Revista Ciencia & Tecnología

No. 44, 31 de octubre de 2024
ISSN impreso: 1390 - 6321

Evaluación del peritaje informático forense en Quito: Desafíos, estándares y recomendaciones para mejorar su eficacia

Evaluation of Computer Forensic Expertise in Quito: Challenges, Standards, and Recommendations for Improving Effectiveness

Iván Hermosa Llanos[1]
administradorplataforma02@*uteg.edu.ec*
https://orcid.org/0009-0009-3768-2926

Lizbeth Adriana Arcos García[2]
desarrolladoronline09@uteg.edu.ec
https://orcid.org/0009-0005-8315-050X

Henry Xavier Murillo Andrade[3]
administradorplataforma03@uteg.edu.ec
https://orcid.org/0009-0004-8377-3910

Priscilla Elizabeth Recalde Rivera[4]
precalde@uteg.edu.ec
https://orcid.org/0000-0002-0742-5509

Recibido: 5/07/2024; Aceptado: 12/11/2024

RESUMEN

Este estudio evalúa la eficacia del peritaje informático forense en Quito, Ecuador, respecto a su alineación con estándares internacionales y nacionales y su impacto en la resolución de casos judiciales. Identifica brechas y desafíos en la recolección, preservación y análisis de evidencia digital mediante una metodología mixta que incluye encuestas y entrevistas a peritos informáticos, juristas y otros actores clave del sistema judicial para obtener datos relevantes sobre prácticas, desafíos y percepciones sobre la efectividad del peritaje informático. Los resultados del estudio revelan brechas significativas entre las prácticas locales y los estándares internacionales, afectando negativamente la calidad y fiabilidad de las investigaciones digitales. Se identifican desafíos como la falta de capacitación especializada, la ausencia de protocolos estandarizados y la necesidad de mejorar la colaboración entre peritos y juristas. Las principales conclusiones destacan la necesidad de alinearse con estándares internacionales para mejorar la eficacia del peritaje informático, implementar programas de capacitación continua para peritos, desarrollar protocolos

[1] MTI, Universidad Tecnológica Empresarial de Guayaquil, Ecuador
[2] Tecnóloga en Comunicación Social, Universidad Tecnológica Empresarial de Guayaquil, Ecuador
[3] MTI, Universidad Tecnológica Empresarial de Guayaquil, Ecuador
[4] MSc. Administración de Empresas, Universidad Tecnológica Empresarial de Guayaquil, Ecuador

estandarizados para la recolección y análisis de evidencia digital, y fomentar una mayor colaboración entre los diferentes actores del sistema judicial para asegurar una administración de justicia más eficiente y precisa en la era digital.

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

ABSTRACT

This study evaluates the effectiveness of computer forensic expertise in Quito, Ecuador, concerning its alignment with international and national standards and its impact on the resolution of judicial cases. It identifies gaps and challenges in the collection, preservation, and analysis of digital evidence through a mixed methodology that includes surveys and interviews with computer forensic experts, jurists, and other key actors in the judicial system to obtain relevant data on practices, challenges, and perceptions about the effectiveness of computer forensic expertise. The study results reveal significant gaps between local practices and international standards, negatively affecting the quality and reliability of digital investigations. Challenges such as the lack of specialized training, the absence of standardized protocols, and the need to improve collaboration between forensic experts and jurists are identified. The main conclusions highlight the need to align with international standards to improve the effectiveness of computer forensic expertise, implement continuous training programs for forensic experts, develop standardized protocols for the collection and analysis of digital evidence, and foster greater collaboration among the different actors in the judicial system to ensure more efficient and accurate justice administration in the digital age.

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

Introducción

El peritaje informático forense ha surgido como un componente crucial en la investigación y resolución de delitos en la era digital. La capacidad de recolectar, preservar y analizar evidencia digital de manera adecuada es fundamental para asegurar la integridad del proceso judicial y la justicia en los casos que involucran tecnologías de la información. Esto se avala en lo que mencionan (Hidalgo et al., 2018) en otro estudio donde indican que, La informática forense implica el uso de técnicas científicas y analíticas especializadas en la infraestructura tecnológica para identificar, preservar, analizar y presentar datos que sean

aceptables en un proceso legal, especialmente en la detección de intrusiones (Hidalgo Cajo, 2014).

