El procedimiento forense, una metodología empleada en la investigación de fraudes financieros y su aplicabilidad

The forensic procedure, a methodology used in the investigation of financial fraud and its applicability

Camilo Augusto Cardona-Patiño [1, 2*]
[1] Fundación Universitaria del Área Andina, [2] UNITEC
[*]Correo para correspondencia: cacardonap@gmail.com

RESUMEN

A través de este trabajo se plantea al objetivo de analizar diferentes metodologías de investigación digital forense y su potencial aplicabilidad en la investigación de fraudes financieros, que serán contratados con los procesos de auditoría contable y el marco legal colombiano, para lo cual, se realiza una revisión documental de modelos forenses que han sido previamente validados e implementados por instituciones educativas o entidades gubernamentales. Estos permitirán identificar las metodologías frecuentemente utilizadas y aceptadas en los procesos de investigación digital, que además sean compatibles con las necesidades regulatorias en Colombia. Para lograrlo, se comparan las propuestas de investigadores Carrier y Spafford para el marco de investigación forense digital basado en eventos, el modelo de Rodney McKemmish y el modelo forense digital abstracto propuesto por Reith, Carr y Gunsch, ya que plantean las tendencias actuales en materia de investigación forense y ciberseguridad. Dentro de las principales conclusiones, se tiene la identificación del modelo ajustado al marco legal colombiano que permite el desarrollo de procesos más transparentes gracias una elevada trazabilidad en cada una de sus etapas.

Palabras clave: informática forense, fraudes financieros, evidencias digitales, procedimiento forense.

ABSTRACT

Through this work, the objective is to analyze different digital forensic investigation methodologies and their potential applicability in the investigation of financial fraud, which will be contracted with the accounting audit processes and the Colombian legal framework, for which, a documentary review of forensic models that have been previously validated and implemented by educational institutions or government entities. These will make it possible to identify the frequently used and accepted methodologies in digital research processes, which are also compatible with the regulatory needs in Colombia. To achieve this, the proposals of researchers Carrier and Spafford for the event-based digital forensic investigation framework, the Rodney McKemmish model and the abstract digital forensic model proposed by Reith, Carr and Gunsch are compared, since they present current trends in the matter forensic investigation and cybersecurity. Among the main conclusions, there is the identification of the model adjusted to the Colombian legal framework that allows the development of more transparent processes thanks to a high traceability in each of its stages.

Keywords: computer forensics, financial fraud, digital evidence, forensic procedure.

Recepción, 09 de diciembre 2022; Aceptado, 29 de diciembre 2022; Publicado, 10 de enero 2023

INTRODUCCIÓN

Durante las últimas décadas, se han venido migrando al campo digital, aspectos que en otras épocas podrían haber sido inverosímiles, por ejemplo, la educación, la compra de alimentos, las transacciones financieras, sin mencionar negocios que no existían como las redes sociales, las aplicaciones para acceder a servicios, de transporte y de hospedaje. Pero a medida que aumenta la dependencia de los sistemas, los usuarios también están más expuestos, pues mayores son los datos que deben estar dispuestos a entregar de forma que sea posible su plena identificación.

Desde su origen en los años 80's, la seguridad informática ha venido evolucionando a la par con los cambios de contexto relacionados con el acceso y los servicios en la Web, y ha sido su principal preocupación, la de brindar canales, técnicas, mecanismos e infraestructuras protegidas para que los usuarios puedan acceder a múltiples plataformas. Así, la seguridad informática es una preocupación y una necesidad de escala global, en la edición número 16, del Informe de Riesgos Globales (2021) del Foro Económico Mundial, que incluye la opinión de más de 700 líderes y expertos de todas partes del planeta, Hall concluyó que el 76.1%, consideran que los ciberataques dirigidos a sistemas financieros aumentarán en 2020, infortunada e inevitablemente muchos de esos ciberataques, resultan en la infiltración de las redes centrales o sistemas empresariales de una compañía, requiriendo procesos de investigación forense encaminados a cuantificar las pérdidas, e identificar a los responsables y las técnicas empleadas por estos.

