


ON THE TRACK OF DIGITAL SECURITY: PROTECTING KNOWLEDGE

 <https://doi.org/10.56238/arev7n2-223>

Submitted on: 19/01/2025

Publication date: 19/02/2025

**José Omar Pais Landim¹, Rafael Dall'Armeline Ramos², Maria das Mercês de Araujo³,
Katarina Maria Ferraz Mendonça⁴ and Paulo Edson Cutrim Silva⁵**

ABSTRACT

This study investigated digital security practices and their effectiveness in protecting knowledge within organizations and educational institutions. The central problem addressed was how digital security practices can be improved to ensure the protection of knowledge in educational and corporate environments. The general objective was to analyze digital security practices and their contributions to the protection of knowledge, highlighting the technologies used and the challenges faced in the implementation of these practices. The research adopted a bibliographic methodology, with a survey of articles, books and other relevant documents on information security, cryptography, artificial intelligence and digital awareness. The results indicated that the combination of advanced technologies, such as cryptography and artificial intelligence, with the continuous awareness of users, is an approach to ensure the protection of knowledge. It was identified that user resistance and lack of resources are challenges to be overcome. In addition, the integration between technology and the continuing education of employees proved to be essential for the success of digital security policies. Closing remarks suggested that digital security should be seen as a collective effort within organizations, and that studies are needed to explore the impact of emerging technologies such as blockchain and AI on knowledge protection.

Keywords: Digital Security. Knowledge Protection. Cryptography. Artificial intelligence. Awareness.

¹ Master in Emerging Technologies in Education

MUST University

E-mail: joseomarpais@hotmail.com

² Master's student in Intellectual Property and Technology Transfer for Innovation

Federal University of Roraima (UFRR)

E-mail: rafadelar@gmail.com

LATTES: <http://lattes.cnpq.br/4731935507616458>

³ Master in Emerging Technologies in Education

MUST University

E-mail: bia_ldm@hotmail.com

LATTES: <http://lattes.cnpq.br/4834437753213994>

⁴ Master's student in Business Administration

MUST university

E-mail: katterraz@gmail.com

LATTES: <https://lattes.cnpq.br/3474603536207473>

⁵ Dr. student in Educational Sciences

Inter-American Faculty of Social Sciences (FICS)

E-mail: pauloedsons@gmail.com

LATTES: <http://lattes.cnpq.br/9657537660565747>

INTRODUCTION

Digital security has become one of the essential pillars in the current context, as society moves towards a connected world. With the increasing digitalization of processes and the interdependence between systems, the protection of information becomes essential to ensure the integrity, confidentiality and availability of data. The digital age imposes new challenges for the protection of knowledge, which involves the management and proper use of information in environments susceptible to cyber attacks. In this way, digital security is not only restricted to data protection, but also to maintaining trust in digital platforms, which support social, educational, and corporate interactions.

The justification for carrying out this research is linked to the need to understand the implications of digital security in the current scenario, especially with regard to the protection of knowledge. With the rise in cyber threats such as *malware*, ransomware attacks, and data leaks, it becomes imperative for individuals and organizations to adopt effective security practices to protect their information. In addition, the growing adoption of digital platforms in the educational and corporate environment amplifies the need to study the security measures necessary to protect both knowledge and personal data. Implementing appropriate security policies and raising awareness of existing threats are key to ensuring the integrity of the knowledge generated and shared in these environments. This study aims to address the main concepts and practices related to digital security, focusing on how these measures impact the protection of knowledge in different spheres.

The question that guides this research is: how can digital security practices be improved to ensure the protection of knowledge in educational and corporate environments? This question seeks to explore the digital security strategies, tools, and policies that are effective in preserving information, highlighting the main vulnerabilities and applicable solutions. By addressing this issue, it is hoped to better understand the role of digital security in the context of knowledge protection and how organizations can implement effective measures to mitigate risks and improve the resilience of systems.

