


DIGITAL SECURITY AND PRIVACY IN EDUCATION: CHALLENGES IN THE USE OF TECHNOLOGIES IN SCHOOL ENVIRONMENTS

 <https://doi.org/10.56238/arev6n4-282>

Submitted on: 18/11/2024

Publication date: 18/12/2024

Elias Nascimento Magalhães¹, Clenya Rejane Barros de Lima², Maria Marta Coelho Miranda³, Crystiane Ribeiro Mendes de Oliveira⁴ and Denise Viviane Boing⁵

ABSTRACT

The present study investigated the challenges faced by schools in the use of digital technologies, focusing on data security and privacy. The central problem of the research involved identifying the main barriers to the implementation of safe practices in schools, considering the lack of training of educators, resistance to change and the absence of adequate infrastructure. The overall objective was to analyze how schools can overcome these challenges and ensure a safe digital environment. The methodology adopted was a literature review, in which academic sources related to digital security in education were analyzed. The results showed that, despite technological innovations, many institutions still face difficulties in implementing efficient security policies. Lack of ongoing training for educators and institutional resistance were identified as key obstacles. Public policies for digital security, although fundamental, still need continuous implementation and monitoring. The final considerations highlighted the need for assertive actions to ensure data protection and digital security in schools, in addition to suggesting that studies be carried out to complement the findings, especially with regard to the adaptation of policies to local realities. This study contributes to the understanding of the challenges faced by schools in implementing technologies in a safe way.

Keywords: Digital Security, Privacy, Education, Technologies, Public Policies.

¹ Master's student in Emerging Technologies in Education
MUST University
Email: mestre.enm@gmail.com

² Dr. in Sciences
Federal University of the State of Rio de Janeiro (UNIRIO)
E-mail: clenyarbarros@uerr.edu.br

³ Master in Emerging Technologies in Education
MUST University
Email: coelhomarta1986@gmail.com

⁴ Master in Emerging Technologies in Education
MUST University
E-mail: crysrmendes@gmail.com

⁵ Master's student in Emerging Technologies in Education
MUST University
E-mail: boingdenise63@gmail.com

INTRODUCTION

Digital security and privacy in education have become relevant issues in the current context, in which digital technologies play a central role in the teaching-learning process. The growing use of technological tools in schools, such as teaching platforms, social networks, and educational management systems, brings with it significant challenges with regard to the protection of student and educator data, in addition to the need to ensure a safe digital environment for all involved. With the advancement of technologies, new forms of interaction and access to information have emerged, which requires the implementation of measures to protect the privacy and security of information shared in the school environment. Digital education, in turn, requires both educators and students to be aware of the risks and know how to navigate the online environment safely.

The justification for conducting this study is based on the context in which digital education has been expanding, driven by public policies and the growing demand for innovative teaching methods. The use of technologies in the educational process offers numerous advantages, such as expanding access to knowledge and developing essential digital skills. However, inappropriate or uninformed use of these technologies can expose students and educators to risks related to data privacy and security. Thus, it is necessary to investigate how schools are dealing with the challenges of digital security and privacy, with regard to the protection of students' personal and academic information. In addition, the implementation of digital security policies in educational institutions must be accompanied by adequate training for teachers and students, in order to promote a culture of responsible use of technologies.

The central problem of this research is related to the challenges faced by educational institutions to ensure digital security and privacy in the use of technologies in school environments. Although schools adopt new technological tools, often the lack of adequate infrastructure, training of education professionals and public policies become obstacles to ensuring a safe and reliable environment. Data privacy concerns, especially with the growing number of personal information shared *online*, highlight the need for a close look at digital security practices in schools. Therefore, it is essential to understand how schools can overcome these challenges and implement efficient strategies to protect student and educator data, as well as ensure the responsible use of technologies.

The objective of this research is to analyze the challenges related to digital security and privacy in education, specifically in the context of the use of technologies in school

environments. The survey seeks to identify the main difficulties encountered by schools and suggest strategies to promote a safe and secure digital environment.

