritos informáticos forenses con las habilidades y conocimientos necesarios para desempeñar su labor de manera efectiva y ética, garantizando así la integridad del proceso de investigación digital forense en la ciudad.

Figura 23. Análisis pregunta 2 Tercera Ronda



Pregunta 3:

¿Qué aspectos específicos de las metodologías forenses digitales considera que son necesarios mejorar en la capacitación de los peritos informáticos?

Al analizar los resultados de la pregunta tres, queda claro que hay una unanimidad entre los participantes con respecto a los aspectos específicos de las metodologías forenses digitales que necesitan mejorar en la capacitación de los peritos informáticos en Quito D.M.

En primer lugar, el 100% de los encuestados señaló que las técnicas de adquisición y preservación de evidencia digital son un área crucial que requiere atención. Esto sugiere que los peritos deben estar mejor equipados con habilidades para recolectar y salvaguardar adecuadamente la evidencia digital para garantizar su integridad y validez en los procedimientos legales.

Además, el 70% de los participantes también identificó el análisis de malware y vulnerabilidades de seguridad como un aspecto clave que necesita mejorarse en la capacitación de los peritos informáticos. Esto indica la importancia de que los

peritos adquieran habilidades avanzadas para detectar y analizar amenazas cibernéticas, lo que les permitirá identificar posibles brechas de seguridad y prevenir ataques digitales.

Por último, el 100% de los encuestados destacó la interpretación de resultados y la elaboración de informes periciales como otro aspecto fundamental que requiere atención en la capacitación de los peritos informáticos. Esto subraya la necesidad de que los peritos adquieran habilidades para analizar de manera efectiva la evidencia digital y comunicar sus hallazgos de manera clara y concisa en informes periciales que puedan ser comprendidos por los profesionales legales y judiciales.

Figura 24. Análisis pregunta 3 Tercera Ronda

Pregunta 4:

¿Qué acciones específicas podrían implementarse para mejorar la formación y capacitación de los peritos informáticos forenses en la ciudad?

Basándonos en los resultados de la pregunta cuatro, se desprende una clara preferencia entre los participantes en cuanto a las acciones específicas que podrían

implementarse para mejorar la formación y capacitación de los peritos informáticos forenses en la ciudad.

En primer lugar, el 100% de los encuestados sugirió desarrollar programas de formación especializados en metodologías forenses digitales. Esto indica la necesidad de establecer currículos educativos específicos que aborden los desafíos y las mejores prácticas en el campo del peritaje informático, garantizando así que los peritos estén debidamente preparados para enfrentar los desafíos tecnológicos y legales en sus funciones.

Además, el 100% de los participantes también señaló la importancia de promover la certificación y acreditación de peritos informáticos. Esta acción puede ayudar a establecer estándares de competencia y ética en la profesión, lo que a su vez puede mejorar la confianza en los resultados periciales y en el proceso judicial en general.

Por último, el 90% de los encuestados sugirió establecer convenios de colaboración con instituciones académicas y centros de investigación. Esto destaca la necesidad de crear asociaciones estratégicas entre el sector académico y el sector forense para fomentar la investigación conjunta, el intercambio de conocimientos y la capacitación continua de los peritos informáticos.

Estas colaboraciones entre instituciones académicas, centros de investigación y los profesionales del peritaje informático forense pueden tener un impacto significativo en el desarrollo y la evolución de la disciplina.

Al establecer vínculos estrechos con el ámbito académico, los peritos informáticos forenses pueden acceder a recursos adicionales, como laboratorios especializados y expertos en diversas áreas relacionadas, lo que enriquece su formación y les permite mantenerse al día con los avances tecnológicos y metodológicos.

Figura 25. Análisis pregunta 4 Tercera Ronda

Pregunta 5:

¿Qué papel deberían desempeñar las instituciones académicas, las organizaciones profesionales y el Consejo de la Judicatura en la mejora de la capacitación de metodologías forenses digitales?

En el análisis de la pregunta sobre el papel de las instituciones académicas, las organizaciones profesionales y el Consejo de la Judicatura en la mejora de la capacitación de metodologías forenses digitales, se observa un respaldo unánime por parte de los participantes hacia todas las opciones presentadas.

Estas opciones abordan aspectos clave para fortalecer la formación en el campo del peritaje informático forense, desde el desarrollo de programas académicos especializados hasta la promoción de la investigación y el desarrollo de nuevas metodologías.

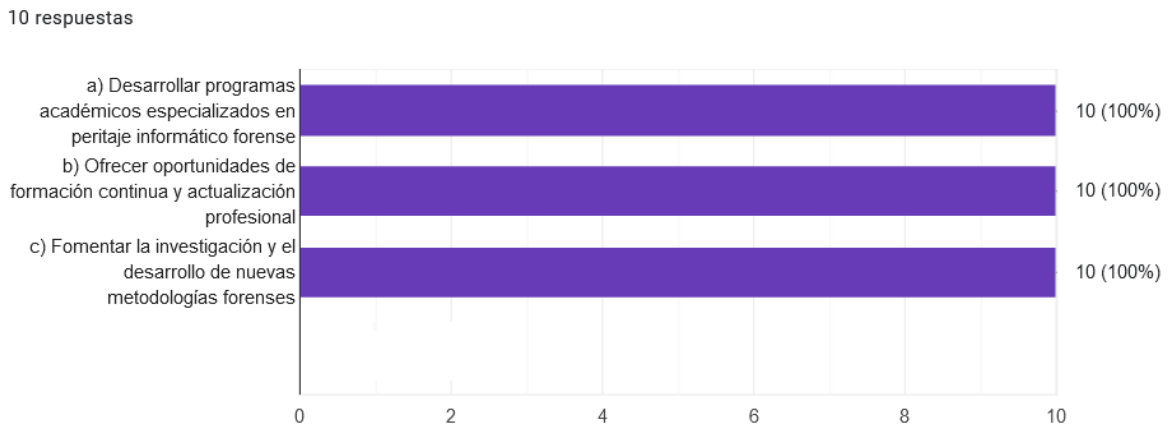
A continuación, se analizará en detalle cada una de estas opciones, considerando el respaldo obtenido y su relevancia para el fortalecimiento del peritaje informático forense en Quito D.M.