La informática forense se ha transformado en un componente crucial del ámbito jurídico actual, desempeñando un papel fundamental en la resolución de casos que involucran evidencia digital (Espinoza Mina, 2019). Este estudio se centra en analizar la efectividad del peritaje informático dentro del sistema legal ecuatoriano, evaluando su contribución en la resolución de casos y su conformidad con los estándares nacionales e internacionales.

En todo el mundo, las normas y prácticas para el manejo de evidencia digital han progresado notablemente, estableciendo estándares que aseguran la precisión y la confiabilidad de las investigaciones forenses (Zambrano, Tubay, Zambrano, & Zambrano, 2021). En Ecuador las entidades públicas implementan el esquema EGSI (Esquema Gubernamental de Seguridad de la Información). Sin embargo, presenta una probabilidad alta de que los recursos se vulneren mediante un delito informático.

El avance tecnológico ha cambiado radicalmente la naturaleza de los delitos y las disputas legales, introduciendo elementos digitales que requieren conocimientos especializados. La disciplina de la informática forense ha evolucionado para enfrentar estos desafíos, ofreciendo a los tribunales herramientas valiosas para interpretar y evaluar pruebas digitales. En Quito, donde el sistema legal enfrenta complejidades crecientes, la efectividad del peritaje informático es de suma importancia.

Vargas menciona que, una de las etapas más cruciales en la respuesta a un incidente de seguridad es la identificación y recuperación de la evidencia asociada con el evento (Vargas Ramos, 2021). Mientras tanto, Oscar Garcés acota que a pesar de ello las computadoras almacenan la información de manera que no puede ser recuperada o analizada mediante métodos convencionales, por lo que se requieren mecanismos alternativos a los tradicionales (Garcés Pérez, 2022).

Procedimientos y resultados en delitos informáticos

En el mismo contexto que se describe, se analizan también casos ocurridos en Ecuador:

> En mayo de 2012, el Ministerio del Ambiente de Ecuador descubrió un desvío de fondos públicos, ascendiendo a $7.600.798,00, transferidos electrónicamente a cuentas de

particulares a través del Sistema Integrado de Gestión Financiera (eSigef). Un año después, en abril de 2013, el Gobierno Autónomo Descentralizado Municipal (GADM) de Riobamba sufrió una pérdida de $13.308.261,00 debido a transferencias electrónicas no justificadas a través del Sistema de Pagos Interbancarios (SPI) del Banco Central del Ecuador. Ambos incidentes compartieron la característica de usar canales electrónicos oficiales para las transferencias de fondos (Caraguay Ramírez, 2020).

El Ministerio del Ambiente llevó a cabo una auditoría especial en 2012 para examinar las transferencias a cuentas de personas sin vínculos laborales ni contractuales con la institución. Se revisaron todo tipo de datos que, según el criterio de Carlos Alcívar, los datos pueden originarse de diversos dispositivos electrónicos, tales como discos duros, cintas de respaldo, laptops, memorias extraíbles, archivos y correos electrónicos (Alcívar, Blanc, & Calderón, 2018). Los resultados mostraron que no se pudo identificar la dirección IP de los dispositivos utilizados ni a las personas responsables de las transacciones. En el caso de Riobamba, la Contraloría General del Estado (CGE) también realizó un examen especial en 2013, pero no incluyó la revisión de los equipos de cómputo incautados por la Fiscalía General del Estado (FGE). De igual manera, no se pudieron rastrear las direcciones IP ni las operaciones electrónicas.

Ambos casos fueron también analizados por la FGE para determinar la posible comisión de delitos informáticos. Un exfuncionario del GADM fue identificado como presunto responsable. El exfiscal general destacó la importancia de la cooperación entre la Contraloría y los procesos judiciales, afirmando que una auditoría forense bien presentada es esencial para el trabajo de los fiscales en la investigación de delitos contra el patrimonio del Estado.

La Ley Orgánica de la Contraloría General del Estado (LOCGE) establece diferentes modalidades de auditoría, como el examen especial, auditoría financiera, auditoría de gestión, auditoría de aspectos ambientales y auditoría de obras públicas o de ingeniería. Sin embargo, no incluye la auditoría forense ni la informática forense, las cuales son cruciales

para el análisis, reconstrucción y validación de información siguiendo estándares internacionales.

La habilidad para clonar evidencias y trabajar con réplicas exactas permite al perito contar con elementos clave para llevar a cabo un análisis detallado de sistemas informáticos complejos y emitir un dictamen con la mayor precisión técnica (Rubio Alamillo & De Manuel, 2022).

