593 Digital Publisher
CEIT
ISSN 2588-0705

Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva legal en Ecuador. Una revision sistemática

Analysis of forensic techniques and tools for the investigation of computer crimes and its legal perspective in Ecuador. A systematic review

Edwin Agustin Echeverría-Espinoza [1]
Universidad Católica de Cuenca - Ecuador
edwin.echeverria.e@gmail.com

Manuel Salvador Álvarez-Vera [2]
Universidad Católica de Cuenca - Ecuador
malvarezv@ucacue.edu.ec

doi.org/10.33386/593dp.2024.6.2775

V9-N6 (nov-dic) 2024, pp 644-652 | Recibido: 10 de septiembre del 2024 - Aceptado: 04 de octubre del 2024 (2 ronda rev.)

1 ORCID: https://orcid.org/0009-0004-2198-2995
2 ORCID: https://orcid.org/0000-0002-2521-0042

Cómo citar este artículo en norma APA:A

Echeverría-Espinoza, E., Álvarez-Vera, M., (2024). Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva legal en Ecuador. Una revision sistemática. 593 Digital Publisher CEIT, 9(6), 644-652, https://doi.org/10.33386/593dp.2024.6.2775

Descargar para Mendeley y Zotero

RESUMEN

La investigación de delitos informáticos en Ecuador se ha convertido en un gran desafío debido al aumento de la conectividad y la sofisticación de las técnicas delictivas. En este contexto, la informática forense juega un papel crucial en la identificación, preservación y análisis de evidencias digitales para apoyar la investigación de estos delitos. El objetivo principal de este artículo es la de realizar un análisis de las técnicas y herramientas forenses para la investigación de estos delitos, así como sus aspectos legales con respecto a la admisibilidad de las pruebas digitales.

Para este propósito, se utilizó bases de datos académicas tales como Scielo, Web of Science y Scopus en la que se incluyeron estudios publicados en los últimos diez años. Se identificaron algunas técnicas forenses y herramientas de software que incluyen la adquisición de imágenes de discos, la recuperación de archivos borrados, el análisis de registros de actividad y el examen de metadatos. Las técnicas más utilizadas incluyen el método Lockdown, el método Stratt y el método GCII, mientras que las herramientas más comunes abarcan tanto software comercial como de código abierto, tales como EnCase, FTK y X-Ways Forensics.

La investigación también reveló que la legislación ecuatoriana proporciona un marco legal general para la investigación de delitos informáticos. No obstante, existen desafíos significativos en la ley en cuanto se refiere a su aplicación práctica, que incluya la necesidad de un marco legal más específico, capacitación de los investigadores forenses, y la necesidad de actualizar las normas para reflejar los avances tecnológicos.

Palabras claves: informática forense, delitos informáticos, técnicas forenses, herramientas forenses, legislación ecuatoriana.

ABSTRACT

The investigation of computer crimes in Ecuador has become a major challenge due to the increase in connectivity and the sophistication of criminal techniques. In this context, forensic computing plays a crucial role in the identification, preservation and analysis of digital evidence to support the investigation of these crimes. The main objective of this article is to perform an analysis of the forensic techniques and tools for the investigation of these crimes, as well as their legal aspects regarding the admissibility of digital evidence.

For this purpose, academic databases such as Scielo, Web of Science and Scopus were used, which included studies published in the last ten years. Some forensic techniques and software tools were identified, including the acquisition of disk images, the recovery of deleted files, the analysis of activity logs and the examination of metadata. The most commonly used techniques include the Lockdown method, the Stratt method, and the GCII method, while the most common tools encompass both commercial and open source software, such as EnCase, FTK, and X-Ways Forensics.

The research also revealed that Ecuadorian legislation provides a general legal framework for the investigation of computer crimes. However, there are significant challenges in the law when it comes to its practical application, including the need for a more specific legal framework, training of forensic investigators, and the need to update regulations to reflect technological advances.