La opción a, que sugiere el desarrollo de programas académicos especializados en peritaje informático forense, recibió el respaldo del 100% de los participantes. Esto destaca la necesidad de establecer programas educativos específicos para formar expertos en este campo, lo que indica un consenso completo sobre la importancia de esta iniciativa para establecer una base sólida de conocimientos en el campo desde el nivel académico inicial.

La opción b, que enfatiza la importancia de ofrecer oportunidades de formación continua y actualización profesional, también recibió el respaldo del 100% de los participantes. Esto resalta la necesidad de programas que aborden temas específicos y emergentes en el campo, reconociendo que la evolución constante de la tecnología y las técnicas forenses requiere un compromiso continuo con el aprendizaje y la actualización profesional.

Por último, la opción c, que destaca la importancia de fomentar la investigación y el desarrollo de nuevas metodologías forenses, también obtuvo el respaldo del 100% de los participantes. Esto indica un reconocimiento generalizado de la relevancia de esta iniciativa, evidenciando el valor de la investigación en la mejora continua de las prácticas y técnicas forenses.

Figura 26. Análisis pregunta 5 Tercera Ronda



3.1.4. Análisis de resultados de las tres rondas de preguntas.

Tras analizar los resultados de las tres rondas de preguntas, se puede observar un consenso generalizado en varios aspectos clave relacionados con el peritaje informático forense en Quito D.M.

En la primera ronda, donde se exploraron las carencias de procedimientos específicos que impactan en la validez de la evidencia digital, se identificó una clara necesidad de establecer protocolos claros y actualizados para la recolección y preservación de evidencia digital, con un respaldo del 80%. Esta es una preocupación fundamental, ya que una preservación inadecuada puede comprometer la integridad de la evidencia y afectar la validez de los resultados periciales.

En cuanto a los desafíos tecnológicos enfrentados por los peritos informáticos forenses en la ciudad, la segunda ronda reveló que la escasez de herramientas especializadas para análisis forense y las limitaciones en la interpretación de datos complejos fueron los aspectos más destacados, con un respaldo del 100% en ambas opciones. Esto subraya la necesidad de inversiones en tecnologías y herramientas avanzadas, así como en el desarrollo de habilidades para abordar la complejidad creciente de la evidencia digital.

En la tercera ronda, que se centró en las implicaciones de la falta de capacitación en metodologías forenses digitales, todas las opciones presentadas obtuvieron un respaldo del 100%. Esto resalta la importancia crítica de la capacitación continua y especializada para garantizar la calidad y la fiabilidad de los resultados periciales en investigaciones digitales.

En resumen, los resultados de las tres rondas de preguntas destacan la necesidad de establecer protocolos claros, mejorar las capacidades tecnológicas y proporcionar una capacitación especializada para fortalecer el peritaje informático forense en Quito D.M. Estos hallazgos pueden servir como base para el desarrollo

de estrategias y políticas destinadas a mejorar la efectividad y la confiabilidad de las investigaciones digitales en la ciudad. A continuación la matriz de consenso:

Tabla 4. Matriz de consenso primera ronda de preguntas

Expertos	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5
Experto 1	a, b, c	a	a, b, c	Moderado	a, c
Experto 2	a, c	a	a, b, c	Suficiente	a, c
Experto 3	a, b, c	a, b, c	a, b, c	Moderado	a, b, c
Experto 4	a, c	a, b, c	a, c	Moderado	a, c
Experto 5	a, c	a, c	a, b, c	Suficiente	a, c
Experto 6	a, b, c	a, c	b	Insuficiente	b
Experto 7	a, c	a, b, c	a, b, c	Moderado	a, c
Experto 8	a, b, c	a, b, c	a, b, c	Insuficiente	b
Experto 9	a, b, c	a, b, c	a, b, c	Moderado	a, b, c
Experto 10	a, b, c	a, b, c	a, b, c	Insuficiente	a, c
Consenso	a, c	a	a, b, c	Moderado	a, c

Análisis matriz de consenso primera ronda

En cuanto a los principales factores que contribuyen a la falta de comprensión del proceso en investigaciones digitales en el contexto de Quito D.M., hay un consenso entre los expertos en que la falta de capacitación en metodologías forenses digitales, la ausencia de protocolos claros y definidos, y las limitaciones tecnológicas en la adquisición y análisis de evidencia digital son los aspectos más relevantes (Respuestas a, b y c).

Respecto a las carencias de procedimientos específicos que impactan en la validez de la evidencia digital en el ámbito forense, los expertos coinciden en que la falta de aplicación de protocolos de preservación de la evidencia es un aspecto crítico (Respuesta a).

La ausencia de ciertos procedimientos afecta principalmente la preservación adecuada de la evidencia digital, la integridad de la cadena de custodia digital y la fiabilidad de los resultados periciales, aspectos en los que también hay consenso entre los expertos (Respuestas a, b y c).

En cuanto al nivel de comprensión del proceso en investigaciones digitales por parte de los profesionales del ámbito legal y judicial en Quito D.M., la mayoría de los expertos lo perciben como moderado (Respuesta Moderado).

Finalmente, las recomendaciones sugeridas para mejorar la comprensión del proceso en investigaciones digitales en la ciudad incluyen implementar programas de capacitación en metodologías forenses digitales, fomentar la colaboración entre peritos informáticos y profesionales del ámbito legal, y que los peritos y juristas se apeguen a guías internacionales para el peritaje informático (Respuestas a, c).

