DERECHO Y CAMBIO SOCIAL
FUNDADA EL AÑO 2000

PROPOSAL OF A CONCEPTUAL FRAMEWORK TO REPRESENT THE HISTORICAL RECORD OF EVENTS IN THE CHAIN OF CUSTODY: A DOCTORAL THESIS REVIEW

PROPOSTA DE UM FRAMEWORK CONCEITUAL PARA REPRESENTAR O REGISTRO HISTÓRICO DE EVENTOS NA CADEIA DE CUSTÓDIA: UMA REVISÃO DE TESE DOUTORAL

PROPUESTA DE UN MARCO CONCEPTUAL PARA REPRESENTAR EL REGISTRO HISTÓRICO DE LOS ACONTECIMIENTOS EN LA CADENA DE CUSTODIA: UNA REVISIÓN DE TESIS DOCTORAL

Fabio Vivan Grigollo[1], Roberto Fabiano Fernandes[2]

DOI: 10.54899/dcs.v22i80.2660
Recibido: 10/02/2025 | Aceptado: 20/02/2025 | Publicación en línea: 07/05/2025.

ABSTRACT

The increasing complexity of digital investigations and the demand for reliable evidence pose challenges to digital forensics, especially with regard to the chain of custody and the security of collected evidence. The absence of a framework that integrates security, privacy, and data protection, combined with the risk of contamination of evidence, compromises its admissibility in legal proceedings. Given this scenario, this study proposes a conceptual framework for the historical record of evidence, covering the stages of collection, acquisition, examination, analysis, and ongoing custody. The methodology adopted combines a literature review, analysis of existing frameworks, and interviews with experts, allowing the validation and improvement of the proposed framework. The conceptual framework developed aims to strengthen the integrity and reliability of digital evidence, mitigating risks associated with its improper handling. In addition, it seeks to ensure that privacy, data protection, and information security are considered in an integrated manner, reducing vulnerabilities and increasing the efficiency in the preservation of digital evidence. The results obtained indicate the feasibility of applying the conceptual framework in real scenarios, contributing significantly to the admissibility of evidence in courts and to the improvement of practices in digital forensics.

Keywords: Computer Forensics. Chain of Custody. Privacy. Data Protection. Information Security.

[1] Doutorando em Research Specialty Projects, Universidad Internacional Iberoamericana, San Juan, Porto Rico. E-mail: fabio.vivan@doctorado.unib.org

[2] Doutor em Engenharia e Gestão do Conhecimento; Universidade Federal de Santa Catarina; Florianópolis, Santa Catarina, Brasil. E-mail: fernandes.roberto@posgrad.ufsc.br

RESUMO

A crescente complexidade das investigações digitais e a demanda por provas confiáveis impõem desafios à forense digital, especialmente no que se refere à cadeia de custódia e à segurança das evidências coletadas. A ausência de uma estrutura que integre segurança, privacidade e proteção de dados, aliada ao risco de contaminação das evidências, compromete sua admissibilidade em processos judiciais. Diante desse cenário, este estudo propõe um *framework* conceitual para o registro histórico de evidências, abrangendo as etapas de coleta, aquisição, exame, análise e custódia contínua. A metodologia adotada combina revisão bibliográfica, análise de estruturas existentes e entrevistas com especialistas, permitindo validar e aprimorar a estrutura proposta. O *framework* conceitual desenvolvido visa fortalecer a integridade e confiabilidade das provas digitais, mitigando riscos associados à sua manipulação inadequada. Além disso, busca garantir que a privacidade, proteção de dados e a segurança da informação sejam contempladas de forma integrada, reduzindo vulnerabilidades e aumentando a eficiência na preservação das evidências digitais. Os resultados obtidos indicam a viabilidade da aplicação do *framework* conceitual em cenários reais, contribuindo significativamente para a admissibilidade das provas em tribunais e para o aprimoramento das práticas na forense digital.

Palavras-chave: Computação Forense. Cadeia de Custódia. Privacidade. Proteção de Dados. Segurança da Informação.