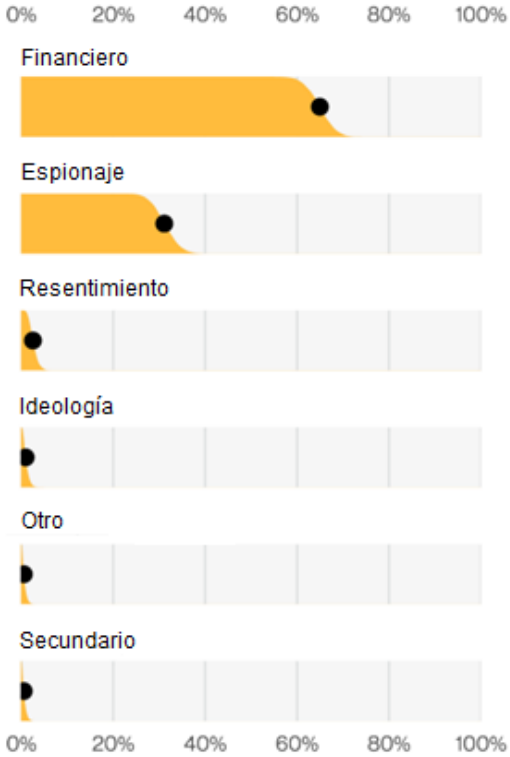
Y es que coherentemente con la masificación y el acceso a internet, también las pérdidas asociadas a ciberdelitos van aumentado año tras año.

Para Gorham (2022), el FBI, en su informe anual de delitos en Internet, revela que las pérdidas fueron de 1.4, 2.7 y 3.5 billones en los años de 2018, 2018 y 2020 respectivamente, encendiendo las alarmas y demandando soluciones en materia de prevención e investigación de estos sucesos. Atendiendo a esta necesidad, este trabajo plantea al objetivo de analizar las metodologías de investigación digital forense con mayor aceptación e identificar posible aplicabilidad en la investigación de fraudes financieros.

De acuerdo con la multinacional de banda ancha y telecomunicaciones Verizon, en su informe sobre violaciones de datos, publicado en 2022, se puede evidenciar que, los motivos que persiguen los ciberdelincuentes, al vulnerar la seguridad informática de una infraestructura empresarial, son predominantemente de naturaleza financiera, (figura 1).

En respuesta a este panorama, las organizaciones demandan de manera urgente, la prestación de servicios de informática forense, para analizar los equipos y redes de datos, permitiendo la recolección, preservación y análisis de evidencias, que permitan soportar y presentar procesos penales o civiles ante los estrados judiciales; y es que a nivel práctico, la identificación y el levantamiento de las evidencias resulta por lo general en una tarea delicada y difícil de ejecutar, según Riadi, Umar y Firdonsyah, A. (2017) "La evidencia digital es frágil, volátil y vulnerable si no se maneja adecuadamente." (p. 156). Para aumentar el grado de complejidad, todos los procedimientos deben estar alineados con la legislación vigente de cada país o países en donde se cometa el ciberdelito, por consiguiente, una inadecuada manipulación de las evidencias podría hacerles perder su valor probatorio ante la ley. Estos desafíos requieren de soluciones ingeniosas que aborden cuestiones técnicas y metodológicas.

Figura 1
Intereses del atacante



Basado en: Verizon. (2022). 2022 Data breach investigations report. Verizon RISK Team

El informe de Tendencias Cibercrimen Colombia 2019-2020, revela que, en Colombia, las empresas pueden perder entre 300 millones y 5.000 millones de pesos por cada ataque, y esto sólo por ataques BEC (Business Email Compromise) y más preocupante aún, según la CCIT (2012), “El 60% de las pequeñas y medianas empresas, no pueden sostener sus negocios más de seis meses luego de sufrir un ciberataque importante” (p. 31), situación que demanda la generación de propuestas enfocadas a la investigación forense de los delitos cibernéticos.