Tabla 5. Matriz de consenso segunda ronda de preguntas

Experto	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5
Experto 1	Sí	a, c	a, b, c	a	a, b, c
Experto 2		a, b, c	a, b, c	a	a, b, c
Experto 3	Sí	a, b, c	a, b, c	a	a, b, c
Experto 4	Sí	a, b, c	a, b, c	a	a, b, c
Experto 5		a, c	a, b, c	a	a, b, c
Experto 6	Sí	a, b, c	a, b, c	a	a, b, c
Experto 7	Sí	a, b, c	a, b, c	a	a, b, c
Experto 8	Sí	a, b, c	a, b, c	a	a, b, c
Experto 9	Sí	a, b, c	a, b, c	a	a, b, c
Experto 10	Sí	a, b, c	a, b, c	a	a, b, c
Consenso	Sí	a, b, c	a, b, c	a	a, b, c

Análisis matriz de consenso segunda ronda

En relación con los factores que contribuyen a la falta de comprensión del proceso en investigaciones digitales, se observa una sólida convergencia de opiniones entre la mayoría de los expertos participantes (Expertos 1, 3, 4, 6, 7, 8, 9 y 10). Estos expertos expresaron su acuerdo con los factores identificados. No obstante, algunos expertos (Expertos 2 y 5) no proporcionaron una respuesta definida, lo que sugiere cierta disparidad en las percepciones.

En cuanto a los principales desafíos tecnológicos enfrentados por los peritos informáticos forenses en Quito D.M., se evidencia un consenso generalizado entre todos los participantes (Expertos 1-10). Estos desafíos incluyen la escasez de

herramientas especializadas, las dificultades en la adquisición de evidencia de dispositivos protegidos y las limitaciones en la interpretación de datos complejos.

Respecto a las tecnologías específicas o herramientas necesarias para abordar estos desafíos tecnológicos, se destaca un consenso unánime entre todos los expertos participantes (Expertos 1-10). Existe acuerdo en la importancia de contar con software de análisis forense de última generación, herramientas de recuperación de datos avanzadas y dispositivos de almacenamiento seguros y compatibles con estándares forenses.

Finalmente, al evaluar el impacto de la falta de acceso o capacitación en tecnologías específicas en el trabajo de los peritos informáticos, se observa nuevamente un consenso generalizado entre todos los expertos (Expertos 1-10). Todos coinciden en que esta carencia limita la capacidad de llevar a cabo investigaciones digitales efectivas, dificulta la identificación y preservación adecuada de la evidencia digital, y afecta la credibilidad de los resultados periciales.

Tabla 6. Matriz de consenso tercera ronda de preguntas

Experto	**Pregunta 1**	**Pregunta 2**	**Pregunta 3**	**Pregunta 4**	**Pregunta 5**
Experto 1	Sí	a, b, c	a, b, c	a, b, c	a, b, c
Experto 2	Sí	a, b, c	a, b, c	a, b, c	a, b, c
Experto 3	Sí	a, b, c	a, b, c	a, b, c	a, b, c
Experto 4	Sí	a, b, c	a, c	a, b	a, b, c
Experto 5	Sí	a, b, c	a, b, c	a, b, c	a, b, c
Experto 6	Sí	a, b, c	a, c	a, b, c	a, b, c
Experto 7	Sí	a, b, c	a, b, c	a, b, c	a, b, c
Experto 8	Sí	a, b, c	a, b, c	a, b, c	a, b, c
Experto 9	Sí	a, b, c	a, b, c	a, b, c	a, b, c
Experto10	Sí	a, b, c	a, c	a, b, c	a, b, c
Consenso	Sí	a, b, c	a, b, c	a, b, c	a, b, c

Análisis matriz de consenso tercera ronda

En cuanto a los desafíos tecnológicos identificados en la segunda ronda, todos los expertos están de acuerdo en que son válidos y relevantes para el contexto de Quito D.M.

Respecto al impacto de la falta de capacitación en metodologías forenses digitales en la fiabilidad de los resultados periciales, todos los expertos coinciden en que compromete la calidad del análisis forense, aumenta el riesgo de errores en la interpretación de datos y afecta la objetividad y neutralidad de los peritajes.

Sobre los aspectos específicos de las metodologías forenses digitales que deben mejorarse en la capacitación de los peritos informáticos, la mayoría de los expertos señalan la necesidad de mejorar en técnicas de adquisición y preservación de evidencia digital, análisis de malware y vulnerabilidades de seguridad, así como la interpretación de resultados y elaboración de informes periciales.

En cuanto a las acciones específicas para mejorar la formación y capacitación de los peritos informáticos forenses en la ciudad, todos los expertos están de acuerdo en desarrollar programas de formación especializados en metodologías forenses digitales, promover la certificación y acreditación de peritos informáticos, y establecer convenios de colaboración con instituciones académicas y centros de investigación.

En relación con el papel que deberían desempeñar las instituciones académicas, las organizaciones profesionales y el Consejo de la Judicatura en la mejora de la capacitación de metodologías forenses digitales, todos los expertos coinciden en la importancia de desarrollar programas académicos especializados en peritaje informático forense, ofrecer oportunidades de formación continua y actualización profesional, y fomentar la investigación y el desarrollo de nuevas metodologías forenses.

Este análisis refleja un fuerte consenso entre los expertos en cuanto a la necesidad de abordar los desafíos tecnológicos y mejorar la capacitación en metodologías forenses digitales en el ámbito del peritaje informático en Quito D.M.

3.2. Análisis comparativo, evolución, tendencias y perspectivas.

En este análisis comparativo, se examinan las prácticas locales de peritaje informático forense en Quito D.M. en contraste con las tendencias internacionales en el campo. A través de la evaluación de convenciones internacionales relevantes, como el Convenio de Budapest sobre Ciberdelincuencia, se busca determinar su aplicabilidad y relevancia para el contexto local.

Este enfoque se apoya en los hallazgos obtenidos por el panel de expertos, lo que permite identificar áreas de mejora y establecer un marco de referencia internacional para el desarrollo futuro del peritaje informático forense en la ciudad.