The objective of this research is to analyze the digital security practices that can be applied to ensure the protection of knowledge in educational and corporate environments, proposing effective solutions to face the challenges encountered. Throughout the text, a discussion on information security will be presented, covering from the basic concepts to emerging technologies that have shown promise in improving security practices.

This work is structured as follows: after the introduction, the theoretical framework section explores the fundamental concepts of digital security, addressing information protection and common cyber threats. Next, the development topics argue the strategies and technologies that can be applied to strengthen digital security, focusing on the impact of these measures on the protection of knowledge. The methodology described details the process of data collection and analysis, while the discussion and results section presents the main findings of the research, with a critical analysis of the effectiveness of safety practices in the context studied. Finally, the final considerations summarize the conclusions of the survey, pointing out future paths for the continuous improvement of digital security.

THEORETICAL FRAMEWORK

The theoretical framework of this work is structured to provide an understanding of the main concepts related to digital security and their application in the protection of knowledge. At first, the fundamentals of information security will be addressed, with emphasis on essential principles such as confidentiality, integrity, and availability, which are the basis of all data protection practices. Then, the culture of information security will be discussed, exploring the relevance of awareness and training of individuals in educational and corporate environments. Based on this, the General Data Protection Law (LGPD) and its relevance for the implementation of security and compliance measures in the various sectors will be presented. In addition, cyber threats, including *malware*, *phishing*, and *ransomware attacks*, will be analyzed, with a focus on strategies for preventing and responding to these threats. The framework will also address emerging technologies such as cryptography, artificial intelligence, and *blockchain*, which have played a growing role in the evolution of digital security practices. Thus, the theoretical framework aims to provide a basis for the analysis of digital security practices in the context of knowledge protection.

DIGITAL SECURITY MODELS AND FRAMEWORKS

Digital security models and frameworks are key to ensuring effective information protection in a variety of contexts, including corporate and educational environments. Digital security is not restricted to the implementation of protection technologies, but involves a set of practices and policies aimed at the integrity and confidentiality of information, as well as the prevention of unauthorized access.

In the educational context, digital security is also linked to digital citizenship, an essential concept to ensure the ethical and responsible use of technologies. Cruz (2023) highlights the importance of digital citizenship and the challenges of its implementation in basic education, stating that:

The world is approaching almost 5 billion users on the internet, making its use an imperceptible habit. We are connected and need to follow a set of rules for a pleasant virtual relationship, for this, digital citizenship arises. Digital citizenship can be understood as a set of rules that we must follow in order to use the digital world, and the different technologies that constitute it, with awareness, responsibility, ethics and security. The theme covers people of all ages and generates special attention for children and adolescents (Cruz, 2023, p. 01).

In this sense, both in the educational and corporate sectors, digital security becomes indispensable to protect sensitive data and avoid financial and reputational losses caused by cyber attacks. For this, security models must be adopted to create a robust protection infrastructure, using resources such as encryption, firewalls, antivirus, and monitoring systems.

In addition to technological solutions, the implementation of effective security policies is also necessary. These policies should range from access control to user awareness of good digital security practices, promoting an environment prepared to deal with virtual threats (Santos; Krawszuk, 2020).

In the educational context, digital security acquires a still critical dimension, considering the amount of sensitive personal data of students and teachers that are managed on teaching platforms. The adoption of security models in educational institutions aims to protect this information and ensure that the learning environment is safe, not only from a technical point of view, but also in terms of protection against fraudulent practices and misuse of digital platforms. In addition, digital security in schools must be addressed in a way that involves the entire academic community, with training and awareness of the importance of safe practices in the virtual environment. The implementation of access control systems, the application of backup policies, and the use of encryption tools are some of the recommended measures to prevent data leakage and ensure the integrity of information (Cruz, 2023).