Mediante este estudio se pretende conocer y analizar las propuestas y desarrollos en materia de metodología de investigación en informática forense, examinando sus componentes y etapas clave, para identificar cuáles son las técnicas más adecuadas en procesos de indagación de delitos relacionados con fraudes financieros.

DISCUSIÓN

Los procesos de investigación forense suelen atravesar una serie de etapas, que permiten la formulación, demostración o descarte de hipótesis sobre el delito ocurrido, por ejemplo, si se tiene la sospecha que algún empleado accede de manera irregular a la información contable de una empresa, el equipo de investigación forense debe identificar las evidencias que le permitan respaldar esta conjetura, por lo general los discos duros de los equipos comprometidos en el delito.

Es crítico para la investigación, asegurar físicamente las evidencias, además del uso de mecanismos lógicos como la creación de imágenes o copias bit a bit de los dispositivos de almacenamiento, de forma que los investigadores forenses digitales tengan la oportunidad y

la tranquilidad de examinar la información en profundidad, teniendo la certeza que no habrá pérdida de información, y eventualmente recuperar ficheros ocultos, eliminados, encriptados o protegidos por algún otro mecanismo, convirtiéndose en evidencias digitales que posteriormente podrán ser presentadas como elementos probatorios del cometimiento del delito informático frente a un tribunal.

En el campo de saber sobre la informática forense, existen muchos modelos metodológicos propuestos. Para el desarrollo de la presente investigación se analizarán cinco modelos reconocidos internacionalmente, como posibles metodologías que se pueden aplicar con éxito en la búsqueda de soluciones a problemas relacionados con la investigación de fraudes financieros.

Estos modelos fueron seleccionados con base en su variedad ya que provienen tanto de instituciones educativas, como de entidades gubernamentales, también con base en sus características, tal como se muestra en la tabla 1.

Tabla 1
Modelos y características

	Características					
Modelo	Identificar las evidencias	Respaldar conjeturas	Asegurar físicamente las evidencias	Uso de mecanismos lógicos	Evitar pérdida de información	Total cumplidos
Marco de investigación forense digital basado en eventos	X	X	X	X		4
Modelo de Lee	X		X		X	3
Modelo forense digital abstracto	X	X	X	X	X	5
Modelo de Rodney McKemmish	X		X	X	X	4
Modelo de Venansius Baryamureeba y Florence Tushabe		X		X		2

Nota: Semprini, G. (2016). Lineamientos para la creación de laboratorios informáticos forenses. In XVI Simposio Argentino de Informática y Derecho (SID 2016)-JAIIO 45 (Tres de Febrero, 2016)

Por tanto, con base a los resultados obtenidos en la tabla 1, se seleccionan los tres moldeos con mayor cantidad de características cumplidas para continuar con su análisis y afinidad con el marco legal colombiano.

- Marco de investigación forense digital basado en eventos: Propuesto por Carrier y Spafford, se trata de un mecanismo que establece una separación del entorno del delito en dos componentes de gran importancia y claramente diferenciados, la escena física del crimen y la escena digital del crimen (Haldar, 2020).
- Modelo de Rodney McKemmish: Lleva el nombre de su creador, profesional forense y cibernético. Fue desarrollado en Australia, como una solución a la necesidad de