Keywords: computer forensics, computer crimes, forensic techniques, forensic tools, ecuadorian legislation.

Introducción

Los delitos informáticos representan una amenaza creciente para la sociedad, caracterizándose por ser cada vez más sofisticados, dañinos y comunes. Los delincuentes cibernéticos emplean una variedad de técnicas para cometer delitos como el robo de identidad, fraude electrónico, ciber espionaje y la distribución de malware. Este panorama se complica aún más debido al acelerado incremento del uso de la tecnología en todos los ámbitos, la mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un plazo breve de tiempo. (seguros informáticos, 2009).

"Los delitos informáticos son actividades ilícitas realizadas por medios, tecnología y equipos de comunicación, con el objetivo de causar daños, desgastes o paralizar el uso de los sistemas informáticos." (Ramírez, 2017, p.1). Bajo esta definición podemos concluir que al igual que cualquier otro tipo de delito buscan un beneficio para el victimario y causan un perjuicio para la víctima, y al estar tipificados en la ley como una conducta o acción antijurídica es penada acuerdo a la gravedad de la misma. (COIP,2014, p.20).

El impacto de estos delitos es significativo y va en aumento. Según un informe del Foro Económico Mundial, el costo global de los delitos cibernéticos en 2022 fue de 6 billones de dólares, representando un incremento del 15% en comparación con 2021. Este impacto puede medirse en términos económicos como robo de información o interrupción de sistemas informáticos, sociales tales como: daños a la privacidad y reputación de las víctimas; y políticos como la desestabilización de gobiernos y manipulación de elecciones (Foro Económico Mundial, 2022).

Ecuador no es la excepción a esta problemática. Según datos de la Policía Nacional, en 2022 se registró un aumento del 30% en las denuncias de delitos informáticos comparados con el año 2021, lo que pone en evidencia lo vulnerable que estamos como país en este sentido. La complejidad creciente de estos delitos ha puesto a prueba la capacidad de las técnicas y herramientas de análisis forense para investigarlos eficazmente, constituyendo un desafío considerable para los investigadores forenses.

El análisis forense digital es una disciplina compleja y en constante evolución. Los investigadores forenses deben poseer experiencia en el uso de técnicas y herramientas específicas y mantenerse actualizados con las últimas tendencias y tecnologías para analizar la evidencia digital. Entre las herramientas utilizadas se incluyen aquellas para la adquisición, preservación y análisis forense de datos, empleando técnicas tanto manuales como automatizadas.

Esta investigación contempla el análisis de las técnicas y herramientas forenses más utilizadas en la investigación de este tipo de delitos y su perspectiva legal en Ecuador.

Además, se busca identificar las brechas existentes en la legislación ecuatoriana y proponer recomendaciones para fortalecer el análisis e investigación de este tipo de delitos. Mejorar la investigación de estos delitos en Ecuador es un reto considerable debido a su complejidad y a la falta de formación especializada en técnicas forenses digitales. Ecuador ha reconocido la importancia de combatir los delitos informáticos y ha promulgado leyes contempladas en el Código Orgánico Integral Penal (COIP) y la ley de comercio electrónico, firmas electrónicas y mensajes de datos. No obstante, la legislación ecuatoriana aún requiere actualización y fortalecimiento para adaptarse a las nuevas modalidades delictivas y las últimas tecnologías. Esta investigación contribuirá a este esfuerzo, proporcionando una visión general de las técnicas y herramientas forenses disponibles y la aplicación de la ley en cuanto se refiere a delitos informáticos (COIP, 2021; Ley de Comercio Electrónico, 2021).

Además, esta investigación pretende apoyar la formación de estudiantes e investigadores forenses, la recomendación de técnicas y herramientas forenses de uso común en la investigación de estos delitos, sus usos de acuerdo a las necesidades, identificar las tendencias en su desarrollo y examinar los delitos informáticos más comunes junto con su tipificación en la legislación ecuatoriana. Todo esto con el fin de mejorar la efectividad de las investigaciones en la recuperación de información, el análisis de archivos y redes de computadoras (Casey, 2011).