This work is structured in different sections that aim to present and discuss the issues around digital security and privacy in education. The introduction offers an overview of the topic, followed by a literature review that addresses the concepts and main theoretical discussions on digital security, privacy and digital citizenship in the educational context. Then, three development topics are presented, which deal with the challenges in the use of technologies in the classroom, the importance of training for educators and students, and the tools and strategies used to ensure digital security in schools. The methodology adopted to carry out the research is described, followed by an analysis of the discussions and results found in the literature, highlighting the main challenges and opportunities related to digital security in schools. Finally, the final considerations present a summary of the findings and suggestions for future research on the subject.

THEORETICAL FRAMEWORK

The theoretical framework of this work is structured to address the main concepts and discussions related to digital security, privacy and digital citizenship in the educational context. Initially, the concept of digital security will be explored, highlighting its fundamentals, common threats in educational environments and data protection strategies. Then, privacy in the school environment will be discussed, with an emphasis on relevant legislation, such as the General Data Protection Law (LGPD), and the challenges faced by educational institutions to ensure the protection of the personal information of students and educators. The last part of the theoretical framework will address digital citizenship, analyzing the responsibility in the use of technologies and the formation of critical and conscious citizens in the *online environment*. The framework aims to provide a basis for understanding the central themes of the research and the challenges related to the implementation of security and privacy measures in the educational environment.

CHALLENGES IN THE USE OF DIGITAL TECHNOLOGIES IN THE CLASSROOM

The use of digital technologies in classrooms has expanded, providing new possibilities for teaching and learning. However, the implementation of safe and efficient practices in schools faces several challenges. One of the main obstacles is the lack of adequate infrastructure, which often makes it difficult to adopt technological tools safely. In

addition, resistance to change on the part of educators and managers also contributes to the limited implementation of practices that ensure data protection and digital security.

The lack of training and qualification of teachers in digital security issues is one of the factors that hinder the adoption of safe practices in schools. According to Araújo (2020, p. 119), "teacher training in digital security needs to be seen as a priority, because without proper preparation, teachers become vulnerable to digital threats, compromising both student safety and the effectiveness of teaching". The relevance of continuous training programs that specifically address security and privacy issues in the use of digital technologies is highlighted, as a way to minimize the risks associated with the inappropriate use of these tools in schools.

Another relevant challenge is the resistance to change in educational institutions, which are often reluctant to adopt new technologies due to factors such as lack of resources, ingrained habits, or fear of the unknown. According to Oliveira and Vaz (2022, p. 76), "teachers sometimes resist the integration of technologies in the teaching-learning process, as change requires us not only to master new tools, but also a new understanding of the role of the educator in the digital context". This behavior reflects the difficulty of adapting to the new pedagogical demands imposed by technology, which is a significant obstacle to creating a safe digital learning environment.

In addition, resistance to change is associated with the perception that technology can replace the role of the teacher, which generates insecurity in relation to their place in education. According to Araújo and Silva (2022, p. 188), "the transition to the use of technologies in education requires a reconfiguration of the teaching role, and this change is not always well received by educators, who may feel threatened in their traditional practice". Therefore, it is evident that resistance to change is not only a matter of adapting to new technologies, but also of reconfiguring the teacher's identity and pedagogical practice.

These challenges – the lack of training in digital security, resistance to change, and inadequate infrastructure – are significant obstacles to the safe implementation of technologies in schools. They therefore demand an integrated approach, which involves both the training of teachers and the development of public policies that encourage the responsible adoption of technologies, with the proper support and training for education professionals.

THE IMPORTANCE OF TRAINING AND AWARENESS FOR EDUCATORS AND STUDENTS

Training and awareness of both educators and students are essential for creating a safe school environment in the use of digital technologies. Continuing teacher training in digital security and privacy is one of the main strategies to ensure that educators are prepared to deal with the risks associated with the digital environment. According to Araújo (2020, p. 119), "it is essential that teachers receive continuous training on digital security, since the constant evolution of technologies requires them to be constantly updated, so that they can ensure the protection of their students and also of their own personal data" (p. 119). It is evident the need for continuous training programs for educators, in order to prepare them to face the challenges of digital security and implement pedagogical practices that protect the information of all those involved in the educational process.

In addition to the training of educators, it is also essential to sensitize students to the risks and responsibilities in the use of technologies. Raising students' awareness is a fundamental step for them to understand the importance of protecting personal data and know how to act responsibly and safely on the internet. As Oliveira and Vaz (2022, p. 76) point out, "students need to be educated about digital risks from an early age, in order to develop a critical stance towards technologies, learning to use digital tools ethically and safely". This awareness can be achieved through activities that promote the debate on privacy and security, encouraging students to reflect on their online actions and their consequences.