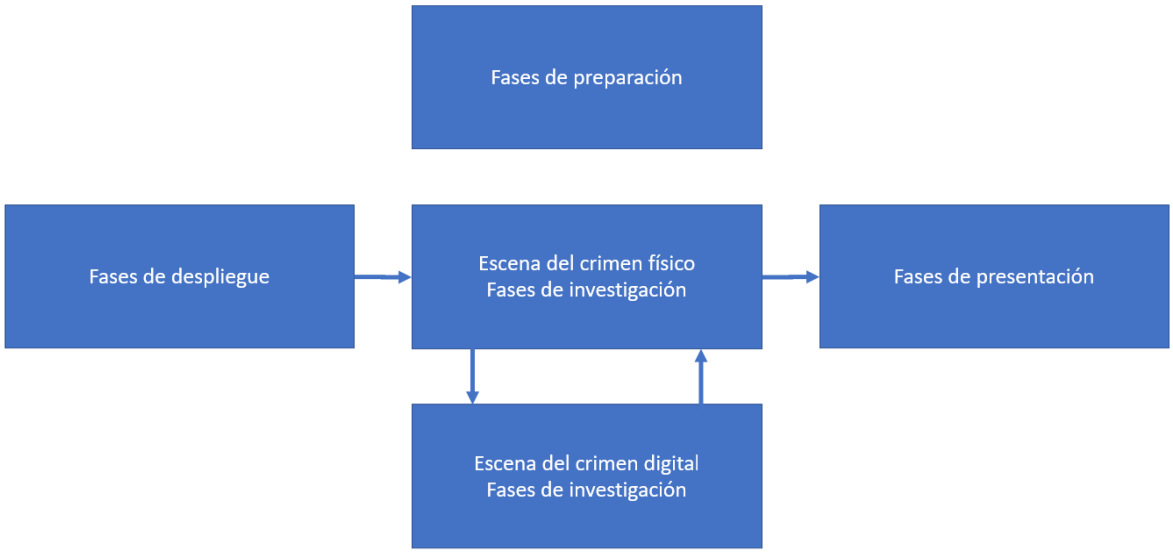
profundizar en diferentes capas binarias, que permitan la reconstrucción de acciones y eventos pasados (Lin, Lin, y Lagerstrom-Fife, 2018).

- Modelo forense digital abstracto: desarrollado en colaboración por Reith, Carr y Gunsch, luego de estudiar varios modelos, con el cual esperaban recopilar las estrategias clásicas de recolección física de evidencias empleadas por las fuerzas de la ley y combinarlas con las prácticas empleadas por comunidades académicas y profesionales (Abbas y Abdulmajeed, 2021).

Para Carrier y Spafford, en su marco de investigación forense digital basado en eventos, el estándar a seguir en el procedimiento forense debe iniciarse desde un conjunto de actividades de preparación previa al incidente, de forma que los recursos técnicos y humanos estén familiarizados con las técnicas para identificar y resguardar adecuadamente las evidencias digitales. En la Figura 2 se puede apreciar el esquema sugerido (Haldar, 2020).

Figura 2

Representación gráfica de las principales categorías de fases del marco



Basado en: Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. Digital Investigation

- Fases de preparación: Capacitar a las personas y disponer las herramientas necesarias para la investigación.
- Fases de implementación: detección y notificación del incidente, que desencadena la acción por parte del grupo de investigación forense.
- Fases de la investigación de la escena física del crimen: investigación de los objetos físicos en la escena del crimen.
- Fases de investigación de la escena del crimen digital: Se lleva a cabo una investigación para cada dispositivo digital.
- Fase de presentación: se presentan los resultados ante un tribunal de justicia.

El marco de investigación forense digital basado en eventos ha sido abordado en contexto educativo con proyección práctica por Areniz (2016), quien ha planteado en su trabajo, la adquisición y análisis de evidencia digital “On Line”, arrojando resultados favorables en entornos corporativos, al realizar un análisis de los sistemas de información financieros. Es importante enfatizar que uno de los ecosistemas preferidos por las empresas en la actualidad es justamente el de mantener una gran cantidad de información desplegada y disponible para los agentes con los que tiene algún tipo de relación: clientes, empleados,

proveedores, entidades gubernamentales, etc., incluyendo aspectos financieros, puesto que suponen agilidad al momento de realizar transacciones e intercambio de información. Esta alta interactividad, claramente expone a las empresas a sufrir diferentes tipos de ataques, que eventualmente dejarán algún tipo de rastros para el investigador forense.

Por otra parte, el modelo de Rodney McKemmish ha sido ampliamente utilizado y probado por el gobierno australiano en procesos de investigación forense. Está conformado por 4 etapas que incluyen: identificación, preservación, análisis y presentación.

Resulta muy llamativo por su simplicidad, ver figura 3. La idea base del modelo es permitir a los investigadores forenses reconstruir la cadena de eventos que se han desarrollarlo en un computador sospechoso de delito informático y poder vincularlos con un usuario.