Método

Para este estudio se realizó una revisión de las técnicas y herramientas forenses más comunes y eficaces, con el objetivo de identificar, analizar e interpretar toda la documentación relevante sobre este tema. La metodología empleada se basó en la selección de la literatura utilizando criterios de búsqueda específicos. Esto permitió enfocarse únicamente en investigaciones y artículos que respaldaran los resultados sintetizados presentados en este trabajo.

La naturaleza de la investigación fue de tipo cualitativa y comparativa, utilizando diversas fuentes de información para conocer las técnicas y herramientas forenses más conocidas y usadas en la investigación de delitos informáticos. La investigación involucró un proceso de descripción narrativa proporcionada por la información compilada a través del cotejo de criterios, así como un análisis correspondiente de cada una de las técnicas y herramientas, además de los delitos establecidos en el COIP y sus respectivas sanciones.

Para abordar el tema de estudio, se planteó la pregunta general: ¿Cuáles son las técnicas y herramientas forenses más utilizadas en la investigación de delitos informáticos y sus aspectos legales en Ecuador?. Se utilizaron palabras clave como: "informática forense", "delitos informáticos", "herramientas forenses", "técnicas forenses" y "legislación ecuatoriana". La pregunta de investigación se subdividió en otras más específicas: ¿Cuáles son las técnicas forenses más utilizadas para la investigación de delitos informáticos? ¿Cuáles son las herramientas de software más utilizadas y eficaces para la investigación de delitos informáticos? ¿Qué tipos de delitos informáticos están contemplados en el COIP y cuáles son las sanciones?. Para identificar las técnicas y herramientas forenses para la investigación de delitos informáticos, se diseñaron estrategias de búsqueda que combinaban términos y palabras clave relevantes. La estrategia se basó en las palabras "delitos informáticos", "técnicas forenses digitales" y "herramientas de software forenses".

Las cadenas de búsqueda estructurada fueron: "técnicas forenses digitales" OR "digital forensic techniques" y "herramientas de software forenses" OR "forensic software tools". La búsqueda se limitó a los títulos de los artículos en las bases de datos electrónicas consultadas, los artículos que contenían las palabras clave definidas fueron recuperados y revisados en detalle, la selección se restringió a publicaciones desde el año 2014 hasta la actualidad. Los tipos de publicaciones fueron principalmente artículos de revistas científicas, mientras que se excluyeron los trabajos en diapositivas, libros y literatura gris que corresponde a artículos no publicados.

Para el proceso de selección y revisión de los trabajos de investigación se tomaron solo aquellos que estuvieron relacionados a la pregunta de investigación, con respecto al procedimiento para seleccionar los estudios se aplicó las cadenas de búsqueda exclusivamente en el título de la publicación; para posteriormente revisar el contenido completo después de haber aplicado todos los criterios de búsqueda.

En la selección inicial de fuentes se realizó la ejecución con las cadenas de búsqueda antes mencionadas, lo cual arrojó muchos documentos por lo cual procedió a aumentar los criterios de búsqueda para reducir los resultados. La segunda búsqueda fue basada en aplicar la cadena de búsqueda en el campo por "título", esto permitió eliminar algunos resultados pocos útiles. Finalmente para obtener la lista definitiva

de estudios primarios, se añadió un filtro de solo los artículos científicos y con texto completo. Al revisar los artículos filtrados se excluyeron los que no estaban escritos como trabajos científicos o porque la temática no era la misma que estábamos buscando. Al final, 16 estudios fueron revisados y analizados en su totalidad.

Resultados

La revisión sistemática realizada evidenció la existencia de un conjunto de técnicas y herramientas forenses para la investigación de delitos informáticos. Entre las técnicas más comunes se encuentran la adquisición de imágenes de discos duros, el análisis de archivos, la recuperación de datos eliminados y el análisis de redes. En cuanto a las herramientas forenses más utilizadas, destacan EnCase Forensic Software, Autopsy y Forensic Toolkit.