Además, se analizan las mejores prácticas adoptadas por organizaciones internacionales como Interpol y otras agencias especializadas en investigación criminal y ciberseguridad. Este análisis comparativo tiene como objetivo integrar lecciones aprendidas a nivel internacional en el contexto local, enriqueciendo así las prácticas de peritaje informático forense en Quito D.M. y mejorando la capacidad de respuesta ante delitos cibernéticos.

3.2.1. Análisis comparativo.

En el análisis comparativo, se examinarán detalladamente las prácticas locales de peritaje informático forense en Quito D.M. en comparación con las tendencias internacionales en este campo. Se evaluarán los protocolos, procedimientos y estándares utilizados localmente en la adquisición, preservación, análisis y presentación de evidencia digital, contrastándolos con las mejores prácticas internacionales y los estándares establecidos por organizaciones relevantes, como la Interpol y las directrices del Convenio de Budapest sobre Ciberdelincuencia.

Este análisis permitirá identificar similitudes, diferencias, fortalezas y áreas de mejora en las prácticas locales, así como establecer un marco de referencia para el alineamiento con estándares internacionales reconocidos.

Comparativa de las prácticas locales del peritaje informático y el Convenio de Budapest.

El análisis comparativo entre las prácticas locales de peritaje informático forense en Quito D.M. y las disposiciones del Convenio sobre la Ciberdelincuencia, comúnmente conocido como el Convenio de Budapest, revela importantes beneficios y oportunidades para mejorar las capacidades y la eficacia de los procedimientos forenses digitales en la ciudad.

En primer lugar, el Convenio de Budapest proporciona un marco integral y coherente para combatir el ciberdelito y abordar la evidencia electrónica, estableciendo normas y directrices para la criminalización de diversas conductas, herramientas de derecho procesal y mecanismos de cooperación internacional. Esta normativa internacional ofrece una guía valiosa para cualquier país que desee desarrollar una legislación nacional integral sobre ciberdelitos y establece un marco para la cooperación entre Estados Parte en el tratado.

Además, el Convenio prevé la adopción de herramientas de derecho procesal que facilitan la investigación de ciberdelitos y la obtención de evidencia electrónica, lo que podría contribuir significativamente a mejorar los procedimientos forenses digitales en Quito D.M. La cooperación internacional ágil y eficiente contemplada en el tratado también podría fortalecer la capacidad de las autoridades locales para investigar y perseguir delitos cibernéticos transfronterizos.

Según (Convenio et al., 2023), al 4 de diciembre del 2023, un total de 89 Estados formaban parte del Convenio, incluyendo países europeos, así como Albania, Alemania, Antigua y Barbuda, Arabia Saudita, Armenia, Australia, Austria, Azerbaiyán, Bahrein, Belarús, Bélgica, Bosnia y Herzegovina, Brunei Darussalam, Bulgaria, Canadá, Chile, China, Colombia, Costa Rica, Croacia, Cuba, Dinamarca,

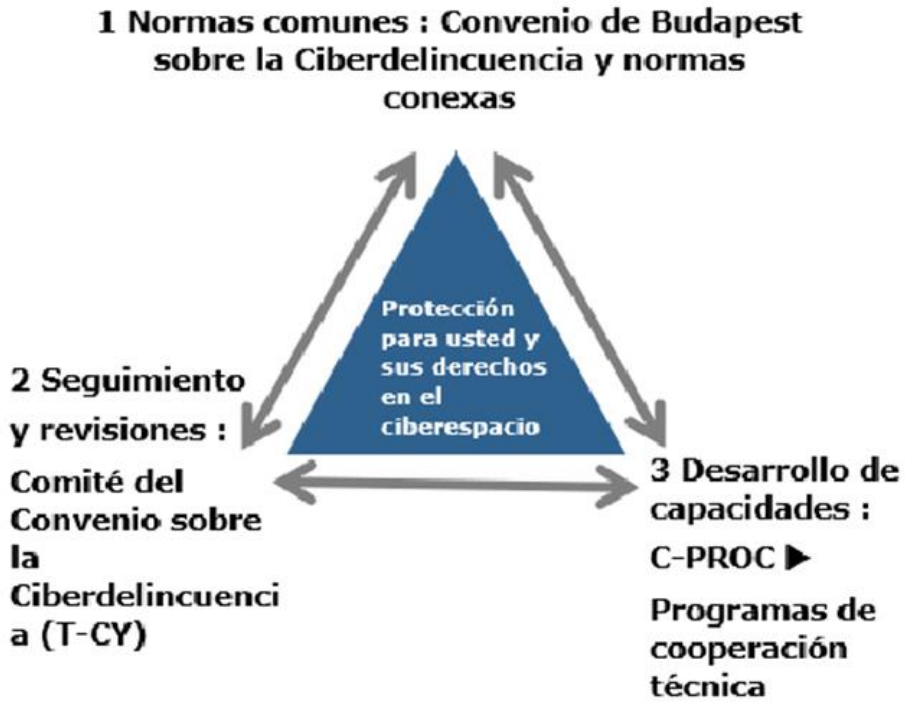
El Salvador, Emiratos Árabes Unidos, Eslovaquia, Eslovenia, España, Estados Unidos de América, Estonia, Federación de Rusia, Filipinas, Finlandia, Francia, Georgia, Grecia, Guatemala, Honduras, Hungría, India, Indonesia, Irlanda, Islandia, Israel, Italia, Japón, Jordania, Kazajstán, Kirguistán, Letonia, Liechtenstein, Lituania, Luxemburgo, Macedonia del Norte, Malasia, Marruecos, México, Mónaco, Montenegro, Nicaragua, Noruega, Nueva Zelandia, Omán, Panamá, Paraguay, Perú, Polonia, Portugal, Qatar, Reino de los Países Bajos, Reino Unido, República Checa, República de Corea, República de Moldova, República Dominicana, República Popular Democrática de Corea, Rumania, Rwanda, Serbia, Singapur, Sudáfrica, Suecia, Suiza, Tayikistán, Trinidad y Tabago, Túnez, Türkiye, Ucrania, Uzbekistán y Viet Nam.