The use of security models must also consider the specificities of each environment, adopting different approaches according to the needs and risks associated with each context. While in corporate organizations the focus is on protecting sensitive data and

minimizing financial risks, in educational institutions digital security focuses on protecting student data and preventing fraud and inappropriate practices in the use of educational platforms (Blefari; Paulon; Lima, 2021). Thus, the application of these security models must be dynamic, adapting to the constant changes in cyber threats and the evolution of technologies used for information protection. The implementation of a digital security culture, which involves both the technological infrastructure and the continuous training of users, is a fundamental factor for the success of these strategies, whether in the corporate or educational environment (Dias; Zechariah; Santos, 2024).

EMERGING TECHNOLOGIES IN INFORMATION SECURITY

Emerging technologies play a key role in the evolution of information security practices, providing new methods of protecting data and systems in the face of complex threats. Artificial intelligence (AI), for example, has proven to be a tool in detecting and mitigating cyberattacks. With the use of machine learning algorithms, AI is able to identify unusual patterns of behavior in systems and detect potential threats before they become critical. This automated, real-time detection process improves the responsiveness of security systems (Martins, 2024). Additionally, AI has been employed in the creation of adaptive security systems, which are able to learn from past attacks and improve their defense strategies.

Another example of a surging technology is *blockchain*, which, although initially associated with the financial market, has also gained prominence in the field of information security. Its decentralized and immutable structure becomes an effective mechanism to ensure data integrity, making it difficult to manipulate and unauthorized access. Blockchain can be used to create secure systems for authenticating and tracking data, especially in sensitive transactions, such as those involving financial and personal information. Its ability to ensure the authenticity and transparency of operations is a significant advance in data protection in distributed systems (Cruz, 2023).

In addition to *blockchain*, other emerging technologies, such as *Big Data* and cloud computing, play a crucial role in the integrity and analysis of large volumes of information, being essential to prevent data manipulation and unauthorized access. According to Dias, Zacarias and Santos (2024, p. 83):

In the socio-technical and organizational landscape that recognizes the interaction between people and technology in an organization, it is challenging to maintain transparency and interoperability between constituent systems. Such constituent systems can interconnect with cloud computing to store data, and *Big Data Analytics* systems to harvest, inspect, treat, and model this data to gain *insights* and identify patterns internal to the organization. *Big data* and cloud computing are important features in business strategies in financial and banking systems.

The growing threat of cyberattacks also reinforces the need for effective strategies to mitigate risks, making it essential to implement robust information security solutions, such as *blockchain*, vulnerability monitoring, and data encryption. As highlighted by Dias, Zacarias and Santos (2024, p. 100):

It is also worth noting the growth in the number and impact of cyber attacks. Cybersecurity is affecting systems, which can hit critical infrastructure, such as an SoS that takes care of an organization's accounting.

The adoption of *blockchain*, therefore, allows control over the integrity of information, essential for environments where trust in data storage and processing is fundamental (Santos; Krawszuk, 2020). In addition, the implementation of complementary technologies, such as *Big Data* and cloud computing, reinforces the security of systems and protection against cyber attacks, ensuring greater reliability in digital processes.

Encryption also continues to be one of the essential technologies in data protection, especially as the amount of sensitive information transmitted over the internet grows. Modern encryption, with its advanced algorithms, ensures that data is ineligible to any unauthorized person, even if intercepted during transmission. The application of strong encryption in communication systems, such as emails, e-learning platforms, and corporate networks, ensures that information is protected from unauthorized access, preventing leaks and hacker attacks. In addition, cryptography plays a key role in the implementation of multi-factor authentication systems, in which data protection does not depend only on a password, but on multiple factors, such as biometrics or temporary codes, which increases security in accessing critical systems (Fernandes; Teixeira, 2024). In this way, encryption continues to be one of the effective lines of defense in protecting sensitive data and ensuring users' privacy.