La falta de regulaciones precisas y la necesidad de ajustarse a un entorno tecnológico en constante evolución presentan desafíos importantes para los peritos informáticos en la capital de Ecuador (Cañarte, Idrovo, Pinargote, & Ponce, 2022). Este estudio pretende examinar en detalle cómo la adhesión a protocolos nacionales e internacionales afecta la eficacia del peritaje informático. Asimismo, se investiga la percepción de la comunidad legal y judicial sobre la contribución de esta disciplina en la resolución de casos.

El objetivo final del peritaje digital es obtener pruebas sólidas que apunten a la persona o personas responsables del delito informático. Este autor (Mohammed.I., 2021), propone un marco con las siguientes fases:

- **Identificación:** La identificación es identificar elementos o dispositivos que pueden incluir: computadoras, teléfonos móviles, tabletas o cualquier otro dispositivo de almacenamiento que pueda contener información digital, la red también y el ciberespacio identificado.
- **Adquisición:** Se realiza mediante la incautación de dispositivos electrónicos encontrados en la escena del crimen y la obtención forense de los datos digitales encontrados y la duplicación y el aislamiento exactos con fines de investigación.
- **Conservación/Almacenamiento:** Una vez adquiridas las pruebas, se mantendrán aisladas y tal como están. Debe haber una cadena concreta para preservar la evidencia de ser alterada. Las imágenes o copias de solo lectura deben mantenerse en esta etapa
- **Examen:** En esta etapa se examina y analiza la evidencia preservada en el paso anterior. La evidencia extraída se puede comparar con los archivos de imagen conservados. El paso de análisis comienza con la identificación de los métodos, las herramientas y las habilidades necesarias para extraer información vital que se puede utilizar en el sistema judicial. En esta etapa de examen se sugiere un comité técnico para aprobar el software o hardware de

análisis forense digital y luego certificar este software como software y hardware de buena fe.

- **Purificación:** Las evidencias deben ser revisadas utilizando las leyes y normas vigentes. Revisar y normalizar estas evidencias digitales con las leyes y actas disponibles en el sistema hará que estas evidencias digitales sean aceptables en el sistema judicial del estado.
- **Documentación/Presentación:** Los examinadores deberán proporcionar y presentar un informe. El informe debe documentar la forma en que se llevó a cabo el proceso forense, señalar cualquier evento extraño, si existió, y las herramientas y métodos utilizados. Se siguieron los protocolos, políticas y aspectos legales, la redacción y la presentación del informe deben ser comprensibles, coherentes y atractivas. Los hechos y hallazgos deben ser precisos y claramente presentados.
- **Difusión:** Debe haber una política clara sobre la transmisión y difusión de la información relativa a todas las etapas anteriores de estos procesos forenses digitales. Es posible que no se divulgue toda la información, pero la información esencial debe servir como fuente para otros casos digitales.

Por lo detallado anteriormente se define que:

> Los delitos informáticos y el peritaje digital tienen tanto que ver con las personas involucradas en este comportamiento desviado como con la tecnología. Por lo tanto, la investigación centrada en las personas es vital a la hora de abordar el fenómeno de los delitos informáticos. El objetivo de la presente investigación es analizar el marco legal de la República del Ecuador que abarca muchos aspectos relacionados con el delito informático y el peritaje digital (Rodríguez, Idrovo, Pinargote, & Ponce, 2022).

La relevancia de esta investigación radica en ofrecer una comprensión integral de la situación actual del peritaje informático en el Distrito Metropolitano de Quito, identificando áreas que necesitan mejoras y proporcionando recomendaciones para fortalecer su papel en

el sistema legal. Utilizando un enfoque mixto que combina métodos cuantitativos y cualitativos, se busca obtener una perspectiva completa y contextualizada que enriquezca el conocimiento en este ámbito.

> En el Ecuador una gran cantidad de casos necesitan ser investigados por las autoridades competentes, los cuales en su gran mayoría no pueden ser atendidos ya que necesitan ciertos conocimientos ajenos a su saber específico y requieren ser auxiliados por personas con conocimientos, procedimientos establecidos y reconocidos legalmente, conocimientos que únicamente especialista en informática forense posee, con el fin de enriquecer la capacidad de juzgar en un procedimiento Penal (COIP) o Civil (COGEP) este último regula la actividad procesal en todas las materias, excepto la constitucional, electoral y penal, con estricta observancia del debido proceso (Loarte & Grijalva, 2017).