An example of good practice for the training of educators is the development of training programs that integrate theory and practice, addressing real digital risk situations. According to Araújo and Silva (2022, p. 188), "it is necessary that teacher training includes simulations of risk scenarios, such as the use of personal data on educational platforms and the analysis of possible threats to digital security, allowing educators to prepare to deal with these issues in their school routine". Such practices help educators not only understand the theoretical issues related to digital security, but also to apply them in a practical way in their daily activities, creating safe environments for teaching and learning.

Therefore, the continued training of educators and the awareness of students are essential actions to ensure digital safety in schools. These practices are essential for educational institutions to take advantage of technologies safely, forming responsible digital citizens who are prepared to face the challenges of the digital age.

TOOLS AND STRATEGIES TO ENSURE DIGITAL SAFETY IN SCHOOLS

The use of tools and strategies to ensure digital safety in schools has become a priority as digital technologies are incorporated into the educational environment. The use of educational platforms and software that prioritize security and privacy is one of the approaches to mitigate risks related to the use of personal data of students and educators. According to Oliveira and Vaz (2022, p. 76), "educational platforms must incorporate tools that guarantee not only pedagogical functionality, but also the protection of users' personal data, complying with legal requirements related to privacy". The need for educational tools not only to fulfill their pedagogical role, but also to respect data privacy and security regulations, creating a safe learning environment, is highlighted.

In addition, schools must adopt clear policies for the use of technologies, which establish guidelines to ensure that the devices and systems used in the educational environment are protected against vulnerabilities. According to Santos (2024, p. 45), "digital security policies in schools should involve the creation of clear standards for the use of technologies, covering everything from access to platforms to the use of data, in order to ensure that everyone involved in the educational process understands their responsibilities in the safe use of these tools". The implementation of these policies is essential for all members of the school community — students, teachers, and managers — to understand the importance of digital security and know how to adopt responsible behaviors.

Another relevant aspect to ensure digital security in schools is the implementation of security protocols in the school network, which aim to protect the information stored and shared within the institution. According to Araújo and Silva (2022, p. 186), "the implementation of security protocols, such as data encryption and user authentication, is essential to ensure that the sensitive information of students and teachers is protected against unauthorized access". The adoption of these protocols not only minimizes the risks of data leakage but also contributes to the creation of a school culture that prioritizes digital security.

Therefore, the adoption of educational platforms and software focused on security, the creation of clear policies for the use of technologies, and the implementation of strict security protocols are essential to protect data and ensure a safe digital educational environment. These strategies help to promote responsible and safe use of technologies in schools, ensuring that the privacy and security of those involved are preserved.

METHODOLOGY

The methodology used in this research is characterized as a literature review, with the objective of analyzing the main concepts and debates on digital security and privacy in education. The type of research is qualitative, since it seeks to understand the issues related to security and privacy in the use of technologies in educational environments. The approach adopted was descriptive, since the research proposes to explore, through the literature review, the challenges faced by schools in the use of technologies and the impacts on the data protection of students and educators. For data collection, academic articles, dissertations, books, book chapters and documents from recognized sources in the area of education and digital security were selected. The search was carried out in scientific databases such as Google *Scholar*, *Scielo*, and Capes Journal Portal, using keywords related to the theme, such as "digital security in education", "privacy in education" and "technologies and education". The technique used for data analysis was the reading and critical analysis of the selected sources, which were organized and systematized to identify the main challenges, solutions and contributions to the study area.

The research resulted in a table that presents the bibliographic references used, organized according to the descriptors of author(s), title, year and type of work. The following table facilitates the visualization of the sources consulted and the organization of the main academic contributions that support the proposed discussion.