Se logró identificar seis principales de técnicas forenses comúnmente empleadas en la investigación de delitos informáticos en el contexto ecuatoriano. Entre estos delitos se encuentran el acceso no autorizado a sistemas informáticos, el robo de datos, el fraude informático, el daño o destrucción de datos, la distribución de malware y la pornografía infantil. Cabe destacar que las técnicas forenses informáticas tienen la capacidad de ser aplicadas en una amplia gama de dispositivos, incluyendo computadoras, tabletas, teléfonos inteligentes, unidades de almacenamiento extraíbles y redes informáticas. La extracción de una evidencia digital se realizará a partir de una utilización amplios recursos, por medio de software, hardware o herramientas para este propósito. De este modo, la extracción de una evidencia puede ser realizada a través de los más variados métodos. (Taborda, 2017).

Bajo este contexto, podemos decir que las técnicas forenses informáticas más comunes incluyen:

- Adquisición de imágenes: es el proceso de crear una copia exacta de un dispositivo de almacenamiento digital como un disco duro o pendrive. La imagen se puede usar para analizar el dispositivo sin riesgo de dañar los datos originales.
- Análisis de archivos: se utiliza para identificar y examinar archivos en un dispositivo de almacenamiento digital. Los analistas forenses pueden buscar archivos específicos, como documentos, imágenes o videos.
- Recuperación de datos: se utiliza para recuperar datos que se han eliminado o dañado. Existen una variedad de herramientas y técnicas para recuperar datos, incluso si se han eliminado intencionalmente.
- Análisis de redes: se emplea para examinar el tráfico de red en busca de indicios de actividad delictiva. Mediante este análisis, se pueden identificar direcciones IP, nombres de usuario, contraseñas y otros datos relevantes que permiten rastrear a los responsables de los delitos.
- Análisis de registros: se utiliza para analizar los registros de un sistema informático en busca de evidencia de actividad delictiva. Los registros pueden incluir información sobre quién ha iniciado sesión en el sistema, qué archivos se han accedido y qué programas se han ejecutado.
- Examen de dispositivos móviles: se utiliza para analizar dispositivos portátiles, como teléfonos inteligentes y tabletas, en busca de pruebas de actividad delictiva. Este proceso permite extraer información crucial como mensajes de texto, registros de llamadas y fotografías que pueden ser determinantes en la investigación.

En cuanto a las herramientas forenses, se identificaron dieciséis principales herramientas de software especializados en la adquisición, análisis y presentación de evidencia digital. La herramienta o herramientas que se utilicen dependerán de las circunstancias específicas de la investigación. Las más utilizadas incluyen:

- Adquisición de evidencia: se utilizan para crear una copia exacta de un dispositivo de almacenamiento digital, como un disco duro o una unidad USB. Entre las herramientas más utilizadas están Forensic Toolkit, Imager, EnCase Forensic y Prozesse.

- Análisis de evidencia: se utilizan para examinar la evidencia adquirida en busca de pruebas de actividad delictiva. Entre las más populares se encuentran Autopsy, The Sleuth Kit y Forensic Toolkit.
- Recuperación de datos: se utilizan para recuperar datos que se han eliminado o dañado. Algunas de las herramientas más utilizadas son Recuva, Disk Drill y Stellar Data Recovery.
- Análisis de redes: se utilizan para capturar y analizar el tráfico de red. Entre las más populares se encuentran Wireshark, NetworkMiner y Bro.
- Investigación de malware: se utilizan para identificar y analizar malware. Algunas de las herramientas más populares incluyen IDA Pro, Malwarebytes y Metasploit.