Estos 89 Estados están involucrados como miembros activos (Partes) u observadores (signatarios o invitados) en el Comité del Convenio sobre la Ciberdelincuencia (T-CY). El T-CY, entre sus funciones, se encarga de evaluar la aplicación del Convenio por parte de los Estados Parte, emite Notas de Orientación y prepara instrumentos jurídicos adicionales.

Por otra parte, los programas de Creación de Capacidad, gestionados por la Oficina especializada del Programa sobre Ciberdelincuencia del Consejo de Europa (C-PROC) en Rumania, proporcionan asistencia a países de todo el mundo para desarrollar las habilidades necesarias para implementar el Convenio de Budapest o para adoptar las recomendaciones del Comité del Convenio sobre la Ciberdelincuencia (T-CY).

Sin embargo, es importante contrastar estas disposiciones internacionales con los hallazgos y recomendaciones obtenidos en el consenso de expertos locales. Aunque el Convenio de Budapest ofrece un marco valioso, su aplicabilidad y relevancia para el contexto específico de Quito D.M. deben ser evaluadas en función de las necesidades y desafíos locales identificados por los expertos en peritaje informático forense en la ciudad.

Figura 27. Convenio de Budapest sobre la delincuencia y normas conexas



La adhesión al Convenio sobre la Ciberdelincuencia conlleva una serie de beneficios para los Estados Parte, incluida una mayor protección legal contra la ciberdelincuencia, una cooperación internacional más efectiva y la posibilidad de participar en el Comité del Convenio sobre la Ciberdelincuencia para intercambiar información y experiencias.

Además, el acceso a programas de desarrollo de capacidades proporcionados por la Oficina especializada del Programa sobre Ciberdelincuencia del Consejo de Europa podría mejorar significativamente las habilidades y recursos disponibles para los peritos informáticos en Quito D.M.

Tabla 7. Comparativa: Situación Actual vs. Convenio de Budapest.

Aspecto	Situación Actual en Ecuador	Disposiciones del Convenio de Budapest	Beneficios Potenciales
Criminalización de conductas cibernéticas	Ecuador cuenta con algunas leyes que abordan delitos informáticos, pero la legislación puede ser fragmentada o insuficiente	El Convenio establece una amplia gama de delitos cibernéticos y proporciona directrices para la criminalización de estas conductas	Una legislación más completa y coherente para abordar una variedad de delitos cibernéticos
Herramientas de derecho procesal	Los procedimientos legales y herramientas para investigar ciberdelitos pueden ser limitados o ineficaces	El Convenio prevé herramientas legales para facilitar la investigación y obtención de pruebas electrónicas	Procedimientos legales más efectivos para investigar delitos cibernéticos y obtener evidencia digital
Cooperación internacional	Ecuador puede enfrentar desafíos en la cooperación internacional para investigar delitos cibernéticos	El Convenio establece mecanismos de cooperación internacional ágiles y eficientes	Mejora de la cooperación internacional en la investigación y persecución de ciberdelitos
Acceso a programas de desarrollo de capacidades	Los recursos y programas de capacitación en peritaje informático pueden ser limitados en Ecuador	El Convenio proporciona acceso a programas de desarrollo de capacidades a través de la Oficina especializada del Programa sobre Ciberdelincuencia del Consejo de Europa	Mejora de las habilidades y recursos disponibles para los peritos informáticos en Ecuador

El análisis comparativo entre las prácticas locales de peritaje informático forense en Quito D.M. y las disposiciones del Convenio sobre la Ciberdelincuencia resalta la crucial relevancia de la adhesión a este tratado internacional como un marco regulatorio sólido y moderno.

Este contraste pone de relieve las discrepancias y similitudes entre los estándares locales y los estándares internacionales, subrayando la necesidad de una alineación más estrecha con las directrices establecidas por el Convenio.

Además, identifica áreas específicas de mejora dentro de los procedimientos forenses digitales en la ciudad, como la adopción de protocolos más rigurosos de adquisición y preservación de evidencia, la mejora de la capacitación y recursos

para los peritos, y el fortalecimiento de los mecanismos de presentación de evidencia en procesos judiciales.

Estas mejoras propuestas no solo pueden optimizar la efectividad y credibilidad del peritaje informático forense en Quito D.M., sino que también pueden contribuir significativamente a la lucha contra la ciberdelincuencia a nivel local y global.

Comparativa de las prácticas locales del peritaje informático y Directrices Globales para Laboratorios Forenses Digitales [INTERPOL]

Los resultados de la entrevista a los expertos ofrecen una ventana única para evaluar la efectividad y la adecuación de los protocolos locales en Quito D.M. en comparación con las mejores prácticas internacionales en el ámbito del peritaje informático forense. Estos protocolos, procedimientos y estándares son esenciales para garantizar la integridad, autenticidad y fiabilidad de la evidencia digital recopilada, preservada, analizada y presentada en los procedimientos legales.

Al comparar estos hallazgos locales con las directrices y estándares establecidos por organizaciones de renombre como INTERPOL, se puede obtener una visión clara de dónde se encuentran las fortalezas y debilidades en los procesos forenses digitales en Quito D.M. Por ejemplo, si los expertos señalan deficiencias en la preservación de la evidencia digital debido a la falta de protocolos claros y actualizados, esto indica una discrepancia con las mejores prácticas internacionales, que según (INTERPOL Global Complex for Innovation, 2019), incluyen pautas detalladas sobre cómo garantizar la integridad de la evidencia a lo largo del proceso forense.

Del mismo modo, se identifican desafíos tecnológicos como la escasez de herramientas especializadas para el análisis forense digital, esto representa una brecha con respecto a los estándares establecidos por organizaciones internacionales, que recomiendan herramientas específicas o enfoques metodológicos para abordar la complejidad de la evidencia digital.