RESUMEN

La creciente complejidad de las investigaciones digitales y la demanda de pruebas fiables plantean desafíos a la investigación forense digital, especialmente en lo que respecta a la cadena de custodia y la seguridad de las pruebas recogidas. La ausencia de una estructura que integre seguridad, privacidad y protección de datos, sumada al riesgo de contaminación de la evidencia, compromete su admisibilidad en procesos judiciales. Ante este escenario, este estudio propone un marco conceptual para el registro histórico de la evidencia, abarcando las etapas de recolección, adquisición, examen, análisis y custodia continua. La metodología adoptada combina revisión bibliográfica, análisis de estructuras existentes y entrevistas a expertos, permitiendo la validación y mejora de la estructura propuesta. El marco conceptual desarrollado busca fortalecer la integridad y confiabilidad de la evidencia digital, mitigando los riesgos asociados a su manejo inadecuado. Además, busca garantizar que la privacidad, la protección de datos y la seguridad de la información se consideren de manera integrada, reduciendo vulnerabilidades y aumentando la eficiencia en la preservación de la evidencia digital. Los resultados obtenidos indican la viabilidad de aplicar el marco conceptual en escenarios reales, contribuyendo significativamente a la admisibilidad de la prueba en los tribunales y a la mejora de las prácticas en informática forense.

Palabras clave: Informática Forense. Cadena de Custodia. Privacidad. Protección de Datos. Seguridad de la Información.

INTRODUCTION

Advances in technology and the digitalization of processes have brought new challenges to computer investigations, requiring more sophisticated approaches to preserving digital evidence. In the forensic context, the reliability of evidence depends on the adoption of rigorous procedures to ensure its integrity, authenticity and admissibility. However, gaps in existing structures can compromise these aspects, especially with regard to security, privacy, data protection and control of evidence contamination.

The chain of custody is one of the fundamental elements to guarantee the reliability of digital evidence, as it documents the path of evidence from its collection to its analysis, storage and eventual return or proper disposal. However, studies indicate that traditional approaches often lack effective mechanisms to protect data and record incidents, such as contamination. The need for a structure that combines traceability, privacy, data protection and information security in a single structure is evident, since the lack of standardization can result in the inadmissibility of digital evidence in court. In this context, this study proposes a conceptual framework for the historical recording of events in the chain of custody, structured to mitigate weaknesses in existing approaches and improve documentation and evidence security procedures. The methodology adopted includes a literature review, a comparative analysis of current structures, and interviews with industry experts to validate the proposed solution. The conceptual framework seeks to integrate security, privacy, and data protection into a modular structure, ensuring that information is stored and processed in a secure and reliable manner. The research results aim to provide a viable framework for the forensic market, strengthening the admissibility of digital evidence in legal proceedings and promoting improvements in investigative practices. The proposal also aims to fill gaps in existing structures by creating a standardized approach to historical records of forensic process events, contributing to the evolution of the sector.

THEORETICAL FRAMEWORK

Computer forensics is an area of digital forensic science that seeks to collect, examine, and analyze digital evidence for investigative and judicial purposes (Ramírez, Gonzales, and Castro, 2019).

The fundamental steps of a forensic process include collection, examination, analysis, and report preparation, as described by Campos, Gomes, and Martins (2016) and reinforced by the research of Ramadhan, Setiawan, and Hariyadi (2022).

According to Voronkova (2011), computer forensics uses investigative methods to identify and collect digital evidence for judicial use.

The analysis of evidence must be conducted with appropriate techniques to extract relevant information and correlate it with the investigation (Campos et al., 2016). The preparation of the final report is highly important to communicate the findings to the legal community in a clear and accessible manner.

The chain of custody is a set of procedures that ensures the traceability and integrity of digital evidence, documenting the entire life cycle of evidence from its collection to analysis and archiving (Carvalho, 2020). This process is essential to prevent contamination, alteration or destruction of evidence.

According to Riaño (2020), the chain of custody is essential to document digital evidence in detail, increasing judicial acceptance.

According to Machado et al. (2021), correctly establishing the chain of custody is important to prevent evidence from being compromised, avoiding questions about its validity in court.

Brezinski and Killalea (2002) emphasize the importance of following recognized standards, such as RFC 3227, to ensure the reliability of evidence.