En el ámbito legal ecuatoriano, el Código Orgánico Integral Penal (COIP) define un marco general de sanciones para los diversos tipos de delitos informáticos. La severidad de la pena impuesta se encuentra en relación directa con la gravedad del delito cometido, los daños causados y los antecedentes penales del infractor. En este sentido el (COIP) tipifica a diez delitos informáticos entre los más importantes, tales como el acceso no autorizado a sistemas informáticos, la interceptación de datos y la falsificación de documentos informáticos. A pesar de estos avances, el COIP presenta vacíos legales en materia de informática forense, lo que obstaculiza la investigación y persecución eficaz de los delitos informáticos.

Es así que, Zambrano-Mendieta, Dueñas-Zambrano y Macías-Ordóñez (2016) demostraron que en el marco jurídico nacional, se consagra el derecho a la protección de datos de carácter personal, a la intimidad personal, al derecho a la inviolabilidad y al secreto de la correspondencia física y virtual, el delito informático atenta contra estos derechos específicos.

A continuación, se presenta un resumen de algunas de las penas más relevantes establecidas en el Código Orgánico Integral Penal (COIP) para sancionar los delitos informáticos:

Tabla 1

Delitos informáticos contemplados en la legislación ecuatoriana - COIP

Descripción del Delito	Artículo	Años de prisión
Distribución de material pornográfico a niñas, niños y adolescentes	Art. 168	1 a 3 años
Violación a la intimidad	Art.178	1 a 3 años
Reprogramación o modificación de información de equipos terminales móviles	Art. 191	1 a 3 años
Revelación ilegal de base de datos	Art. 229	3 a 5 años
Interceptación ilegal de datos	Art. 230	3 a 5 años
Transferencia electrónica de activo patrimonial	Art. 231	3 a 5 años
Ataque a la integridad de sistemas informáticos	Art. 232	3 a 5 años
Delitos contra la información pública reservada legalmente	Art. 233	7 a 10 años
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	Art. 234	3 a 5 años.
Interceptación de comunicaciones o datos informáticos	Art. 476	3 a 5 años

Nota: Datos tomados del Código Orgánico Integral Penal de Ecuador

Cabe recalcar que las penas descritas anteriormente representan solo las de mayor aplicabilidad de aquellas contempladas en el COIP para los delitos informáticos. Además de las penas privativas de libertad, el COIP establece un conjunto de sanciones complementarias, tales como: multas, decomiso de equipos informáticos, inhabilitación profesional y reparación del daño causado. La aplicación de estas sanciones dependerá de las particularidades de cada caso y será determinada por un juez competente.

Conclusiones

El auge de los delitos informáticos es una realidad innegable, impulsada en gran medida por los avances tecnológicos y la falta de conocimiento por parte de los usuarios sobre el uso seguro y responsable de estas herramientas. Abordar esta problemática de manera efectiva requiere de un compromiso profundo con la investigación y la implementación de medidas preventivas adecuadas. En el panorama actual, caracterizado por la omnipresencia de la tecnología, resulta prácticamente imposible

encontrar un delito en el que los dispositivos digitales, las tecnologías de comunicación y las computadoras no estén involucrados de alguna manera, ya sea directa o indirecta. Esta realidad pone de manifiesto la urgente necesidad de contar con profesionales forenses altamente capacitados, así como con técnicas y herramientas eficaces para investigar y combatir estos delitos de manera eficiente. En este sentido, González-Sánchez et al (2019) argumentan que el Estado ecuatoriano debe priorizar la formación de especialistas forenses y tecnologías adecuadas para implementar políticas públicas de combate a los crímenes informáticos.

Los estudios analizados se centraron en la investigación forense en diversos entornos: computadoras, redes, dispositivos móviles y la información almacenada en la nube. Entre estos, el análisis forense en la nube se presenta como uno de los más desafiantes y complejos, debido a que muchas de las técnicas forenses tradicionales, como el acceso físico a la evidencia, no son aplicables en este entorno, especialmente en nubes públicas, privadas virtuales y de la comunidad. En estos casos, la recopilación y organización de las pruebas dependen en gran medida de la colaboración con los proveedores de servicios en la nube, quienes suministran los datos forenses necesarios.