Figura 3
Modelo Rodney McKemmish

Basado en: Lin, X., Lin, X., & Lagerstrom-Fife. (2018). Introductory Computer Forensics. Springer International Publishing

Para fortalecer su modelo, McKemmish incluye 4 criterios enfocados en brindar admisibilidad a las evidencias en un eventual proceso judicial:

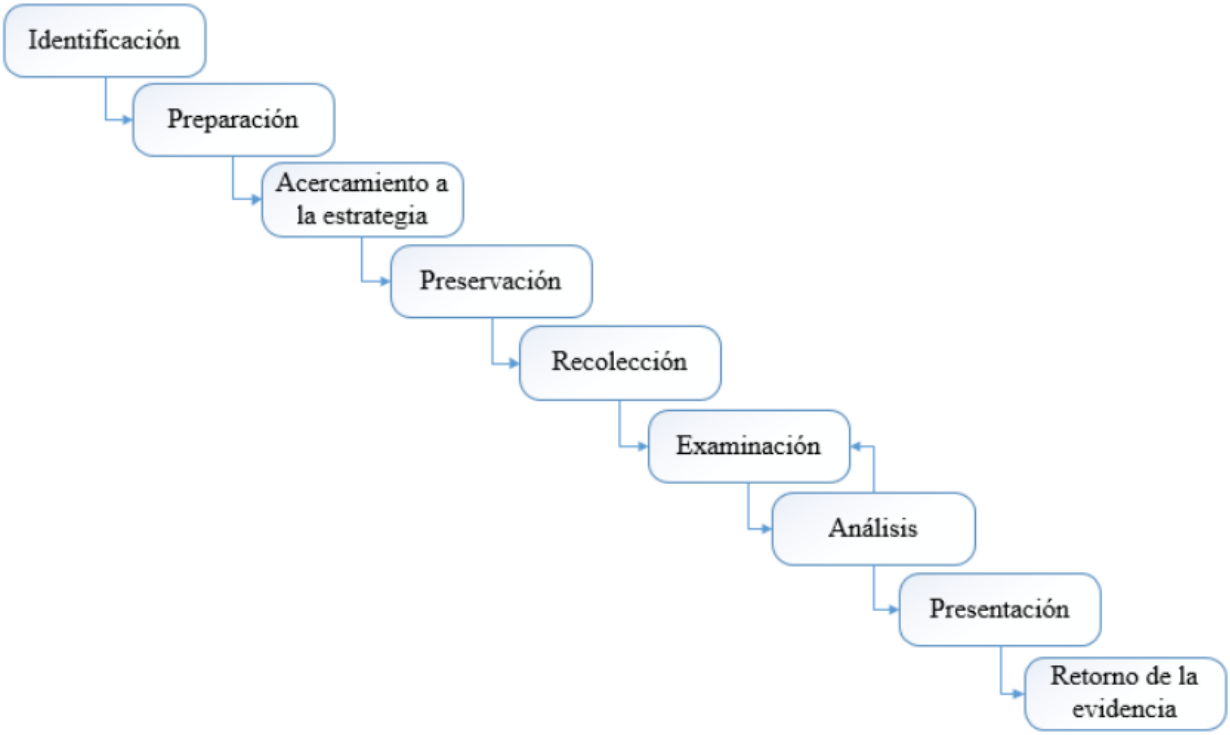
- Meaning: Tener cuidado con el diseño de los procesos digitales de levantamiento de evidencias para que no modifiquen los datos.
- Error: Tener cuidado con el diseño de los procesos digitales de levantamiento de evidencias para evitar errores frecuentes.
- Transparency: Verificar las evidencias, las copias y la cadena de custodia, incluyendo cualquier error, inconsistencia o problema con los equipos o los procesos forenses.
- Experience: procurar asignar investigadores con experiencia en materia del levantamiento de evidencias digitales.