Tomlinson, Smith and Radosta (2006) point out that automating the chain of custody through management systems can reduce errors and improve evidence traceability. The effectiveness of an investigation using digital evidence involves the collection, protection and proper storage of evidence (Cantore, 2014). ISO/IEC 27037:2013 provides guidelines for the identification, collection, acquisition and preservation of digital evidence, ensuring the reliability of evidence in investigative and judicial processes (ISO, 2013). NIST 800-86, although earlier, complements this approach, providing guidance on the integration of forensic techniques in incident response, in the light of Kent et al., 2006. According to research by Yalçın and Kılıç (2019), it appears that standards such as ISO/IEC 27041 and 27043 offer detailed guidelines for evidence management, while ISO/IEC 27701:2019 establishes specific requirements for privacy and data protection.

These standards are essential to ensure the validity of evidence and mitigate risks associated with improper handling of information. Furthermore, information security is an essential aspect in the preservation of digital evidence. Netto and Silveira (2007) point out that the fundamental principles of security include integrity, confidentiality, and availability of information. ISO/IEC 27001 establishes guidelines for the implementation of information security management systems (Sansigolo, 2015).

With the advancement of privacy legislation and the need to comply with Data Protection Regulations, standards such as ISO/IEC 27701:2019 have become requirements for the secure management of personal information (Anwar and Gill, 2020).

Ferreira et al. (2022) highlight that technological advancement increases challenges related to privacy, especially due to the intensive use of personal data by digital devices.

Riaño (2020) warns that the volume of data processed is subject to risks such as breaches and interceptions, requiring effective procedures in the collection of evidence. Arias (2014) highlights that many countries lack adequate standards on chain of custody. Nandhakumar, Agarwal and Faizal (2012) investigate the use of AFF4 to better manage digital evidence. Beebe and Clark (2004) note that the structures evaluated are not very tangible, based on abstract models. Voronkova (2011) points out difficulties in analyzing mobile evidence, such as the constant changes in smartphone data. Ćosić and Bača (2010) mention the use of RFID in the USA to track evidence, but with privacy issues to be studied. Köhn, Eloff and Olivier (2008) criticize the informality of forensic models, advocating greater formalization. Ferreira, Pinheiro and Marques (2022) warn about the improper collection of personal data by technological devices. The motivation for this study is based on the limitations faced by professionals in the historical recording of chain of custody events, highlighting weaknesses in current approaches, especially regarding integration with security, privacy, data protection and contamination control. Despite advances and the existence of several methodologies, there is still a lack of a unified structure that covers all stages of the forensic process and ensures the traceability of digital evidence, including the recording of related incidents. Thus, the development of a new conceptual and integrated framework capable of filling these gaps in a complete and secure manner is justified.

The proposed conceptual framework seeks to structure an approach that integrates the stages of computer forensics with the principles of security, privacy and data protection, providing a robust solution for the historical recording of evidence.

This novel approach proposes a modular structure, capable of documenting each event in the chain of custody and ensuring the reliability of digital evidence.

The analysis of existing approaches highlights the need for an innovative framework that records events in the chain of custody considering incidents related to security, privacy and data protection.

The purpose of this study seeks to fill these gaps, strengthening the admissibility of digital evidence in legal proceedings.

METHODOLOGY

The research is exploratory in nature and has a qualitative approach, based on theoretical concepts and research techniques. The study investigates weaknesses in the historical record of the chain of custody and digital forensics, structured around a literature review, semi-structured interviews with professionals in the field, data analysis and development of the conceptual framework. The qualitative approach seeks to understand the deficiencies and needs of the current structures of historical record in the chain of custody and digital forensics.

According to Trivinos (1987), the semi-structured interview allows an in-depth analysis of the context and institutional practices, by combining flexibility in data collection with a structured theoretical framework, encouraging interaction between researcher and participant. Malhotra (2019) highlights that qualitative research explores participants' motivations and perceptions through a flexible approach, providing an in-depth understanding of the topic investigated.

Content analysis, conducted with the support of specialized software, allows the categorization and interpretation of the data obtained. The study is not based exclusively on measurable variables, but considers qualitative factors that impact the chain of custody and the preservation of digital evidence, with special attention to evidence recording, data security and privacy, as well as evidence contamination.

The methodological processes begin with the collection of secondary data through a literature review on digital forensics, chain of custody, security, privacy and data protection. Then, primary data collection occurs through semi-structured interviews with two groups: professionals in the area of digital forensics working in national companies and specialists who provide services both in Brazil and abroad. The objective is to understand evidence recording practices, challenges faced and the security of historical records in the chain of custody.