Therefore, emerging technologies, such as artificial intelligence, *blockchain*, and cryptography, offer new possibilities for the protection of data and systems, impacting information security practices. The use of these technologies has proven effective in strengthening cyber defenses, increasing the detection capacity, integrity, and

confidentiality of data, essential aspects for digital security in the current scenario (Dias; Zechariah; Santos, 2024).

THE IMPORTANCE OF DIGITAL SECURITY AWARENESS

Awareness of digital security is a fundamental aspect to ensure the protection of data and systems in any organization or educational institution. The adoption of appropriate security practices depends, to a large extent, on the continuous training of professionals and users on the risks and the best approaches to prevent threats. Studies indicate that most digital security incidents occur due to inappropriate user behavior, such as using weak passwords or opening emails (Fernandes; Teixeira, 2024). Therefore, awareness and training are essential to mitigate risks related to human error, which is still one of the biggest vulnerabilities in digital security systems.

In addition, digital security training should be an ongoing process, as cyber threats are constantly evolving, and new forms of attack emerge. Organizations need to invest in training programs for their employees, which should be periodically updated to reflect changes in the digital security landscape (Cruz, 2023). The implementation of awareness programs should involve everything from the identification of fraudulent emails to the application of security practices on mobile devices, considering that the use of personal devices for professional purposes also represents a growing concern in terms of security (Santos; Krawszuk, 2020). As such, it is necessary to ensure that users are trained to recognize and avoid risky situations such as *phishing attacks*, *malware*, and other types of digital fraud.

In the educational context, awareness of digital security also becomes essential, since students and teachers are involved with digital technologies, which can pose risks if not used with caution. Training in digital security in schools and universities should cover both the safe use of e-learning platforms and the protection of students' and teachers' personal information (Blefari; Paulon; Lima, 2021). The creation of a culture of digital security within these institutions contributes to the formation of a generation aware of privacy and data protection issues, preparing them to act safely in a digital world.

Therefore, digital security awareness is an essential measure for protecting data and systems in any environment. The continuous training of professionals and users, through effective training programs, contributes to reducing vulnerabilities caused by human errors and improving the effectiveness of the security policies adopted. The integration of these

practices into corporate and educational environments is essential to ensure that cyber threats are minimized and that data protection is maintained effectively (Dias; Zechariah; Santos, 2024).

METHODOLOGY

The present research is characterized as a bibliographic research, whose objective is to explore the theme of digital security and its relationship with the protection of knowledge. The bibliographic research was chosen due to the need to understand, from the existing literature, the main approaches, concepts and practices related to information security, which are essential for the construction of a theoretical framework. According to Santana, Narciso and Fernandes (2025), bibliographic research allows the identification, analysis and synthesis of knowledge already produced on a given topic, contributing to the formulation of new perspectives and theoretical deepening.

The approach adopted was qualitative, since the study seeks an analysis of digital security concepts and practices, without the need to collect primary data. The instruments used for data collection, according to Santana and Narciso (2025) for this type of research, were academic articles, books, dissertations, theses, and other scientific documents that address digital security, risk management, cyber threats, and emerging technologies related to information protection. For the selection of materials, a survey was carried out in academic databases, *such as Google Scholar, ResearchGate and Scielo*, prioritizing recent publications that contribute to the understanding of the theme. The analysis techniques consisted of a critical reading and comparison of the different approaches presented in the selected sources, with the aim of identifying the best practices and gaps in digital security, especially in the context of knowledge protection (Narciso. Santana, 2024). The research sought to integrate the ideas and solutions proposed by several authors, with a view to building a vision of the challenges and solutions for the protection of digital information.

Below is the table with the references used in the research. This table was prepared with the objective of organizing and clearly presenting the sources consulted, facilitating consultation throughout the literature review. The table contains the essential information about each reference, including the author, the title of the work, the year of publication and the type of document, allowing the reader to verify the sources consulted.