De acuerdo con Hooper, et al. (2013) el modelo Rodney McKemmish ha requerido el establecimiento de acuerdos entre múltiples jurisdicciones estatales en Australia para adelantar investigaciones de informática forense sobre casos relacionados al cibercrimen como acceso abusivo de equipos en la nube y fraudes financieros. La cooperación es coordinada por la Comisión Australiana del Crimen.

El modelo forense digital abstracto formulado por Reith, Carr y Gunsch, mostrado en la Figura 4, propone como base, la utilización de las técnicas tradicionales para el levantamiento de evidencias forenses físicas, ajustándolas para el entorno informático a través de nueve componentes: identificación, preparación, acercamiento a la estrategia, preservación, recolección, examinación, análisis, presentación y retorno de la evidencia.

Al agregar componentes de preparación y estrategia, el modelo demanda una planificación de infraestructura, así como una preparación para la operación, que consiste en identificar el incidente con base en los indicios y el tipo de delito, permitiendo maximizar la recolección de evidencias digitales y su calidad.

Figura 4
Diagrama modelo forense digital abstracto



Basado en: Kebande, V. R., & Venter, H. S. (2019). A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. Wiley Interdisciplinary Reviews: Forensic Science, 1(6), e1350

En el ámbito empresarial, ha sido implementado con éxito en industrias dedicadas al análisis de datos, sistemas de redes de información y servidores empresariales, dedicados a procesos de recolección, análisis y alertas automatizadas como manejo de personal, redes sociales y transacciones bancarias.

De los modelos antes mencionados, podemos ver claramente algunos hechos interesantes:

- Existen algunas similitudes entre ellos a pesar de que provienen de diferentes investigadores, instituciones y gobiernos de todo el mundo, lo que permite evidenciar alineación entre práctica y teoría.
- Cada modelo tiene énfasis en la secuencialidad de las etapas que permite la construcción de un caso de investigación criminal.
- Aunque existen algunas diferencias entre los modelos, uno de los objetivos principales es el de extraer la evidencia digital, que eventualmente servirá como material probatoria ante un tribunal.

Auditoría contable

En los entornos empresariales generalmente se implementan sistemas informáticos para facilitar la gestión eficiente de grandes volúmenes de datos, con estructuras robustas enfocadas en brindar altos estándares de disponibilidad, como bases de datos distribuidas y sistemas de alta confiabilidad. Es por ello, que cuando se detecta un hecho sospechoso de fraude financiero, por su especialidad en materia contable, el investigador forense debe seleccionar adecuadamente la identificación, preparación y preservación de las evidencias, normalmente con el apoyo de contadores públicos.

Además de las capacidades técnicas para la manipulación de los datos digitales, es necesario contar con el conocimiento, asesoría o acompañamiento en materia contable para maximizar la cantidad de evidencias relacionadas con delitos financieros identificados. Por ejemplo, para el investigador forense, es relativamente fácil reconocer las situaciones de riesgo financiero como acceso privilegiado y control inadecuado a los sistemas contables. Sin embargo, el perfil contable puede reconocer una evidencia en un flujo de efectivo negativo o reiterada conversión de activos líquidos en efectivo.

Marco legal colombiano

A continuación, se describe la normatividad del sistema nacional colombiano, que reglamenta la informática forense en el desarrollo de investigaciones sobre delitos informáticos.

- Ley 594 de 2000: Ley general de archivos.
- Ley 599 de 2000: Código Penal, que tipifica los delitos informáticos.
- Ley 962 de 2005: Trámites y procedimientos administrativos de los organismos y entidades del Estado.
- Acuerdo nº PSAA06-3334 de 2006: Utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia.
- Ley 1266 de 2008: Habeas data y de regulación del manejo de la información contenida en bases de datos.
- Ley 1273 de 2009: Piedra angular del análisis forense, “de la protección de la información y los datos”.
- Ley Estatuaria 1581 de 2012: Establece categorías especiales para lo datos digitales.
- Resolución 670 de 2017: Manual de políticas y procedimientos para la protección de datos personales.
- Ley 1918 de 2018: Se aprueba el “Convenio sobre la Ciberdelincuencia”, aprobado en 2001 en Budapest.