In this approach, the data are categorized and analyzed following the methodology of Bardin (1977), organized in three stages: transcription and segmentation of interviews, categorization of data and interpretation of the information collected. Based on this information, a preliminary conceptual framework is developed, with validation through peer review that considers structural clarity, alignment with research objectives and suitability to market needs.

Table 1

Summary of validations with guests and interviewees

Field validations	*Description*
Activity 1	Review of the semi-structured script with (02) two professionals in the field;
Activity 2	Application of semi-structured script with (02) two national private companies;
Activity 3	Application of a semi-structured script with (02) two national private companies that also provide services outside the country;
Activity 4	Review of the validation script of the previous conceptual framework, with (02) two market professionals and experienced teachers;
Activity 5	Joint validation of the previous conceptual framework, with (04) four professionals in the field.

Source: From the author.

Finally, the consistency of the conceptual framework and its practical applicability are verified, analyzing security, privacy and data protection standards, as well as presenting controls and the possibility of recording correlated incidents. The activities can be seen in Table 1.

The methodological procedures described support a structured and well-founded investigation, resulting in the development of a conceptual framework that can improve historical recording processes in digital forensics.

RESULTS AND DISCUSSIONS

The analysis of the primary data collected in the field was carried out with the support of the Atlas.ti tool, allowing the organization of the responses from the semi-structured interviews into specific categories, where 16 main categories were identified, according to Table 2.

Table 2

Codes

Evidence Contamination Control
Privacy Control
Data Protection Control
Security Control
Custody as a Continuous Step
Documentation/Record of Collection, Acquisition, Examination and Analysis
Chain of Custody Experience
Gaps and Weaknesses that the Framework can Mitigate
Need for a framework
Historical record
Suggested contributions for the development of the new framework
Suggested Privacy Control Improvements
Suggestion for improvements to Data Protection Control
Suggestion for Security Control Improvements
Suggestions for improvements to the Historical Record fields
Chain of Custody Training

Source: From the author.

The data were segmented, quantified and analyzed qualitatively, providing detailed inferences about the companies' practices. This approach allowed us to verify patterns, correlations and weaknesses in the historical record of evidence, serving as a basis for improving the proposed framework. Improvements were suggested, such as standardization of terminology; integration of security, privacy, data protection and contamination control; detailed recording of actions taken on the evidence and implementation of blockchain for immutability of records (proposed for future work). The solutions were based on the results of the interviews and the literature review, demonstrating an alignment between theory and practice. The results of the field research brought relevant contributions to the development of the conceptual framework. The integrated approach of security, privacy, data protection and contamination control proved to be relevant for the reliability of the historical record of evidence, consolidating the importance of this research in the field of computer forensics. The construction of the conceptual framework, from its initial formulation to the final validation, highlighted the interrelations of the theoretical and empirical approaches that underpin it. The preliminary conceptual framework was developed to enhance the advanced historical recording of chain of custody events, overcoming limitations of traditional frameworks.

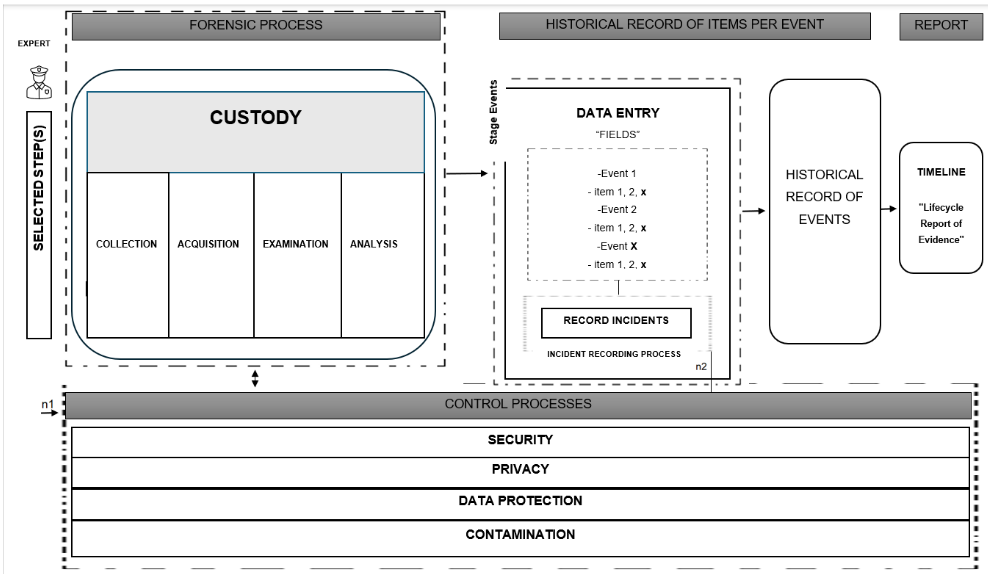
It incorporates additional variables, allowing comprehensive control over security, privacy, data protection and evidence contamination.