Este estudio aspira a proporcionar aportes significativos a las comunidades académica, jurídica y pericial, ofreciendo una visión integral sobre el estado actual y las perspectivas futuras de la informática forense en el contexto legal ecuatoriano.

Sera el transcurso de los años los que juzgaran el verdadero efecto del nuevo régimen en la sociedad ecuatoriana y en qué medida se cumple de manera efectiva las sanciones ante acciones ilícitas, y que beneficios nacionales se obtienen con las mismas (Aparicio, 2022).

Metodología

Este estudio adopta un enfoque exploratorio-descriptivo, utilizando una metodología mixta que combina tanto métodos cualitativos como cuantitativos. El diseño de investigación exploratorio-descriptivo permite una comprensión profunda y detallada de las prácticas y desafíos asociados con el peritaje informático forense en Quito, Ecuador. Ochoa y Yunker (2021) indican que "este enfoque es especialmente adecuado para examinar fenómenos donde la información es escasa o requiere una nueva interpretación contextual." (p. 17)

La población del estudio incluye a peritos informáticos, juristas y otros actores clave del sistema judicial en Quito, que poseen experiencia relevante en el uso y aplicación del peritaje informático. La muestra se selecciona mediante un muestreo intencional, eligiendo expertos con conocimientos profundos y experiencia práctica en el área de investigación.

Criterios de inclusión:

- Profesionales con al menos cinco años de experiencia en peritaje informático.
- Juristas con experiencia en casos que involucren evidencia digital.
- Actores del sistema judicial con participación directa en la gestión de pruebas digitales.

Criterios de exclusión:

- Profesionales sin experiencia directa en peritaje informático.
- Actores judiciales sin interacción con evidencia digital.
- Técnicas e instrumentos de recolección de datos

Las técnicas de recolección de datos incluyeron:

Encuestas estructuradas: Dirigidas a peritos informáticos y juristas, para obtener datos cuantitativos sobre prácticas, desafíos y percepciones respecto al peritaje informático.

Entrevistas semiestructuradas: Realizadas con actores clave del sistema judicial, proporcionando datos cualitativos profundos y detallados.

Revisión documental: Incluye la revisión de leyes, normativas y protocolos tanto nacionales como internacionales relacionados con el peritaje informático.

Instrumentos de recolección:

Cuestionarios: Diseñados para recoger información sobre prácticas y desafíos en el peritaje informático.

Guías de entrevista: Estructuradas para explorar temas específicos en profundidad durante las entrevistas.

Los datos cuantitativos recopilados a través de encuestas fueron analizados mediante estadística descriptiva, utilizando software especializado como SPSS. Esto permitió identificar patrones y tendencias en las prácticas y percepciones de los participantes.

Los datos cualitativos obtenidos de las entrevistas se analizaron utilizando análisis de contenido temático. Este enfoque facilitó la identificación de temas recurrentes y emergentes, proporcionando una comprensión rica y contextualizada de los desafíos y prácticas en el peritaje informático forense en Quito.

La combinación de métodos cuantitativos y cualitativos en esta investigación proporciona una visión integral de la situación actual del peritaje informático forense en Quito. Esta metodología mixta permite no solo cuantificar las percepciones y prácticas, sino también explorar en profundidad los contextos y razones detrás de estos hallazgos, lo cual es esencial para formular recomendaciones prácticas y efectivas para mejorar la eficacia del peritaje informático en el sistema judicial ecuatoriano.

Resultados y discusión

Se llevó a cabo un análisis exhaustivo de los resultados obtenidos de una ronda de preguntas dirigida a expertos en peritaje informático y juristas mediante el método Delphi. Se exploraron temas relacionados con el debido proceso en investigaciones digitales, desafíos tecnológicos y el impacto de la falta de capacitación especializada.

- **Análisis de resultados de las tres rondas de preguntas**

Tras analizar los resultados de las tres rondas del método Delphi, se observa un consenso generalizado en varios aspectos clave del peritaje informático forense en Quito D.M. Se destaca la necesidad de establecer protocolos claros para la recolección de evidencia digital, mejorar las capacidades tecnológicas y proporcionar capacitación especializada para fortalecer las investigaciones digitales en la ciudad.