Para que la evidencias tengan admisibilidad ante un tribunal, todos los procedimientos relacionados con la identificación, recolección, conservación, y análisis, así como la cadena de custodia, deben acogerse a las disposiciones legales, en caso contrario, cualquier duda o inconsistencia con el tratamiento de las pruebas podría invalidarlas. En Colombia se han tenido avances en materia legislativa sobre el reconocimiento y tipificación de delitos informáticos, sin embargo, aún existen carencias reglamentarias en la práctica que establezcan procedimientos generalizados para la identificación y recolección de evidencias digitales, especialmente las relacionadas con delitos financieros, por lo que se hace evidente la necesidad de proponer una metodología que ayude al investigador digital forense en los procesos de investigación, sin que las evidencias corran el riesgo de ser desestimadas en un proceso legal.

CONCLUSIONES

Con base en lo observado en cada una de las metodologías y su aplicabilidad podemos concluir que el modelo forense digital abstracto, podría ser el más adecuado para el contexto colombiano puesto que proporciona características de detalle a nivel de identificación, estrategia, preservación, y análisis especialmente, favoreciendo la trazabilidad de todo el proceso de investigación digital forense, cualidades fundamentales para la presentación y validación de evidencias dentro del marco legal colombiano.

Se han propuesto una serie de metodologías para orientar ejercicios de investigación forense, de manera que los procesos sean más transparentes y con una elevada trazabilidad. Esto facilita su alineación a los requerimientos legales. Sin embargo, a pesar de que existe una sólida reglamentación en el campo jurídico, se puede apreciar que aún existen vacíos para prácticas específicas como los fraudes financieros, que los ciberdelincuentes aprovechan para atacar plataformas tecnológicas y lograr impunidad. Sin una tipificación del ciberdelito, tanto los investigadores forenses, como los abogados se ven incapaces de judicializar a los responsables aun logrando recabar las evidencias digitales.

REFERENCIAS BIBLIOGRÁFICAS

Abbas, T. M. J., & Abdulmajeed, A. S. (2021). Identifying Digital Forensic Frameworks Based on Processes Models. Iraqi Journal of Science, 249-258.

Abedi, M., & Sedaghat, S. (2018). Crawler and Spiderin usage in Cyber-Physical Systems Forensics. OIC-CERT Journal of Cyber Security, 1(1), 53-61. Available: https://www.oic-cert.org/en/journal/pdf/1/1/117.pdf

Aksentijević, Saša, Edvard Tijan, and Alen Jugović. "Financial impact of forensic proceedings in ICT." 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2017.

Areniz Arevalo, G. A. (2016). Definición De Una Metodología Práctica Para La Adquisición Y Análisis De Evidencia Digital En El Contexto De Un Análisis Forense Digital On Line (Doctoral dissertation). Available: http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/1171/1/28780.pdf

Caicedo Cárdenas, S. P., & Higuera, A. (2019). Estrategias de prevención y detección del fraude financiero en las empresas de la Ciudadela Parque Industrial de Duitama. Available: https://repositorio.uptc.edu.co/handle/001/3111

Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. Digital Investigation. Available: https://digital-evidence.org/papers/dfrws_event.pdf

CCIT (2020). Tendencias Cibercrimen Colombia 2019-2020, Available: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. arXiv preprint arXiv:1708.01730. Available: https://arxiv.org/abs/1708.01730

Fernández, E. E. C., & Herrera, R. D. J. G. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. NOVUM, 1(10), 61-80. Available: https://revistas.unal.edu.co/index.php/novum/article/view/84210

Gamboa Pena, D. A. (2018). Procesos de informática forense y marco legal colombiano (Bachelor's thesis, Universidad Piloto de Colombia). Available: http://repository.unipiloto.edu.co/handle/20.500.12277/2736

Gorham, M. (2022). 2021 INTERNET CRIME REPORT. Federal Bureau of Investigation, Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Hall, M. (2021). Burning Planet: Climate Fires and Political Flame Wars Rage. World Economic Forum, Available: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Graeme, H. (2020). Part 1: -quality assurance mechanisms for digital forensic investigations: Introducing the Verification of Digital Evidence (VODE) framework. Forensic Science International: Reports, 2, 100038. Available: https://www.sciencedirect.com/science/article/pii/S2665910719300386

Haldar, N. A. H. (2020). Advances in digital forensics frameworks and tools. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications, 165.