Chart 1 – References Used in the Research

Author(s)	Title as published	Year	Type of Work
SANTOS, H. M.; KRAWSZUK, G. L.	Organizational knowledge management: archival treatment for the reuse of administrative information	2020	Investigación Bibliotecológica
BLEFARI, R.; PAULON, P. P.; LIMA, K. A.	Using the Cause and Effect Model and Graph Theory to develop an information security prioritization mechanism for an enterprise environment	2021	Information Security Journal
NEVES, D. L. F.; LOPES, T. S. A.	Information security meets LGPD compliances	2021	Processing Knowledge Magazine
CRUZ, J. O.	A Guide to Digital Citizenship Education for Elementary School	2023	Dissertation (Master's Degree) – Federal University of Campina Grande
DIAS, R. M.; ZACARIAS, R. O.; SANTOS, R. P.	Ontology for Information Security Management in Systems-of-Systems	2024	ResearchGate
FERNANDES, R. M. M.; TEIXEIRA, C. M. F.	Security and responsibility in the use of computer technology – A proposal for an approach to <i>Malware</i> in the first year of elementary school	2024	Brazilian Symposium on Information and Computer Systems Security (SBSeg)
MARTINS, A. M.	Trail – <i>Software Security</i>	2024	The Developer's Conference (TDC)

Source: authorship.

This table presents the sources consulted for the elaboration of the research, which were selected based on their relevance to the topics addressed and their contribution to the understanding of digital security, its practices and challenges. By organizing the references in this way, it is easier to consult each material used, allowing the reader to follow the sources and verify the theoretical basis that supports the analysis developed throughout the work.

RESULTS AND DISCUSSION

The Word Cloud presented below highlights the frequent and significant terms present in the frame of reference, which will be addressed in the subsequent topics, results and discussions of this research. The terms visualized reflect the centrality of key concepts related to digital security, data protection, cyber threats, and emerging technologies that impact information security. These concepts are essential for understanding the challenges and solutions in the context of knowledge protection in organizations.

Nuvem de Palavras: Relevant Terms for Digital Security



CHALLENGES OF IMPLEMENTING DIGITAL SECURITY PRACTICES

REVISTA ARACÊ, São José dos Pinhais, v.7, n.2, p.8395-8411, 2025

In addition, the lack of resources, both financial and human, for the implementation of proper security practices is another important challenge. Many organizations, especially those that are small or have limited budgets, face difficulties in investing in cutting-edge technologies, such as monitoring systems, advanced encryption, and awareness programs for their employees (Fernandes; Teixeira, 2024). In educational institutions, budget limitations can also hinder the adoption of technologies that ensure the digital security of teaching platforms and the storage of sensitive student data. In this way, the lack of adequate investment compromises the effectiveness of digital security practices and increases vulnerability to cyber attacks.

Another significant challenge in implementing good digital security practices is the constant evolution of cyber threats. With the growth of new attack techniques, such as *ransomware* and sophisticated *phishing* attacks, defense strategies need to be updated to remain effective (Santos and Krawszuk, 2020). Many organizations and schools lack the necessary structure to keep up with these rapid changes, which results in the application of outdated security measures. This scenario requires not only the adoption of emerging technologies, but also a continuous review of security policies and constant training of users, in order to ensure that everyone is prepared to face the new types of threats (Blefari; Paulon; Lima, 2021).

Therefore, effectively implementing digital security practices is fraught with challenges, including user resistance, lack of resources, and constantly evolving threats. Overcoming these difficulties requires a joint effort between IT managers, security professionals and users, in addition to investing in appropriate technologies and constantly updating security policies (Dias; Zechariah; Santos, 2024). As such, it is critical for organizations and institutions to take a holistic approach, which includes not only the implementation of technological solutions but also ongoing awareness and training of everyone involved.