Chart 1: Bibliographic References Used in the Research

Author(s)	Conforming title published	Year	Type of work
RABAY, G.; NEVES, K.	Perception of privacy and security in the use of the Internet by students of technological education at CEFET in Nepomuceno.	2017	Event proceedings
ARAÚJO, V. S.	Teacher training for the critical teaching of the Portuguese language: an experience in the pedagogy course through the 'Blackboard' platform.	2020	Dissertation (Master's Degree in Language, Literature and Interculturality)
ARAÚJO, V. S.; LOPES, C. R.	Conceptions of critical training of teachers in university education.	2020	Book Chapter
NETO, J. N. A.; QUINTINO, A. S. de S.	The invasion of hackers in educational management: a study on data preservation in remote teaching in the light of digital security.	2021	Event proceedings
ARAÚJO, V. S.; SILVA, N. N.	Reading in the formation of the citizen in the light of critical literacy.	2022	Book Chapter
OLIVEIRA, V. B.; VAZ, D. A. F.	Physical and mental health of teachers in the remote teaching period in public schools in Goiás.	2022	Book Chapter
OLIVEIRA, V. B.	Discussions of evaluation practices in ninth grade classes of elementary school in a state public school in Goiânia and the teachers' testimonies from the perspective of historical-cultural conceptions.	2023	Dissertation (Master's Degree in Education)
SANTOS, D. S. dos; BARROS, A. M. R.	Technologies, citizenship and education: strategies to deal with the risks of digital practices in school institutions.	2023	Journal article
CARVALHO JÚNIOR, P. C. de	Digital law and its applications: privacy violation, data protection and remedy measures.	2024	Journal article
NARCISO, R.; SILVA, A. A. U.; BARROS, A. M. R.	Ethics and privacy in digital education: the ethical and privacy challenges in the use of digital technologies.	2024	Journal article
SAINTS, S. M. A. V.; Frank, A. S. (orgs.)	Media and technology in the curriculum: innovative strategies for contemporary teacher training.	2024	Book Organization
REIS, S. R. F.; REIS, T. S. M.; ALMEIDA, G. L. de; JÚNIOR, T. A. F.	Challenges of the LGPD regarding privacy in educational environments: a systematic mapping.	2024	Journal article
SANTOS, S. M. A. V. (org.)	Education 4.0: management, inclusion and technology in the construction of innovative curricula.	2024	Book Organization
SANTOS, S. M. A. V. (org.)	Education in the XXI century: interdisciplinary and technological approaches.	2024	Book Organization
SANTOS, S. M. A. V. (org.)	Integral inclusion: contemporary challenges in education and society.	2024	Book Organization
SAINTS, S. M. A. V.; Frank, A. S. (orgs.)	Educational innovation: emerging practices in the twenty-first century.	2024	Book Organization
SILVA, A. P. da.	Digital security x digital citizenship: concepts and relations with education in the twenty-first century.	2024	Journal article

Source: authorship.

After the presentation of the table, it can be observed that the selected sources cover a variety of approaches on the topic of digital security and privacy in education. The references range from discussions on data protection legislation and policies to studies that

address pedagogical practices related to the safe use of technologies in the school environment. From this framework, it is possible to understand the main issues raised by the literature about the use of technologies in educational environments and the implications for the privacy and digital security of those involved.

IMPACTS OF THE LACK OF DIGITAL SECURITY IN SCHOOLS

The lack of digital security in schools can result in serious consequences for students and educators, putting the privacy and integrity of data shared across educational platforms and systems at risk. The exposure of personal information, such as academic data and contact information, can be used in, affecting both trust in the school environment and the well-being of the people involved. According to Oliveira (2023, p. 115), "the vulnerability of schools to cyberattacks compromises not only data security, but also the relationship of trust between educators, students, and the institution, making it difficult to build a safe learning environment". This reflection highlights how the lack of adequate protection measures can undermine mutual trust, a fundamental aspect in the educational process.

In addition to the emotional and institutional implications, the consequences of a lack of digital security can be tangible and financial in the event of a data breach. Araújo and Silva (2022, p. 190) highlight that "the lack of adequate security in school networks can result in cyber attacks, such as the theft of sensitive information or the introduction of malware into systems, which can cause irreversible damage to the technological infrastructures of institutions". The analysis reveals that the absence of security protocols can lead to significant material losses, such as the corruption of school data, in addition to affecting the continuity of the teaching and learning process.

Real cases of data breaches in schools show how the lack of digital security can have dramatic consequences. As an example, Santos and Barros (2023) report that in several educational institutions, *ransomware* attacks compromise not only administrative systems, but also affect the privacy of students and educators, exposing personal information without consent. Cases like this illustrate the severity of security breaches, which can result in long-term negative impacts for both the affected individuals and the institution's reputation.