The theoretical foundation is based on an extensive literature review and analysis of pre-existing frameworks, covering elements of digital forensics, chain of custody, privacy, data protection and information security.

This conceptual framework was also adjusted based on the needs identified in the field research, ensuring alignment between theory and practice.

Figure 1

Pilot Structure of the Conceptual Framework



Source: From the author.

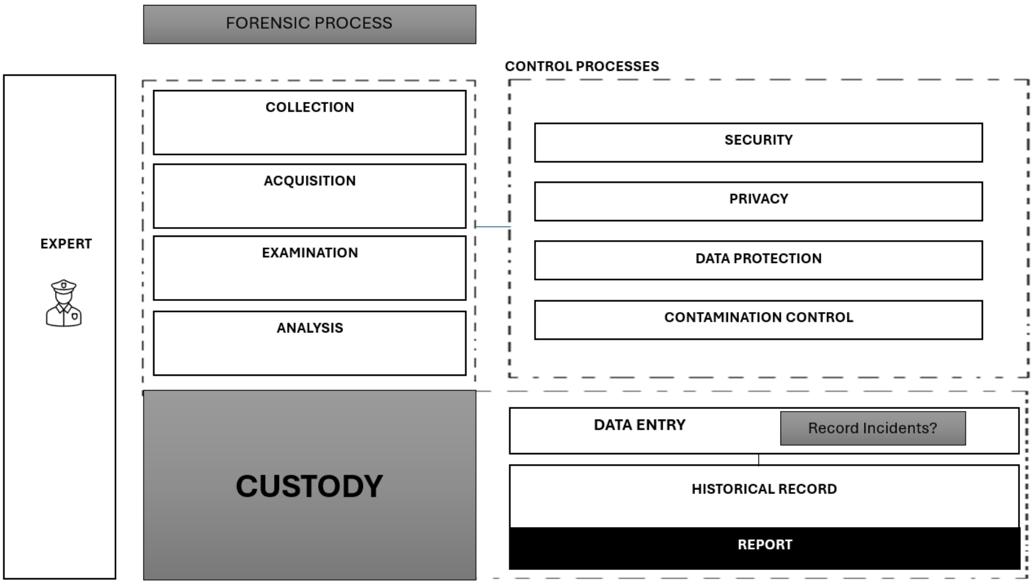
The pilot conceptual framework, shown in Figure 1, structures the flow of forensic evidence, documenting the interactions between the stages of collection, acquisition, examination, analysis and ongoing custody. In addition, it introduces distinct levels of control, with level 1 dealing with preventive control of security, privacy, data protection and contamination. Level 2 deals with recording incidents with the evidence, with regard to security, privacy, data protection and contamination. The structuring of the conceptual framework followed a rigorous flow, considering the identification of theoretical and practical gaps, the creation of an initial structure based on the literature and interviews and validation by experts in the field. This framework enables the tracking and accurate documentation of each event in the chain of custody, ensuring that all actions are auditable and legally defensible.

To validate the conceptual framework, reviews were conducted at some stages, with the pre-testing of the validation script, carried out by two experienced engineers and professors, ensuring the coherence and applicability of the script. The final review was carried out by experts, where four professionals in the area of digital forensics analyzed the conceptual framework for clarity, representativeness of the forensic process and suitability to security and privacy requirements.