IMPACT OF DIGITAL SECURITY ON KNOWLEDGE PROTECTION

Digital security plays a key role in protecting knowledge within organizations, ensuring that sensitive and strategic information is not improperly accessed or compromised by leaks. Digital security practices, such as access control, encryption, and constant monitoring of systems, are key to protecting the knowledge generated within these entities, whether it is in the form of documents, financial data, or intellectual property.

Implementing appropriate security strategies helps prevent unauthorized access to sensitive information by ensuring that only authorized individuals can access and handle critical data (Fernandes; Teixeira, 2024). In addition, employee awareness of good security practices also contributes to the protection of knowledge, since many security leaks and incidents happen due to human error, such as the use of weak passwords or the opening of emails (Cruz, 2023).

Another aspect is the impact of emerging technologies, such as encryption, which ensures the protection of data during transmission and storage. Encryption acts as an additional layer of security, making data unreadable to any unauthorized person, which is especially relevant when it comes to protecting sensitive knowledge within organizations. The use of advanced encryption in internal and external communications helps to ensure that knowledge shared between departments or between organizations is protected against interception and unauthorized access (Santos; Krawszuk, 2020). The application of these security practices is also essential in sectors such as education and industry, where the protection of data and strategic information is a priority.

In addition, the use of digital security models and frameworks, which include risk management policies and the implementation of monitoring systems, helps in the early detection of security incidents and the mitigation of possible damage. Continuous monitoring of user and system activities enables organizations to identify suspicious patterns of behavior and take preventive action before a major incident occurs (Blefari; Paulo; Lima, 2021). This ensures that knowledge, considered a strategic asset, is protected from cyber threats and other vulnerabilities, reducing the risk of leaks and targeted attacks.

Therefore, digital security practices are essential for the protection of knowledge within organizations. By adopting effective protection measures, such as encryption, access control, and continuous monitoring, organizations are able to protect their sensitive data and strategic information in a timely manner. In addition, user awareness and the implementation of emerging technologies, such as artificial intelligence for threat detection, are key to strengthening defenses against unauthorized access and preventing information leaks (Dias; Zechariah; Santos, 2024). In this way, digital security not only protects data, but also ensures the integrity and continuity of processes within organizations.

SUCCESS AND FAILURE STORIES IN DIGITAL SECURITY

The analysis of real cases of digital security implementation allows a better understanding of the factors that contribute to the success or failure of the strategies adopted by organizations. In many cases, effective implementation of digital security has been critical to protecting sensitive data and preventing financial or reputational damage. However, there are also examples where a lack of adequate investment, resistance to change, or neglect to apply security practices have resulted in serious failures. One of the success factors observed in organizations that have effectively implemented digital security was the commitment to employee education and awareness. Organizations that have invested in continuous training for their employees, focusing on good security practices, have been able to reduce incidents caused by human error, which is one of the main causes of failures in security systems (Fernandes; Teixeira, 2024). In addition, the implementation of monitoring and access control tools was essential to identify suspicious behavior and prevent unauthorized access.

On the other hand, common failures in digital security implementations occur due to a lack of adequate resources and a lack of continuous updating of security policies. In several cases of failure, organizations have not been able to keep up with the evolution of cyber threats, which has resulted in the vulnerability of their systems to new types of attacks, such as *ransomware* and *phishing*. The lack of investments in emerging technologies, such as encryption and artificial intelligence for threat detection, has been a critical factor in the exposure of sensitive data and the failure to protect strategic information (Santos; Krawszuk, 2020). Users' resistance to adopting security measures, such as multi-factor authentication or the use of strong passwords, also contributes to the occurrence of security incidents, as individuals often underestimate the risks associated with poor digital security practices (Martins, 2024, p. 3).

In addition, in some cases, the lack of an integrated approach to digital security, involving both technology and people, has resulted in significant failures. The isolated implementation of security tools, without an organizational culture that encourages compliance with security policies, is often not enough to ensure effective data protection. The lack of a clear IT governance strategy and the absence of an incident response plan have also been identified as common causes of digital security failures (Blefari; Paulo; Lima, 2021). Therefore, the integration of security policies, user training, and the

application of appropriate technologies are essential elements for the success of any digital security strategy.