Tabla 1 Matriz de consenso primera ronda de preguntas

xpertos	regunta 1	regunta 2	regunta 3	regunta 4	Pregunta 5
Expert 1	a, b, c	A	a, b, c	Moderado	a, c
Expert 2	a, c	A	a, b, c	uficiente	a, c
Expert 3	a, b, c	a, b, c	a, b, c	Moderado	a, b, c
Expert 4	a, c	a, b, c	a, c	Moderado	a, c
Expert 5	a, c	a, c	a, b, c	uficiente	a, c
Expert 6	a, b, c	a, c	b	suficiente	B
Expert 7	a, c	a, b, c	a, b, c	Moderado	a, c
Expert 8	a, b, c	a, b, c	a, b, c	suficiente	B

Expert 9	a, b, c	a, b, c	a, b, c	Moderado	a, b, c
xpert 10	a, b, c	a, b, c	a, b, c	suficiente	a, c
onsenso	a, c	A	a, b, c	Moderado	a, c

Fuente: Perdomo Córdova (2024)

Los expertos coinciden en que la falta de capacitación, protocolos definidos y limitaciones tecnológicas son los principales factores que contribuyen a la falta de comprensión del proceso en investigaciones digitales en Quito D.M. Se destaca la importancia de aplicar protocolos de preservación de evidencia. Hay un nivel moderado de comprensión del proceso desde los profesionales legales. Las recomendaciones implementan programas de capacitación, fomento de colaboración entre peritos informáticos y profesionales legales, y guías internacionales para peritaje informático.

Tabla 2 Matriz de consenso segunda ronda de preguntas

Expert o	**Pregun ta 1**	**Pregun ta 2**	**Pregun ta 3**	**Pregun ta 4**	**Pregun ta 5**
Expert 1	Sí	a, c	a, b, c	A	a, b, c
Expert 2		a, b, c	a, b, c	A	a, b, c
Expert 3	Sí	a, b, c	a, b, c	A	a, b, c
Expert 4	Sí	a, b, c	a, b, c	A	a, b, c
Expert 5		a, c	a, b, c	A	a, b, c
Expert 6	Sí	a, b, c	a, b, c	A	a, b, c
Expert 7	Sí	a, b, c	a, b, c	A	a, b, c
Expert 8	Sí	a, b, c	a, b, c	A	a, b, c
Expert 9	Sí	a, b, c	a, b, c	A	a, b, c
Expert 10	Sí	a, b, c	a, b, c	A	a, b, c
Conse nso	Sí	a, b, c	a, b, c	A	a, b, c

Fuente: Perdomo Córdova (2024)

La mayoría de los expertos (Expertos 1, 3, 4, 6, 7, 8, 9 y 10) están de acuerdo en los factores que contribuyen a la falta de comprensión en investigaciones digitales, aunque algunos

(Expertos 2 y 5) no dieron respuestas claras, mostrando disparidad en las percepciones. Todos los expertos (Expertos 1-10) coinciden en los principales desafíos tecnológicos para los peritos informáticos en Quito D.M., así como en las tecnologías necesarias para abordarlos. También hay consenso en que la falta de acceso o capacitación en tecnologías específicas limita la efectividad de las investigaciones digitales y la credibilidad de los resultados periciales

Tabla 3 Matriz de consenso tercera ronda de preguntas

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

Fuente: Perdomo Córdova (2024)

Los expertos están de acuerdo en que los desafíos tecnológicos identificados son válidos para el contexto de Quito D.M. Todos coinciden en que la falta de capacitación compromete la calidad del análisis forense y aumenta el riesgo de errores. La mayoría señala la necesidad de mejorar en técnicas de adquisición y preservación de evidencia digital, análisis de malware y interpretación de resultados. Todos están de acuerdo en desarrollar programas especializados, promover la certificación de peritos informáticos y colaborar con instituciones académicas.

Conclusiones

La investigación realizada sobre la eficacia del peritaje informático forense en Quito, Ecuador, ha revelado importantes hallazgos que contribuyen significativamente al conocimiento en esta área. En primer lugar, se identificaron brechas significativas entre las prácticas locales y los estándares internacionales, lo que afecta negativamente la calidad y fiabilidad de las investigaciones digitales. Este hallazgo subraya la necesidad urgente de alinear las prácticas locales con los estándares internacionales para asegurar la integridad de la evidencia digital y la validez de los resultados periciales.

Uno de los desafíos más críticos detectados fue la falta de capacitación especializada entre los peritos informáticos. La carencia de formación continua y actualizada compromete la capacidad de los profesionales para realizar análisis precisos y detallados, lo que puede influir directamente en los resultados de los casos judiciales. Por lo tanto, es imperativo implementar programas de capacitación continua que aborden las últimas metodologías y tecnologías en el campo del peritaje informático forense.