The experts confirmed that the conceptual framework was well structured, highlighting the clarity and structural cohesion, that is, the flow of information was considered well connected and easy to understand; the representation of custody, where they validated the continuous custody approach as essential for the integrity of the evidence; the historical record and traceability, where the structure was recognized as adequate to document and guarantee the reliability of the evidence; finally, the security, privacy, data protection and contamination controls were evaluated at levels 1 and 2, where it was recorded that the conceptual framework includes efficient mechanisms to control issues related to security, privacy, data protection and contamination of evidence, as well as to record incidents in these categories, should they occur. The suggestions made by the experts were incorporated, improving the visual layout of the structure and reinforcing the clarity of the terminology. The final conceptual framework integrates an iterative and modular system, as suggested in Figure 2, allowing for continuous reviews and adjustments as new industry needs are identified.

Figure 2

Historical Record of Events in the Chain of Custody.

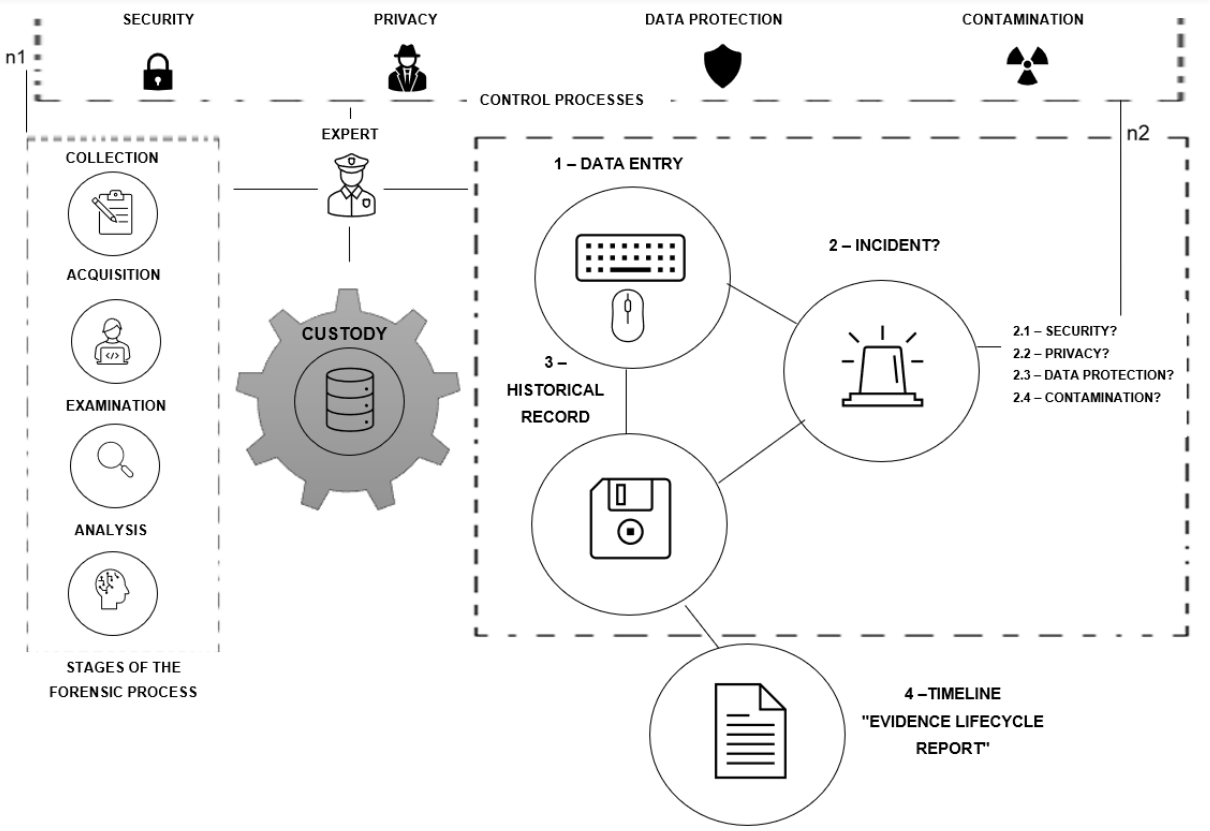


Source: From the author.

After the validation steps, the final version of the conceptual framework was developed, as shown in Figure 3.

Figure 3

Conceptual Framework for the Historical Record of Events in the Chain of Custody.



Source: From the author.