In summary, the analysis of success and failure cases in digital security highlights the importance of a holistic approach, which considers both technological and human aspects. Investing in emerging technologies, such as encryption and artificial intelligence, as well as in user awareness and constantly updating security policies, are factors that contribute to the effective protection of data and systems. Failures to implement these practices in an integrated manner can result in serious vulnerabilities, compromising information security and the continuity of organizational processes (Cruz, 2023).

FINAL CONSIDERATIONS

Digital security practices play a key role in protecting knowledge within organizations, as evidenced by the findings of this survey. The analysis revealed that the adoption of effective security measures, such as encryption, access control, and user awareness, are essential to ensure the integrity, confidentiality, and availability of information. Digital security strategies, when implemented, help prevent leaks and unauthorized access, protecting sensitive data and organizational systems. Therefore, digital security practices are essential not only for protecting information but also for ensuring the continuity of operations and maintaining trust in digital platforms.

In response to the survey question, 'how can digital security practices be improved to ensure the protection of knowledge in educational and corporate environments?', the results indicate that combining advanced technologies with the continuous education of users is an effective approach. The use of tools such as cryptography and artificial intelligence, along with the implementation of digital security awareness policies, has proven effective in protecting knowledge. Users' resistance to adopting safety practices, often due to a lack of awareness, is a challenge to overcome, which reinforces the need for ongoing training and awareness campaigns. Thus, the issue of digital security is linked to the empowerment of individuals and the use of emerging technologies that make systems secure and resilient.

In addition, the study revealed that the implementation of an effective digital security model depends on an integrated approach, which combines existing technologies with organizational awareness and employee commitment. Organizations that invest in both technological solutions and human training are able to reduce the risks of security incidents

and increase the resilience of systems. While emerging technologies such as artificial intelligence and *blockchain* offer new possibilities for information security, human factors such as awareness and adherence to security policies remain critical elements for the success of any digital protection strategy.

The survey also highlighted the importance of a holistic approach, where digital security is seen not only as a responsibility of the IT department, but as a collective effort that involves all members of the organization. In educational settings, digital security awareness is vital, as students and teachers are exposed to cyber threats. In this context, the adoption of security practices must be accompanied by education about the risks and ways to mitigate them, creating an organizational culture that values the protection of information and the safe use of digital platforms.

While the results provide insight into digital security practices and their impacts, it is clear that studies are needed to broaden understanding of emerging technologies and their role in the evolution of security practices. The study of the impact of new technologies, such as artificial intelligence for threat detection and the use of *blockchain* to ensure data integrity, should be explored, considering the rapid changes in the field of cybersecurity. Additionally, it would be important to investigate how different sectors, such as education, can tailor digital security practices to their specific needs in order to improve knowledge protection in educational settings.

In conclusion, digital security practices are key to protecting knowledge within organizations, preventing leaks and unauthorized access. The use of advanced technologies, coupled with continuous user awareness, is key to addressing digital security challenges. However, the constant advancement of cyber threats requires security strategies to be updated and adapted, which reinforces the need for continuous investments in new technologies and in the training of individuals. The research suggests that while great progress has been made, there is still much to be explored to ensure knowledge protection in organizations.