Therefore, the absence of digital security in schools can lead to a series of adverse effects, including damage to trust, institutional reputation, and the protection of personal data. Schools need to implement measures to protect student and educator data in order to

avoid the risks associated with exposing sensitive information and ensure a safe and efficient teaching environment.

THE INFLUENCE OF PUBLIC POLICIES ON SCHOOL DIGITAL SAFETY

Digital security in schools does not depend only on internal actions, but also on the implementation of public policies that guide educational institutions in creating safe environments in the use of technologies. The analysis of public digital security policies reveals how they shape the way schools approach the protection of student and educator data. As Santos (2024) points out, public digital security policies play a fundamental role in creating a secure infrastructure, establishing guidelines that must be followed by schools, including data protection and education for the responsible use of technologies. The importance of public policies is highlighted, which should serve as a basis for the implementation of practices and systems that guarantee privacy and security in schools.

In addition, the government and educational institutions have joint responsibilities in protecting the personal and academic data of those involved in the educational process. According to Araújo and Silva (2022), it is imperative that the government provides the necessary support for schools to implement adequate digital security policies, such as the creation of specific regulations for the use of educational technologies and the definition of protocols for the management of sensitive data. This perception reinforces that, in addition to the responsibility of schools, there is a requirement from the government to ensure that institutions follow appropriate practices that protect the data of students and educators, creating a safety net for the entire school community.

The role of government goes beyond creating regulations; It also involves monitoring compliance with digital security policies in schools, ensuring that institutions implement the necessary measures to protect sensitive information. According to Santos and Barros (2023), the implementation of public policies depends on continuous inspection, which ensures that schools are complying with the established standards and adapting to the new needs and challenges of digital security. This monitoring and inspection are essential to ensure that public policies are not only created, but also put into practice, ensuring digital safety in the school environment.

Therefore, public digital security policies have a significant impact on the way schools approach data protection and *online* security. Government and educational institutions need to work together to create and implement regulations that ensure the

security and privacy of student and educator data, ensuring the creation of safe and responsible learning environments.

THE FUTURE OF DIGITAL EDUCATION: CHALLENGES AND OPPORTUNITIES

The future of digital education presents both challenges and opportunities, as new technologies emerge and are incorporated into the school environment. Trends such as education 4.0, the use of artificial intelligence, and collaborative tools promise to transform pedagogical practices and, at the same time, require a greater focus on digital security. As Santos (2024, p. 82) points out, "emerging trends, such as education 4.0 and the use of collaborative tools, offer new ways of learning, but also impose new challenges with regard to the security and privacy of student data". The argument highlights the necessary balance between innovation in education and data protection, as advanced technologies can make schools vulnerable to cyber risks, especially when security measures are not adequate.

In addition to collaborative tools, artificial intelligence (AI) emerges as a significant innovation in digital education, offering new ways to personalize learning and optimize the use of pedagogical resources. However, the integration of AI also requires care regarding data security. As Araújo e Silva (2022, p. 188) points out, "artificial intelligence has the potential to revolutionize education, but it is necessary to ensure that the use of data for personalization of teaching is done with total transparency and respect for student privacy". The need for clear regulations that protect student privacy is highlighted, especially when technologies such as AI are used to collect and analyze large volumes of personal data.

Education 4.0, characterized by the integration of technologies such as AI, big data, and the Internet of Things (IoT), also requires a careful approach to digital security. According to Oliveira (2023, p. 115), "with the advent of education 4.0, schools must implement solutions to protect data and ensure that the use of these new technologies is safe for everyone involved". This education model, which is based on interactivity and personalization of teaching through technologies, implies that student data is treated with maximum security, to prevent leaks or abuse of information.

Therefore, the future of digital education brings with it both opportunities and challenges when it comes to digital security. The use of emerging technologies, such as AI and collaborative tools, presents vast potential to improve the quality of education, but at the same time requires significant investment in security protocols and privacy policies. The

way schools deal with these issues will be decisive for the success of digital education, creating safe and innovative learning environments.