Hooper, Christopher, Ben Martini, and Kim-Kwang Raymond Choo. "Cloud computing and its implications for cybercrime investigations in Australia." Computer Law & Security Review 29.2 (2013): 152-163. Available: https://www-sciencedirect-com.proxy.bidig.areandina.edu.co/science/article/pii/S0267364913000241

Jaya Cáceres, K. A. (2017). Desarrollo de una guía de procedimientos en base al estudio de modelos de análisis forense de datos, aplicada en análisis a dispositivos móviles (Bachelor's thesis, PUCE). Available: http://repositorio.puce.edu.ec/handle/22000/13484

Kebande, V. R., & Venter, H. S. (2019). A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. Wiley Interdisciplinary Reviews: Forensic Science, 1(6), e1350. Available: https://wires.onlinelibrary.wiley.com/doi/epdf/10.1002/wfs2.1350

Khanafseh, M., Qatawneh, M., & Almobaideen, W. (2019). A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics. Int. J. Adv. Comput. Sci. Appl, 10(8), 610-629. Available: https://pdfs.semanticscholar.org/9d68/19e6799204f28a634dc8195d31c139dcee3e.pdf

Lin, X., Lin, X., & Lagerstrom-Fife. (2018). Introductory Computer Forensics. Springer International Publishing. Available: https://link.springer.com/book/10.1007%2F978-3-030-00581-8

López Reina, L. D., & Rincón Leal, J. C. (2019). Mecanismos de recolección de pruebas forenses en los encargos de aseguramiento contable aplicables al sector cooperativo de ahorro y crédito. Available: https://repository.ucc.edu.co/handle/20.500.12494/13694

Meneses Obando, O. A. (2019). Informática forense desde el recurso humano y tecnológico, en las instituciones judiciales que cuentan con el servicio especializado de peritaje informático en Colombia. Available: https://bdigital.uexternado.edu.co/handle/001/1696

Mir, Sara Sarwar, Umar Shoaib, and Muhammad Shahzad Sarfraz. "Analysis of digital forensic investigation models." International Journal of Computer Science and Information Security 14.11 (2016): 292.

Mora Pérez, D. A., & Ramírez Bautista, L. M. (2019). Delitos informáticos contables en Villavicencio. Available: https://repository.ucc.edu.co/handle/20.500.12494/12018

Quishpe Cumba, D. P., & Toinga Villafuerte, M. L. (2018). Análisis Forense Digital a la Placa Raspberry Pi (Bachelor's thesis, Quito, 2018.). Available: http://bibdigital.epn.edu.ec/handle/15000/19483

Riadi, I., Umar, R., & Firdonsyah, A. (2017). Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. International Journal of Computer Science and Information Security (IJCSIS), 15(5), 155-160. Available: https://www.researchgate.net/profile/Imam_Riadi/publication/317620078_Identification_Of_Digital_Evidence_On_Android's_Blackberry_Messenger_Using_NIST_Mobile_Forensic_Method/links/5943f0cd0f7e9b6910ee2624/Identification-Of-Digital-Evidence-On-Androids-Blackberry-Messenger-Using-NIST-Mobile-Forensic-Method.pdf

Sanghamitra, Mridul Sankar Barik, and Indrajit Banerjee. "A Digital Forensic Process Model for Cloud Computing." 2020 IEEE Calcutta Conference (CALCON). IEEE, 2020.

Souto, L., Moreira, H., Tavares, F., Pombo, L., & Pinho, R. (2016). Euro4science: Using Forensic Science As An Educational Strategy. Brief Contents, 60.

Verizon. (2022). 2022 Data breach investigations report. Verizon RISK Team, Available: https://www.verizon.com/business/resources/T6ec/reports/dbir/2022-data-breach-investigations-report-dbir.pdf