The final framework incorporates detailed event logging using standard and advanced fields, the application of security, privacy, data protection and contamination controls at all stages of the forensic process selected for research, as well as continuous monitoring of the chain of custody, ensuring complete traceability of evidence. In addition, it also incorporates the possibility of recording incidents to strengthen compliance and mitigate legal risks.

The implementation of the proposed conceptual framework allowed the identification of challenges in the digital evidence chain of custody and the construction of a solution to overcome them. During development, it was observed that the lack of standardization in forensic evidence records made traceability difficult and compromised data reliability. To minimize this weakness, standardized fields and uniform terminologies were created and validated, ensuring greater accuracy in documentation.

Another challenge identified was the deficiency in records on evidence contamination, which could compromise its legal validity. To mitigate this risk, the conceptual framework included specific controls for identifying and documenting incidents, preventing questions about the integrity of the evidence. Furthermore, security, privacy and data protection control mechanisms were incorporated, ensuring that these dimensions were also treated in an integrated manner, and not just in isolation, as occurs in some conventional approaches.

The research also revealed that the adoption of emerging technologies can further strengthen the security and traceability of evidence. Suggestions such as the use of blockchain for record immutability and artificial intelligence for access monitoring and anomaly detection were raised as future improvement strategies.

The main benefits observed with the implementation of the conceptual framework include the reduction of the risk of invalidating evidence, ensuring that the stages of the forensic process are rigorously documented. It also supports greater transparency and reliability, allowing effective audits and detailed reviews of evidence. Another benefit concerns the standardization of expert documentation, enabling uniformity in records between different experts and institutions. Finally, it enables scalability and modularity, ensuring compatibility with new technologies and allowing adaptation to future demands without the need for complete restructuring.

The validation process, carried out with experts in the field, confirmed that the proposed structure is suitable for practical application, meeting the criteria of clarity, traceability, reliability and market compliance. Suggestions received during this phase were incorporated into the final structure, ensuring a logical and intuitive flow for the chain of custody.

The results thus show that the conceptual framework fills gaps in the historical record of forensic events, promoting a safer and more robust structure for the documentation of digital evidence.

CONCLUSION

The research achieved its main objective by developing and validating a structured conceptual framework for the historical recording of events in the chain of custody of digital evidence, ensuring the traceability, security and integrity of the evidence. The proposed solution improves forensic documentation by introducing standardized processes, contamination controls and integrated security, privacy and data protection mechanisms.

Among the main lessons learned, the importance of active listening and multidisciplinary collaboration for the refinement of the framework stands out. The contributions of experts were essential to ensure that the conceptual framework was aligned with the needs of the sector, reinforcing the need for continuous adaptation in the face of the challenges encountered.

However, some limitations need to be considered. The implementation of the conceptual framework will depend on the adherence of forensic institutions, and may face resistance from organizations accustomed to traditional practices. In addition, its adoption may represent additional costs for companies and agencies with limited resources, especially due to the need for training and adaptation of internal processes.

Despite these restrictions, the conceptual framework has significant implications for digital forensic practice and chain of custody regulation. The research offers a consolidated technical framework aligned with current regulations, also contributing to strengthening legal certainty in the production of digital evidence and reducing questions about the authenticity of the evidence.

In this way, the general and specific objectives of the research were fully achieved, consolidating a framework applicable both in theory and in practice.

The proposed conceptual framework represents a significant advance in the documentation and preservation of digital evidence, offering a solid basis for future research and regulatory improvements in the area of digital forensics.

REFERENCES

Anwar, M. J., & Gill, A. Q. (2020). Developing an integrated ISO 27701 and GDPR based information privacy compliance requirements model. In *Proceedings of the Australasian Conference on Information Systems (ACIS 2020), Wellington.*

Arias, E.C. (2014). Un estudio comparado en Latinoamérica sobre la cadena de custodia de las evidencias en el proceso penal. *Revista de la Facultad de Derecho y Ciencias Políticas, 44*.

Beebe, N. L., & Clark, J. G. (2004). A hierarchical, objectives-based framework for the digital investigations process. Digital Forensic Research Workshop.

Brezinski, D., & Killalea, T. (2002). Guidelines for evidence collection and archiving. *Network Working Group*. In-Q-Tel; neart.org. RFC 3227. *Best Current Practice No. 55.*

Bardin, L. (1977). *Análise de conteúdo* (L. A. Reto & A. Pinheiro, Trads.). Edições 70.