FINAL CONSIDERATIONS

The conclusions of this study were based on the analysis of digital security and privacy in the use of technologies in school environments, focusing on the main difficulties faced by schools to implement secure practices and protect student and educator information. The main finding of the research was the identification of significant barriers, such as the lack of adequate training for educators and resistance to change in educational institutions. These difficulties impact the effectiveness of digital security policies, generating vulnerabilities in systems and processes that should ensure the protection of personal and academic data. In addition, the survey pointed out that public policies for digital security, although essential, need to be well implemented and closely monitored, both by the government and by school institutions.

The central question of the research, which involved the analysis of the challenges in the use of digital technologies in schools, was answered from the observation that, despite the growing adoption of technologies, the implementation of security practices remains a constant challenge. The study showed that, in many schools, the lack of infrastructure and the lack of preparation of education professionals to deal with digital security issues compromise the protection of student data. This, in turn, can lead to a range of consequences, such as the leakage of personal information and the compromise of trust between students, parents, and educators. Therefore, it is essential that schools adopt a set of strategies to overcome these obstacles, such as the continuous training of teachers, the implementation of public policies, and the adoption of strict safety protocols.

The contributions of this study are significant for understanding the challenges faced by schools in the implementation of digital security. It provides a reflection on the relevance of integrating educational technologies in a secure way, highlighting the need to ensure data privacy and protection against cyber threats. In addition, the study reinforces the importance of public policies that establish clear standards for the safe use of technologies in the school environment, in addition to the implementation of awareness and training programs for all those involved in the educational process. By providing an overview of the obstacles and possible solutions, this work contributes to the discussion on how schools can improve digital security and ensure the privacy of all their members.

However, it is essential to highlight that the research also revealed that many of these problems still lack effective and sustainable solutions, which indicates the need for studies that complement the findings of this work. The implementation of digital security policies, as well as the continuous training of educators, needs to be better monitored and adapted to the reality of schools. It would be interesting for future research to investigate how schools are dealing with technological changes in a practical way, identifying cases of success and failure in the implementation of these policies. It would also be relevant to analyze the impact of these digital security practices on student performance and the quality of teaching, since trust in the school environment and data security are fundamental factors for good academic and personal development.

Therefore, this study offers an important starting point for understanding the challenges of digital security in schools, but also points to the need for continuous advances, both in public policies and in the training of education professionals. The issue of digital security in schools must be treated as a priority, as the protection of student and educator data is essential to ensure a safe teaching environment.

REFERENCES

1. Araújo, V. S. (2020). Formação de professoras para o ensino crítico de língua portuguesa: uma experiência no curso de pedagogia por meio da plataforma “Blackboard” (Dissertação de Mestrado). Câmpus Cora Coralina, Universidade Estadual de Goiás, Goiás, GO. Disponível em: https://www.bdttd.ueg.br/bitstream/tede/786/2/VITOR_SAVIO_DE_ARAUJO.pdf. Acesso em: 27 nov. 2024.
2. Araújo, V. S., & Lopes, C. R. (2020). Concepções de formação crítica de professoras em formação universitária. In E. B. Silva & R. B. Gonçalves (Orgs.), Recortes linguísticos sob uma perspectiva intercultural (pp. 81-88). Maringá, PR: Uniedusul. Disponível em: <https://abrir.link/ATCOo>. Acesso em: 27 nov. 2024.
3. Araújo, V. S., & Silva, N. N. (2022). A leitura na formação do cidadão à luz do letramento crítico. In M. G. Avelar, C. C. Freitas, & C. R. Lopes (Orgs.), Linguagens em tempos inéditos: desafios praxiológicos da formação e professoras/es de línguas: volume dois (v. 2, pp. 187-203). Goiânia: Scotti. Disponível em: <https://abrir.link/wjpPA>. Acesso em: 27 nov. 2024.
4. Carvalho Júnior, P. C. de, [...]. (2024). Direito digital e suas aplicações: a violação de privacidade, a proteção de dados e medidas de solução. Revista [...]. Disponível em: <https://periodicorease.pro.br/rease/article/view/16960>. Acesso em: 27 nov. 2024.
5. Narciso, R., Silva, A. A. U., & Barros, A. M. R. (2024). Ética e privacidade na educação digital: os desafios éticos e de privacidade no uso de tecnologias digitais. Revista [...]. Disponível em: <https://ojs.focopublicacoes.com.br/foco/article/view/4123>. Acesso em: 27 nov. 2024.
6. Neto, J. N. A., & Quintino, A. S. de S. (2021). A invasão de hackers na gestão educacional: um estudo sobre a preservação de dados no ensino remoto à luz da segurança digital. Anais do Encontro [...]. Disponível em: <https://ciltec.textolivre.pro.br/index.php/CILTecOnline/article/view/734>. Acesso em: 27 nov. 2024.
7. Oliveira, V. B. (2023). Discussões das práticas avaliativas em turmas do nono ano do ensino fundamental de uma escola pública estadual de Goiânia e os depoimentos dos docentes sob o olhar das concepções de cunho histórico-cultural (Dissertação de Mestrado). Escola de Formação de Professores e Humanidades, Pontifícia Universidade Católica de Goiás, Goiânia. Disponível em: <https://tede2.pucgoias.edu.br/handle/tede/4960>. Acesso em: 27 nov. 2024.
8. Oliveira, V. B., & Vaz, D. A. F. (2022). Saúde física e mental do professor no período remoto de ensino nas escolas públicas de Goiás. In D. A. F. Vaz, E. A. S. Ávila, & M. M. M. Oliveira (Orgs.), Temas Educacionais na Cultura Digital: novas leituras em tempo de pandemia (pp. 75-78). São Carlos: Pedro & João Editores. Disponível em: <https://pedroejoaoeditores.com.br/wp-content/uploads/2022/05/Cultura-Digital.pdf#page=76>. Acesso em: 27 nov. 2024.