Tabla 8. Prácticas locales del peritaje informático VS Directrices Globales para Laboratorios Forenses Digitales [INTERPOL]

Aspecto	Prácticas Locales en Quito D.M.	Directrices Globales para Laboratorios Forenses Digitales [INTERPOL]
Preservación de Evidencia	Se identifican deficiencias debido a la falta de protocolos claros y actualizados.	INTERPOL proporciona pautas detalladas sobre cómo garantizar la integridad de la evidencia a lo largo del proceso forense.
Análisis de Evidencia	Se señala la escasez de herramientas especializadas para el análisis forense digital.	INTERPOL establece estándares y recomienda herramientas específicas o enfoques metodológicos para abordar la complejidad de la evidencia digital.
Protocolos y Estándares	Se reconocen como esenciales para garantizar la integridad, autenticidad y fiabilidad de la evidencia digital en procedimientos legales.	INTERPOL proporciona estándares globales para laboratorios forenses digitales que son referencia para asegurar la calidad y confiabilidad de las investigaciones digitales.

El análisis comparativo entre los procedimientos locales y las mejores prácticas internacionales proporciona una base sólida para la identificación de áreas de mejora y el desarrollo de estrategias para elevar los estándares del peritaje informático forense en Quito D.M.

Esta evaluación crítica es fundamental para garantizar la calidad y la confiabilidad de las investigaciones digitales en el contexto local y para mantenerse al día con los avances y las expectativas en el campo de la forense digital a nivel mundial.

Figura 28. Directrices Globales para Laboratorios Forenses Digitales [INTERPOL]

Fuente: INTERPOL Global guidelines for digital forensics laboratories

A pesar de que los estándares en el campo del peritaje informático forense son ampliamente reconocidos a nivel internacional y respaldados por organizaciones de renombre, como INTERPOL, se observa una disparidad significativa en su aplicación efectiva. Esta disparidad puede deberse a múltiples factores que afectan tanto a los juristas como a los peritos.

Por un lado, existe una falta generalizada de comprensión y conocimiento especializado en tecnología forense entre los profesionales del derecho, lo que dificulta la correcta interpretación y aplicación de los estándares establecidos. Además, la naturaleza dinámica y en constante evolución de la tecnología digital añade una capa adicional de complejidad, ya que los estándares deben adaptarse continuamente para abordar nuevos desafíos y escenarios emergentes.

Además, la falta de recursos y capacitación especializada para los peritos informáticos forenses también puede contribuir a la falta de aplicación de los estándares internacionales. Muchos peritos pueden carecer de acceso a la formación adecuada o a herramientas avanzadas necesarias para llevar a cabo

investigaciones forenses digitales de manera efectiva y en línea con los estándares internacionales.

Esta brecha entre los estándares internacionales y su aplicación efectiva en los procedimientos legales puede tener consecuencias significativas en la integridad y la validez de la evidencia digital presentada en los tribunales. La falta de cumplimiento de los estándares puede llevar a errores en la recopilación, preservación, análisis y presentación de la evidencia digital, lo que debilita la confianza en el sistema judicial y puede resultar en decisiones judiciales erróneas.

En consecuencia, es fundamental aumentar la conciencia y la educación sobre los estándares internacionales de peritaje informático forense tanto entre los juristas como entre los peritos. Se requiere un esfuerzo conjunto para proporcionar la capacitación y los recursos necesarios para garantizar que los profesionales involucrados en investigaciones digitales y procesos legales estén equipados para cumplir con los estándares internacionales y garantizar la integridad y la validez de la evidencia digital en el sistema judicial.

Tabla 9. Análisis de expertos Vs. Comparativa Internacional

Hallazgos Locales de Expertos en Quito D.M.	**Comparativa Internacional**	**Recomendaciones para Quito D.M.**	**Impacto y Beneficios**
Falta de protocolos claros para la recolección de evidencia digital. Escasez de herramientas especializadas	Muchos países han desarrollado protocolos detallados y herramientas avanzadas para análisis forense, como se establece en el Convenio de Budapest sobre Ciberdelincuencia.	Adoptar mejores prácticas internacionales en la elaboración de protocolos y la implementación de herramientas tecnológicas avanzadas.	Mejora significativa en la calidad y eficiencia de las investigaciones digitales en Quito D.M. Fortalecimiento de la capacidad para combatir delitos cibernéticos y proteger

para análisis forense.	Alinear con estándares internacionales y actualizar protocolos. Adquirir tecnologías utilizadas en otros países.	a los ciudadanos en un entorno digitalizado.

La correlación entre los hallazgos locales y las prácticas internacionales en el ámbito del peritaje informático forense es fundamental para comprender tanto los desafíos locales como las soluciones que se han implementado a nivel global. Al analizar los resultados obtenidos por los expertos en Quito D.M. y compararlos con las prácticas internacionales, se pueden identificar similitudes, brechas y oportunidades para mejorar los procedimientos locales.

En primer lugar, los hallazgos locales resaltan desafíos específicos que enfrentan los peritos informáticos forenses en Quito D.M., como la falta de protocolos claros para la recolección de evidencia digital y la escasez de herramientas especializadas para el análisis forense. Estos problemas pueden obstaculizar la efectividad de las investigaciones digitales y comprometer la integridad de la evidencia recopilada.

Al comparar estos hallazgos con las prácticas internacionales, se observa que muchos países han desarrollado protocolos detallados y herramientas avanzadas para abordar estos mismos desafíos. Por ejemplo, el Convenio de Budapest sobre Ciberdelincuencia establece estándares internacionales para la recolección, preservación y análisis de evidencia digital, así como para la cooperación internacional en la lucha contra delitos cibernéticos.

Esta comparación resalta la importancia de adoptar un enfoque global en el peritaje informático forense, ya que permite beneficiarse de las lecciones

aprendidas y las mejores prácticas desarrolladas en otros lugares. Al alinear los procedimientos locales con los estándares internacionales, se puede mejorar la calidad y la eficiencia de las investigaciones digitales.