Este estudio busca contribuir al conocimiento actual sobre la investigación forense digital y servir como base para futuras investigaciones en este campo en constante evolución. Entre las líneas de trabajo futuro se propone un análisis detallado de las herramientas tecnológicas disponibles para el análisis de información en la nube, tomando en cuenta la complejidad que este análisis presenta debido a la dispersión física de los datos en múltiples servidores. Adicionalmente, se identifica la necesidad de explorar en profundidad el perfil laboral o profesional que debe tener el especialista forense en la actualidad, un aspecto que no ha sido ampliamente abordado en la literatura. En este sentido, se presenta la oportunidad de desarrollar una revisión sistemática adicional de las publicaciones relacionadas con este tema, lo cual permitiría enriquecer aún más la comprensión y las capacidades para enfrentar los retos que plantean los delitos informáticos en la era digital.

Discusión

La investigación de delitos informáticos en Ecuador presenta una serie de desafíos que abarcan tanto el ámbito técnico como el legal. Uno de los principales obstáculos técnicos reside en la volatilidad de la evidencia digital, la cual puede ser fácilmente alterada o eliminada, dificultando el proceso de investigación y la obtención de pruebas contundentes. Esto hace que sea crucial contar con procedimientos adecuados de adquisición y preservación de la evidencia. La volatilidad de los datos requiere técnicas precisas y confiables para garantizar que la información recopilada sea válida y admisible en un tribunal.

Otro desafío técnico importante es la complejidad de los sistemas informáticos, lo que dificulta la identificación y extracción de evidencia digital relevante. Los sistemas actuales, con su gran cantidad de datos y complejas estructuras, requieren herramientas forenses especializadas y personal capacitado para su uso. Es indispensable invertir en formación continua para los profesionales forenses, así como en la adquisición de herramientas tecnológicas avanzadas que permitan manejar la complejidad de las investigaciones.

En el ámbito legal, la legislación ecuatoriana aún necesita ser más específica en la regulación de la investigación de delitos informáticos. Esta falta de especificidad genera incertidumbre jurídica y puede dificultar la admisibilidad de la evidencia digital en los procesos judiciales. Una legislación más clara y detallada proporcionaría un marco sólido que garantizaría la validez de las pruebas digitales y facilitaría el trabajo de los investigadores.

A pesar de estos desafíos, existen también oportunidades significativas para mejorar la eficacia de las investigaciones de delitos informáticos en Ecuador. Una de las principales oportunidades es el desarrollo de capacidades

forenses en las instituciones encargadas de la investigación criminal. Esto incluye la capacitación del personal, la adquisición de herramientas forenses y la implementación de procedimientos adecuados de adquisición, preservación y análisis de evidencia digital. Invertir en estas áreas fortalecerá la capacidad de respuesta ante delitos cibernéticos. La necesidad de formar profesionales calificados para combatir estos delitos se ha vuelto imperante, ya que las tasas de criminalidad en el ciberespacio experimentan un alarmante crecimiento día a día (Merve, Ibrahim & Huseyin, 2016).

Otra oportunidad importante es la modernización de la legislación ecuatoriana para incluir disposiciones específicas sobre la investigación de delitos informáticos. Establecer un marco legal claro y sólido para la admisibilidad de la evidencia digital y el desarrollo de investigaciones forenses efectivas permitirá a los investigadores actuar con mayor certeza y eficiencia. Además, una legislación actualizada contribuirá a la armonización de las normas locales con los estándares internacionales, facilitando la cooperación transfronteriza en casos que involucren múltiples jurisdicciones.