9. Rabay, G., & Neves, K. (2017). Percepção da privacidade e da segurança no uso da Internet por alunos do ensino tecnológico no CEFET de Nepomuceno. 27^a Mostra Específica de Trabalhos e [...]. Disponível em: <https://www.conferencias.cefetmg.br/index.php/27META/27META/paper/view/4013>. Acesso em: 27 nov. 2024.
10. Reis, S. R. F., Reis, T. S. M., Almeida, G. L. de, & Júnior, T. A. F. (2024). Desafios da LGPD quanto à privacidade em ambientes educacionais: um mapeamento sistemático. Revista de Gestão e [...]. Disponível em: <https://ojs.revistagesec.org.br/secretariado/article/view/3292>. Acesso em: 27 nov. 2024.
11. Santos, D. S. dos, & Barros, A. M. R. (2023). Tecnologias, cidadania e educação: estratégias para lidar com os riscos das práticas digitais nas instituições escolares. Revista Amor [...]. Disponível em: <https://journal.editorametrics.com.br/index.php/amormundi/article/view/290>. Acesso em: 27 nov. 2024.
12. Santos, S. M. A. V. (Org.). (2024). Educação 4.0: gestão, inclusão e tecnologia na construção de currículos inovadores. São Paulo: Editora Arché. ISBN 978-65-6054-098-9. Acesso em: 27 nov. 2024.
13. Santos, S. M. A. V. (Org.). (2024). Educação no século XXI: abordagens interdisciplinares e tecnológicas. São Paulo: Editora Arché. ISBN 978-65-6054-130-6. Acesso em: 27 nov. 2024.
14. Santos, S. M. A. V. (Org.). (2024). Inclusão integral: desafios contemporâneos na educação e sociedade. São Paulo: Editora Arché. ISBN 978-65-6054-112-2. Acesso em: 27 nov. 2024.
15. Santos, S. M. A. V., & Franqueira, A. S. (Orgs.). (2024). Inovação educacional: práticas surgentes no século XXI. São Paulo: Editora Arché. ISBN 978-65-6054-120-7. Acesso em: 27 nov. 2024.
16. Santos, S. M. A. V., & Franqueira, A. S. (Orgs.). (2024). Mídias e tecnologia no currículo: estratégias inovadoras para a formação docente contemporânea. São Paulo: Editora Arché. ISBN 978-65-6054-106-1. Acesso em: 27 nov. 2024.
17. Silva, A. P. da. (2024). Segurança digital x cidadania digital: conceitos e relações com a educação do século XXI. Tecnologias [...]. Disponível em: https://www.researchgate.net/profile/Alberto-Franqueira/publication/372737753_EDUCACAO_E_AS_NOVAS_TECNOLOGIAS/link/s/663956ed352430415367a2d4/EDUCACAO-E-AS-NOVAS-TECNOLOGIAS.pdf#page=33. Acesso em: 27 nov. 2024.