Además, esta conexión con las prácticas internacionales proporciona un marco para la mejora continua al identificar áreas específicas donde se pueden implementar cambios y actualizaciones. Por ejemplo, la adopción de protocolos claros basados en estándares internacionales puede mejorar la consistencia y la calidad de las investigaciones digitales, mientras que la inversión en herramientas tecnológicas avanzadas puede aumentar la capacidad de los peritos para analizar evidencia digital de manera efectiva.

En resumen, la conexión entre los hallazgos locales y las prácticas internacionales resalta la importancia de adoptar un enfoque global en el peritaje informático forense en Quito D.M. Esto no solo permite abordar los desafíos locales de manera más efectiva, sino que también proporciona un marco para la mejora continua y el desarrollo de capacidades en el campo del peritaje informático.

3.2.2. Evolución

La evolución en el campo de las investigaciones digitales ha sido notable en las últimas décadas. Desde sus inicios, la aplicación de técnicas forenses en entornos digitales ha experimentado un crecimiento exponencial impulsado por avances tecnológicos, cambios legislativos y la creciente complejidad de los delitos cibernéticos.

Anteriormente centrado en la recuperación de datos básicos, el peritaje informático forense ha evolucionado hacia un enfoque más sofisticado que abarca áreas como el análisis de malware, la identificación de brechas de seguridad y la preservación de la cadena de custodia digital.

3.2.3. Tendencias

Las tendencias actuales en investigaciones digitales apuntan hacia una mayor integración de tecnologías emergentes como la inteligencia artificial y el análisis predictivo para mejorar la detección y prevención de delitos cibernéticos.

Así mismo, se observa una tendencia hacia la colaboración interdisciplinaria entre expertos en informática, ciberseguridad, derecho y aplicación de la ley para abordar de manera más efectiva los desafíos complejos en el ámbito forense digital. Asimismo, se destaca el creciente énfasis en la privacidad y la protección de datos, impulsado por regulaciones como el Reglamento General de Protección de Datos (GDPR) en Europa y leyes similares en otras regiones.

3.2.4. Perspectivas

En el futuro, se espera que las investigaciones digitales continúen evolucionando rápidamente en respuesta a la rápida innovación tecnológica y la sofisticación de las amenazas cibernéticas. Se prevé que la demanda de expertos en peritaje informático forense siga aumentando, junto con la necesidad de programas educativos y de capacitación especializados para satisfacer esta demanda.

Además, se espera que la regulación en torno a la privacidad y la seguridad de los datos siga siendo un tema central, lo que requerirá una adaptación continua por parte de los profesionales en el campo. De tal manera que el futuro de las investigaciones digitales se perfila como desafiante, con amplias oportunidades para aquellos que estén dispuestos a mantenerse al día con los avances tecnológicos y legales en constante cambio.

CONCLUSIONES

Del estudio realizado en el presente trabajo de investigación, fundamentado en el juicio experto y contrastado con las buenas prácticas a considerar en el ejercicio del peritaje forense informático, se puede concluir que:

- Tras analizar los resultados, se puede concluir que la falta de capacitación en metodologías forenses digitales, la ausencia de protocolos claros y definidos, así como las limitaciones tecnológicas en la adquisición y análisis de evidencia digital son los principales factores que contribuyen a la falta de comprensión del proceso en investigaciones digitales en el contexto de Quito D.M. Estos hallazgos resaltan la importancia de abordar estas deficiencias para fortalecer la integridad del proceso de investigación digital forense.

- Se evidenció que los desafíos tecnológicos enfrentados por los peritos informáticos en Quito D.M. incluyen la escasez de herramientas especializadas para análisis forense, dificultades en la adquisición de evidencia de dispositivos protegidos y limitaciones en la interpretación de datos complejos. Estos hallazgos subrayan la necesidad de invertir en tecnologías avanzadas y capacitar a los peritos para abordar la complejidad creciente de la evidencia digital.

- La falta de capacitación en metodologías forenses digitales compromete la calidad del análisis forense, aumenta el riesgo de errores en la interpretación de datos y afecta la objetividad y neutralidad de los peritajes. Es imperativo implementar programas de formación especializados y promover la certificación de peritos informáticos para garantizar la fiabilidad de los resultados periciales en investigaciones digitales.

RECOMENDACIONES

- Se recomienda implementar programas de capacitación en metodologías forenses digitales para todos los profesionales involucrados en investigaciones digitales en Quito D.M. Estos programas deben abordar la falta de conocimiento sobre protocolos de preservación de evidencia y brindar orientación sobre las mejores prácticas en la adquisición y análisis de evidencia digital.

- Se sugiere realizar inversiones en tecnologías avanzadas y herramientas especializadas para análisis forense digital. Además, es crucial proporcionar capacitación continua a los peritos informáticos para que puedan aprovechar al máximo estas herramientas y abordar eficazmente los desafíos tecnológicos en el proceso de investigación digital forense.

- Se recomienda establecer convenios de colaboración entre instituciones académicas, organizaciones profesionales y el Consejo de la Judicatura para desarrollar programas de formación especializados en metodologías forenses digitales. Estos programas deben enfocarse en mejorar las habilidades técnicas y analíticas de los peritos informáticos y garantizar que estén al tanto de las últimas tendencias y avances en el campo del peritaje informático forense.

- Se recomienda ampliar el presente estudio incluyendo una mayor diversidad de expertos participantes a nivel nacional. Esto permitirá obtener una perspectiva más completa y enriquecedora sobre los desafíos y las necesidades en este ámbito en el Ecuador, así como identificar soluciones y mejores prácticas de manera más exhaustiva.

BIBLIOGRAFIA

Alberdi, J., Battaglia, N., Blanco, M., Cardacci, G., Castellote, M., Cistoldi, P., Constanzo, B., Curti, H., Delgado, M., Gaspar, E., Gamalero, M., Giaccaglia, M., GiordanoLerena, R., Greco, F., Herlein, J., Iturriaga, J., Lamperti, S., Lasia, S., Lombardo, M., … Waimann, J. (2017). El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense. *Universidad FASTA*, 556. http://info-lab.org.ar/images/pdf/Libro.pdf

Alcívar, C., Blanc, G., & Calderón, J. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. *Revista Espacios*, *39*(42), 10.