En la actualidad ya se discute sobre la necesidad de que los investigadores desarrollen sus propias herramientas en el ámbito forense, con soluciones hechas a medida para problemas específicos. Estos desarrollos resaltan la necesidad de herramientas adaptables y personalizables que puedan ser utilizadas en diversas situaciones investigativas. La capacidad de los investigadores para personalizar sus herramientas es crucial en un campo donde cada caso puede presentar desafíos únicos.

En el complejo mundo de la investigación de delitos informáticos, la naturaleza del dispositivo involucrado, la actividad sospechosa detectada y el software instalado en el mismo determinan las técnicas y métodos que se emplearán para desentrañar la verdad. Los especialistas forenses, cual avezados detectives digitales, deben poseer la capacidad de recuperar información crucial de una amplia gama de dispositivos, incluyendo teléfonos celulares, computadoras, tabletas, unidades de almacenamiento externo y sistemas GPS. La selección adecuada de métodos, herramientas y técnicas forenses depende en gran medida de una comprensión profunda de las características y requerimientos específicos de cada investigación (Vincze, 2016).

El dinámico mundo de la tecnología no solo transforma nuestra realidad, sino que también impacta de manera directa en los estándares y las prácticas forenses. Las constantes mejoras y cambios en las herramientas y técnicas forenses conllevan, sin duda, inversiones considerables, las cuales no siempre se recuperan de manera inmediata. Sin embargo, estas inversiones son cruciales para mantenerse a la vanguardia de las innovaciones tecnológicas y garantizar la eficacia en la lucha contra el cibercrimen.

Referencias bibliográficas

Asamblea Nacional, (10 de febrero de 2014). Código Integral Penal. Registro Oficial Suplemento 180. Quito, Quito, Ecuador.

Asociación Latinoamericana de Investigación en Criminalística y Ciencias Forenses: https://www.aicef.info/ Esta organización promueve la investigación y el desarrollo en el campo de la criminalística y las ciencias forenses en América Latina.

Aparicio, V(2021). Delitos informáticos en Ecuador según el COIP: un análisis documental. Recuperado de: https://orcid.org/0000-0002-1417-2036.

Corte Suprema de Justicia de Ecuador: https://www.cortenacional.gob.ec/ Este sitio web contiene información sobre el sistema legal ecuatoriano, incluyendo las leyes relacionadas con los delitos informáticos.

Espinoza, M. (2019). Informática forense: una revisión sistemática de la literatura. Rehuso, 4(2), 126-145. Recuperado de: https://doi.org/10.33936/rehuso.v4i2.1641

Informática forense: una revisión sistemática de la literatura (http://scielo.senescyt.gob.ec/) por Caviglione, Wendzel

y Mazurczyk (2017). Este artículo proporciona una descripción general de las técnicas y herramientas forenses utilizadas en la investigación de delitos informáticos, y analiza su perspectiva legal en Ecuador.

Merve, O., İbrahim, K., & Hüseyin, Ç. (2016). General Evaluation and Requirement of Computer Forensics Education. Bilişim Teknolojileri Dergisi, Cilt, 9(2), 137-146. doi: 10.17671/btd.31631

Ramírez, R. (06 de 25 de 2017). *policia.gob.ec.* Obtenido de policia.gob.ec: https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Ramos-Torres C.A., Vieira, D. F., & Jacobovski, R. (2021). Estrutura institucional na avaliação e monitoramento de políticas públicas: uma análise nos países do MERCOSUL. Revista Brasileira de Administração Científica, 12(2), 232–245. https://doi.org/10.6008/cbpc2179-684x.2021.002.0019

Taborda, K. Branco, J., Cardoso, J., El uso de la informática en la pericia criminal y sus herramientas. *Revista Espacios*. Vol. 38, Año 2017. Número 51 Pág. 25 Recuperado de: ttp://www.revistaespacios.com/a17v38n51/a17v38n51p25.pdf

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

Zambrano, K. I. D., & Ordoñez, L. M. M. (2016). Delito Informático. Procedimiento Penal en Ecuador. *Dominio de las ciencias*, *2*(2), 204-215.