Carvalho, R. W. R. (2020). A Importância da Cadeia de Custódia na Computação Forense. *Revista Brasileira de Criminologia, 9*(2), 134-138. DOI: http://dx.doi.org/10.15260/rbc.v9i2.463

Cantore, J. A. G. (2014). Cadena de custodia de evidencias [Chain of custody of evidence]. *Anales de la Facultad de Ciencias Médicas (Asunción), 47*(1).

Campos, L. M. O., Gomes, E., & Martins, H. P. (2016). Forensic Expertise in Storage Device USB Flash Drive: Procedures and Techniques for Evidence. *IEEE Latin America Transactions, 14*(7).

Ćosić, J., & Bača, M. (2010). A framework to (im)prove chain of custody in digital investigation process. In Proceedings of the 21st Central European Conference on Information and Intelligent Systems (pp. 435-438).

Ferreira, D. A. A., Pinheiro, M. M. K., & Marques, R. M. M. (2022). Privacidade e proteção de dados pessoais: perspectiva histórica. *InCID: R. Ci. Inf. e Doc., Ribeirão Preto, 12*(2), 151-172. https://doi.org/10.11606/issn.2178-2075.v12i2p151-172

International Organization for Standardization. (2013). *ISO/IEC 27037:2013 Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence.* ISO.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (*NIST Special Publication 800-86*). *National Institute of Standards and Technology*. https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response.

Machado, N. T., Basile, F. R. M., Amate, F. C., & López, L. J.R. (2021). Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta. *Revista Científica General José María Córdova, 19*(33), 181-203. http://dx.doi.org/10.21830/19006586.726.

Malhotra, N. K. (2019). *Pesquisa de Marketing: Uma Orientação Aplicada.* Brasil: Bookman.

Nandhakumar, N. K., Agarwal, U., & Faizal, H. (2012). Use of AFF4 Chain of Custody - Methodology for Foolproof Computer Forensics Operation. *International Journal of Communication and Networking System, 1*(1), 49. ISSN: 2278-2427.

Netto, A. da S., & Silveira, M. A. P. da. (2007). Gestão da segurança da informação: Fatores que influenciam sua adoção em pequenas e médias empresas. *Journal of Information Systems and Technology Management, 4*(3), 375-397. TECSI FEA USP. ISSN 1807-1775.

Ramadhan, R. A., Setiawan, P. R., & Hariyadi, D. (2022). Digital forensic investigation for non-volatile memory architecture by hybrid evaluation based on ISO/IEC 27037:2012 and

NIST SP800-86 framework. *IT Journal Research and Development (ITJRD)*, *6*(2). https://doi.org/10.25299/itjrd.2022.8968

Riaño, J. J. K. B. (2020). Avances de la informática forense en Colombia en los últimos cuatro años. *Revista Ingeniería, Investigación y Desarrollo, 20*(1), 69-78.

Ramírez, D. A. M., Gonzales, R. M., & Castro, G. A. H. (2019). Digital evidence focused on solid state drives (SSD): a review. *Revista Ingeniería, Investigación y Desarrollo, 20*(1), 69-78. https://doi.org/10.14483/issn.2248-4728.

Sansigolo, G. (2015). A importância da série ISO 27000. *Faculdade de Tecnologia de São José dos Campos.*

Tomlinson, J. J., Elliott-Smith, W., & Radosta, T. (2006). Laboratory information management system chain of custody: reliability and security. *Journal of Automated Methods and Management in Chemistry*. Hindawi Limited.

Trivinos, A. N. S. (1987). *Introdução à pesquisa em ciências sociais: A pesquisa qualitativa em educação.* Atlas.

Voronkova, S. (2011). A Computational Forensic Methodology for Malicious Application Detection on Android OS (*Master's thesis*). Free University of Bozen/Bolzano, Faculty of Computer Science.

Yalçın, N., & Kılıç, B. (2019). Digital evidences according to ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 and ISO/IEC 27043 standards. In *Proceedings of the 4th International Symposium on Innovative Approaches in Engineering and Natural Sciences* (pp. 444). https://doi.org/10.36287/setsci.4.6.118