Asociación Española de Normalización. (2020). Informes de Normalización. *Asociacion Española de Normalizacion*, *1*, 24.

Avenía, C. (2017). Fundamentos de seguridad informática. In *Areandina* (Issue 2).

Blanqueto, C. (2019). Sustento del uso justo de materiales protegidos por derechos de autor para fines educativos. *Universidad Para La Cooperación Internacional*, *0*(0), 1–23. https://n9.cl/qwqjp

Cajo, I. M. H., Pucuna, S. Y., Cajo, B. G. H., Coronado, V. M. O., & Orozco, F. V. S. (2018). Estudio Comparativo De Las Metodologías De Análisis Forense Informático Para La Examinación De Datos En Medios Digitales. *European Scientific Journal, ESJ*, *14*(18), 40. https://doi.org/10.19044/esj.2018.v14n18p40

Cazar, D. (2022). *Colateral*.

Convenio, E., Parte, E., Convenio, E., Convenio, E., Adicional, P. P., Adicional, S. P., Estados, L., Exteriores, R., General, S., Partes, E., & Partes, L. (2023). *Adhesión al Convenio sobre la Ciberdelincuencia: Beneficios Convenio sobre la Ciberdelincuencia*.

Fiscalía General del Estado. (2018). *Sentencia de un año de privación de libertad contra perito que alteró informe en caso Odebrecht*. https://www.fiscalia.gob.ec/sentencia-de-un-ano-de-privacion-de-libertad-contra-perito-que-altero-informe-en-caso-odebrecht/

Fisher, K., Mandelbaum, Y., & Walker, D. (2006). The next 700 data description languages. *Conference Record of the Annual ACM Symposium on Principles of Programming Languages*, 2–15. https://doi.org/10.1145/1111037.1111039

García Brito, P. J., & Arciniegas Castro, C. L. (2023). Las nuevas tecnologías frente al código orgánico integral penal. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, *4*(4), 116–127. https://doi.org/10.56712/latam.v4i4.1202

Gervilla Rivas, C. (2014). *METODOLOGÍA PARA UN ANÁLISIS FORENSE Trabajo de Final de Máster*. 55. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

Icaza, E. P. (2010). *Informática Forense como medio de prueba en el Ecuador Forensic computer science as way of test in Ecuador Informática forense como medio de prueba en el Ecuador Forensic computer science as way of test in Ecuador*. *108*(3).

Incibe. (2014). *RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento*. 18/06/2014. https://www.incibe.es/incibe-cert/blog/rfc3227

INTERPOL Global Complex for Innovation. (2019). Global Guidelines for Digital Forensics Laboratories. *INTERPOL Global Complex for Innovation*, *May*, 1–80. https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

ISO/IEC 27040. (2015). Information technology — Security techniques —

Guidelines for the analysis and interpretation of digital. *Iso/Iec*, *2015*.

Javier, A. (2018). *Peritaje informático: marco teórico-practico*.

Lara. (2022). *RESOLUCIÓN 147-2022 EL PLENO DEL CONSEJO DE LA JUDICATURA*. *8.5.2017*, 2003–2005. www.aging-us.com

Mairata De Anduiza, F. (2019). *Historias De Un Perito Informático Forense*.

María, P., & Sosa, E. (2023). *Evidencia digital Su importancia en la*. *466*, 1–4.

Martinez, C. (2018). Investigación Descriptiva: Tipos y Características. *Lifeder.Com*, 7.

Martins, B. (2022). *Convenio de Budapest sobre la Ciberdelincuencia en América Latina :*

Mckemmish, R. (1999). What is Forensic Computing ? *Change*, *118*(118), 1–6. http://www.mendeley.com/catalog/forensic-computing-2/

Meza, M. (2017). HRM558 | Investigación Exploratoria. *UlaOnline HRM558*, 2. http://practicasprofesionales.ula.edu.mx/documentos/ULAONLINE/Maestria/MAN/HRM558/Publicación/Semana_3/Estudiante/HRM558_S3_E_Inv_explo.pdf

MINTEL. (2022). *CIBERSEGURIDAD DEL ECUADOR*.

Na, D. E. C., & Hipertensiva, C. (2022). *Serie de Tratados Europeos n° 185*.

Nessi, A. M. (2017). *Manual de Evidencia Digital*. 64.

Nuñez, I. M. (2023). *SEÑORAS Y SEÑORES JUECES DE LA CORTE CONSTITUCIONAL DEL ECUADOR. - Nro. de Caso: 0002-19-IC*. 1–9.

Nur, F. (2020). Pengaruh Kewajiban Penyediaan Modal Minimum (Kpmm), Beban Operasional Pada Pendapatan Operasional (Bopo) Dan Financing To Deposit

Ratio (Fdr) Terhadap Profitabilitas Pt Bank Syariah Mandiri. *Skripsi*, *21*(1), 1–104. http://journal.um-surabaya.ac.id/index.php/JKM/article/view/2203%0Ahttp://mpoc.org.my/malaysian-palm-oil-industry/

Ochoa Arévalo, P. A. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. *Revista Economía y Política*, *XIV*(28), 35–46. https://doi.org/10.25097/rep.n28.2018.03

OEA. (2019). Ciberseguridad: Marco Nist. *White Paper Series*, 20. https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Salazar Méndez, D. D., Mauricio, M., Maldonado, T., Beatriz, M., & Tapia, R. (n.d.). *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad FISCALÍA GENERAL DEL ESTADO COMITÉ EDITORIAL*.

Torrado-fonseca, M. R.-álvarez M. (2016). El método Delphi. *REIRE. Revista d'Innovación i Recerca En Educación*, *9*(9 (1)), 0–2. https://doi.org/10.1344/reire2016.9.1916