Además, la ausencia de protocolos estandarizados para la recolección y análisis de evidencia digital fue otro punto destacado en la investigación. La implementación de estos protocolos es esencial para garantizar un manejo consistente y riguroso de la evidencia digital, minimizando el riesgo de errores y aumentando la confiabilidad de los hallazgos forenses.

La colaboración entre peritos y juristas también se identificó como un área que necesita fortalecerse. Una mayor cooperación y comunicación entre estos actores puede mejorar significativamente la interpretación y uso de la evidencia digital en los procesos judiciales, asegurando así una administración de justicia más precisa y eficiente.

Futuras líneas de investigación podrían explorar en mayor profundidad los impactos específicos de la capacitación y los protocolos estandarizados en la efectividad del peritaje informático. También sería valioso investigar la adopción de nuevas tecnologías y metodologías en el análisis forense y su integración en el sistema judicial ecuatoriano.

Este estudio proporciona una base sólida para futuras investigaciones y destaca áreas clave donde se pueden implementar mejoras para fortalecer el papel del peritaje informático forense en el sistema legal de Quito. Las recomendaciones presentadas no solo buscan mejorar las prácticas actuales, sino también promover un enfoque más cohesionado y eficiente en el manejo de evidencia digital, contribuyendo así a la evolución y sofisticación de la justicia en la era digital.

Referencias bibliográficas

Alcívar, C., Blanc, G., & Calderón, J. (2018). Aplicación de la ciencia forense en los. *Espacios*, *39*(42), 15. https://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Aparicio, V. (2022). Computer crimes in Ecuador according to the COIP: documentary analysis. *3*(1). https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/284

Cañarte, T., Idrovo, P., Pinargote, A., & Ponce, F. (2022). Peritaje digital y delito informático. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *4*(5). https://editorialalema.org/index.php/pentaciencias/article/view/271

Caraguay Ramírez, S. (2020). Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007-2019. *Scielo*, *2*(11). doi:http://orcid.org/0000-0001-6027-786X

Espinoza Mina, M. (2019). Informática Forense: Una revisión sistemática de la literatura. *Revista de Ciencias Humanísticas y Sociales*, *4*(2), 18. https://www.redalyc.org/pdf/6731/673171022006.pdf

Garcés Pérez, O. (2022). Estructura de un laboratorio de Informática Forense para la Dirección de Seguridad Informática. *Scielo*, *16*(4), 15. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992022000400134#B15

Hidalgo Cajo, I. (2014). Análisis preliminar y Diseño de una Herramienta de toma de decisiones como soporte para las tareas de Análisis Forense Informático.

Hidalgo Cajo, I., Yasaca Pucuna, S., Hidalgo Cajo, B., Oquendo Coronado , V., & Salazar Orozco, F. (2018). Estudio Comparativo De Las Metodologías De Análisis Forense Informático Para la Examinación de Datos en Medios Digitales. *European Scientific Journal*, *14*(18), 40. doi:https://doi.org/10.19044/esj.2018.v14n18p40

Loarte, B., & Grijalva, J. (2017). Marco de trabajo estandarizado para el análisis forense de la evidencia digital. *Revista Publicando*, *4*(11), 37. https://revistapublicando.org/revista/index.php/crv/article/view/463/pdf_341

Mohammed.I., A. (2021). A novel study of preventing the cyber security threats. doi:https://www.sciencedirect.com/science/article/pii/S2214785321029345?via%3Dihub

Ochoa Pachas, J., & Yunkor Romero, Y. (2021). El estudio descriptivo en la investigación científica. *Acta Jurídica Peruana*, *2*(2). http://revistas.autonoma.edu.pe/index.php/AJP/article/view/224

Rodríguez, T., Idrovo, P., Pinargote, A., & Ponce, F. (2022). Peritaje digital y delito informático. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *4*(5). https://editorialalema.org/index.php/pentaciencias/article/view/271

Rubio Alamillo, J., & De Manuel, C. (2022). Peritaje informático, análisis forense digital y respuesta a incidentes. *Seguridad de la información*(19). https://revista.uclm.es/index.php/ruiderae/article/view/3087

Vargas Ramos, D. (2021). Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta. *Revista PGI*, *8*, 4. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/55

Zambrano, M., Tubay, C., Zambrano, J., & Zambrano, D. (s.f.). Informática forense – el caos de la manipulación de la información digital. *Suplemento CICA Multidisciplinario*, *5*(11). https://uleam.suplementocica.org/index.php/SuplementoCICA/article/view/34