REFERENCES

1. BLEFARI, R.; PAULON, P. P.; LIMA, K. A. Utilizando o Modelo de Causa e Efeito e a Teoria dos Grafos para o desenvolvimento de um mecanismo de priorização em segurança da informação para um ambiente corporativo. **Revista de Segurança da Informação**, v. 5, n. 2, p. 45-67, 2021. Disponível em: <https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/download/16/1>. Acesso em 09 de fevereiro de 2025.
2. CRUZ, J. O. **Um guia para educação em cidadania digital voltado ao ensino fundamental**. Dissertação (Mestrado) – Universidade Federal de Campina Grande, Campina Grande, 2023. Disponível em: <http://dspace.sti.ufcg.edu.br:8080/xmlui/handle/riufcg/34750>. Acesso em 09 de fevereiro de 2025.
3. DIAS, R. M. **Ontologia para o gerenciamento de segurança da informação em sistemas-de-sistemas**. ResearchGate, 2024. Disponível em: https://www.researchgate.net/profile/Roberto-Dias-8/publication/361289641_Ontologia_para_o_Gerenciamento_de_Seguranca_da_Informacao_em_Sistemas-de-Sistemas/links/62a8e00ec660ab61f87c7c88/Ontologia-para-o-Gerenciamento-de-Seguranca-da-Informacao-em-Sistemas-de-Sistemas.pdf. Acesso em 09 de fevereiro de 2025.
4. FERNANDES, R. M. M.; TEIXEIRA, C. M. F. Segurança e responsabilidade no uso de tecnologia computacional – Uma proposta de abordagem de Malwares no primeiro ano do ensino fundamental. In: Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg), 2024, Brasil. **Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2024. Disponível em: <https://sol.sbc.org.br/index.php/sbceb/article/view/28687>. Acesso em 09 de fevereiro de 2025.
5. MARTINS, A. M. **Trilha – Software Security**. The Developer's Conference (TDC), 2024. Disponível em: https://cdn.thedevconf.com.br/presentations/TDC2019SP/softwaresecurity/MOR-6749_2019-07-21T112010_TDA_SoftwareSecurity_SP_Boas_Pr%C3%A1ticas_de_Security_e_Privacy_by_Design_para_um_SDLC_Seguro%20%20-%20%20Modo%20de%20Compatibilidade.pdf. Acesso em 09 de fevereiro de 2025.
6. NARCISO, R.; SANTANA, A. C. de A. Metodologias Científicas na Educação: uma Revisão Crítica e Proposta de Novos Caminhos. **ARACÊ**, v. 6, n. 4, p. 19459–19475, 2024. DOI: 10.56238/arev6n4-496. Disponível em: <https://periodicos.newsciencepubl.com/arace/article/view/2779>. Acesso em: 12 feb. 2025.
7. NEVES, D. L. F.; LOPES, T. S. A. A segurança da informação de encontro às conformidades da LGPD. **Revista Processando o Saber**, v. 10, n. 4, p. 122-138, 2021. Disponível em: <https://fatecpqg.edu.br/revista/index.php/ps/article/view/171>. Acesso em 09 de fevereiro de 2025.

8. SANTANA, A. C. de A.; NARCISO, R.; FERNANDES, A. B. Explorando as metodologias científicas: tipos de pesquisa, abordagens e aplicações práticas. **Caderno Pedagógico**, v. 22, n. 1, p. e13333, 2025. DOI: 10.54033/cadpedv22n1-130. Disponível em: <https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/13333>. Acesso em: 09 fev. 2025.
9. SANTANA, A. C. de A.; NARCISO, R. Pilares da Pesquisa Educacional: Autores e Metodologias Científicas em Destaque. **ARACÊ**, v. 7, n. 1, p. 1577–1590, 2025. DOI: 10.56238/arev7n1-095. Disponível em: <https://periodicos.newsciencepubl.com/arace/article/view/2782>. Acesso em: 12 fev. 2025.
10. SANTOS, H. M.; KRAWSZUK, G. L. Gestão do conhecimento organizacional: tratamento arquivístico para reuso da informação administrativa. **Investigación Bibliotecológica**, v. 34, n. 2, p. 75-94, 2020. Disponível em: https://www.Scielo.org.mx/SciELO.php?pid=S0187-358X2020000200103&script=sci_arttext. Acesso em 09 de fevereiro de 2025.