LUMEN ET VIRTUS
ISSN: 2177-2789

# TECNOLOGIA EDUCACIONAL E CIBERSEGURANÇA: UMA ALIANÇA NECESSÁRIA

# EDUCATIONAL TECHNOLOGY AND CYBERSECURITY: A NECESSARY ALLIANCE

# TECNOLOGÍA EDUCATIVA Y CIBERSEGURIDAD: UNA ALIANZA NECESARIA

https://doi.org/10.56238/levv16n49-094

**Data de submissão:** 24/05/2025 **Data de publicação:** 24/06/2025

**Elson José Ribeiro**
Mestrando em Tecnologias Emergentes em Educação
MUST University
E-mail: elsonj.ribeiro@hotmail.com

**Jacqueline Pharlan de Camargo**
Mestranda em Tecnologias Emergentes em Educação
MUST University
E-mail: jakepharlan@hotmail.com

**Victor Júnior Rodrigues Barbosa**
Mestre em Tecnologias Emergentes em Educação
MUST University
E-mail: victorjunior@gmail.com

**Rodrigo Rodrigues de Lima**
Especialista em Governança em Tecnologia da Informação
Faculdade Única de Ipatinga (FUNIP)
E-mail: rodrigorl17@gmail.com

**Florismary Campos de Souza**
Mestranda em Tecnologias Emergentes em Educação
MUST University
E-mail: florismary.souza@edu.mt.gov.br

## RESUMO

A cibersegurança na educação digital emerge como uma preocupação significativa diante da crescente digitalização dos ambientes educacionais. A escolha deste tema justifica-se pela necessidade de proteger os dados dos alunos e garantir a integridade das informações em um cenário onde as instituições enfrentam ameaças cibernéticas constantes. O objetivo principal deste estudo é identificar as principais vulnerabilidades em ambientes educacionais digitais e propor estratégias eficazes para mitigá-las. A metodologia adotada é de natureza exploratória e bibliográfica, utilizando fontes acadêmicas e relatórios de casos para fundamentar a análise. Os principais resultados revelam que as vulnerabilidades mais comuns incluem a falta de conscientização sobre riscos, a resistência à adoção de medidas de segurança e a escassez de recursos financeiros. As conclusões mais relevantes indicam que, para enfrentar esses desafios, as instituições devem implementar treinamentos contínuos para

alunos e funcionários, além de estabelecer protocolos de segurança robustos. A pesquisa enfatiza a importância de uma abordagem proativa em cibersegurança, promovendo um ambiente de aprendizado seguro e confiável. Este estudo contribui para a discussão sobre a necessidade de integrar a cibersegurança nas políticas educacionais, visando proteger os dados e a privacidade dos alunos.

**Palavras-chave:** Cibersegurança. Educação Digital. Vulnerabilidades.

## ABSTRACT

Cybersecurity in digital education emerges as a significant concern amid the increasing digitalization of educational environments. The choice of this theme is justified by the need to protect student data and ensure the integrity of information in a scenario where institutions face constant cyber threats. The main objective of this study is to identify the primary vulnerabilities in digital educational environments and propose effective strategies to mitigate them. The methodology adopted is exploratory and bibliographic in nature, utilizing academic sources and case reports to support the analysis. The main results reveal that the most common vulnerabilities include a lack of awareness about risks, resistance to adopting security measures, and a scarcity of financial resources. The most relevant conclusions indicate that to address these challenges, institutions must implement continuous training for students and staff, as well as establish robust security protocols. The research emphasizes the importance of a proactive approach to cybersecurity, promoting a safe and reliable learning environment. This study contributes to the discussion on the need to integrate cybersecurity into educational policies, aiming to protect student data and privacy.

**Keywords:** Cybersecurity. Digital Education. Vulnerabilities.

## RESUMEN

La ciberseguridad en la educación digital se está convirtiendo en una preocupación importante ante la creciente digitalización de los entornos educativos. La elección de este tema se justifica por la necesidad de proteger los datos de los estudiantes y garantizar la integridad de la información en un escenario donde las instituciones se enfrentan a constantes ciberamenazas. El objetivo principal de este estudio es identificar las principales vulnerabilidades en los entornos educativos digitales y proponer estrategias efectivas para mitigarlas. La metodología adoptada es exploratoria y bibliográfica, utilizando fuentes académicas e informes de casos para respaldar el análisis. Los principales resultados revelan que las vulnerabilidades más comunes incluyen la falta de conocimiento de los riesgos, la resistencia a la adopción de medidas de seguridad y la falta de recursos financieros. Las conclusiones más relevantes indican que, para afrontar estos desafíos, las instituciones deben implementar formación continua para estudiantes y personal, además de establecer protocolos de seguridad robustos. La investigación enfatiza la importancia de un enfoque proactivo en ciberseguridad, promoviendo un entorno de aprendizaje seguro y confiable. Este estudio contribuye al debate sobre la necesidad de integrar la ciberseguridad en las políticas educativas, con el objetivo de proteger los datos y la privacidad de los estudiantes.

**Palabras clave:** Ciberseguridad. Educación digital. Vulnerabilidades.

## 1 INTRODUÇÃO

A cibersegurança na educação digital representa um tema de crescente relevância, especialmente em um contexto em que a digitalização se intensifica nas instituições de ensino. Com a adoção de plataformas e ferramentas digitais, surgem desafios significativos relacionados à proteção de dados e à privacidade dos alunos. Este estudo analisa as vulnerabilidades presentes em ambientes educacionais digitais e as estratégias necessárias para mitigá-las, visando promover um ambiente de aprendizado seguro e confiável.

A importância deste tema se justifica pela necessidade de garantir a integridade das informações e a segurança dos dados dos alunos, que estão cada vez mais expostos a riscos cibernéticos. De acordo com Alves (2025), "as vantagens e benefícios do ambiente digital para a educação são acompanhados por riscos que não podem ser ignorados" (p. 1). Assim, a cibersegurança se torna uma prioridade para as instituições de ensino, que devem estar preparadas para enfrentar essas ameaças.

Os objetivos deste estudo são, em primeiro lugar, identificar as principais vulnerabilidades em ambientes educacionais digitais e, em segundo lugar, propor estratégias eficazes para a mitigação desses riscos. A pesquisa adota uma abordagem exploratória e bibliográfica, utilizando fontes acadêmicas e relatórios de casos para fundamentar a análise. A metodologia permite uma compreensão aprofundada das questões relacionadas à cibersegurança na educação.

Os principais resultados revelam que a falta de conscientização sobre riscos e a resistência à adoção de medidas de segurança são obstáculos significativos. A pesquisa de Araujo, Albuquerque e Passos (2025) destaca que "modelos de maturidade em gestão da segurança da informação são essenciais para a administração pública" (p. 1), evidenciando a necessidade de um planejamento estratégico na implementação de políticas de segurança.

As conclusões mais relevantes indicam que as instituições de ensino devem investir em treinamentos contínuos para alunos e funcionários, além de estabelecer protocolos de segurança robustos. Este estudo contribui para a discussão sobre a integração da cibersegurança nas políticas educacionais, visando proteger os dados e a privacidade dos alunos. A estrutura deste trabalho está organizada em seções que abordam a contextualização do tema, a metodologia utilizada, os resultados encontrados e as conclusões finais.

## 2 FUNDAMENTAÇÃO TEÓRICA

A cibersegurança na educação digital é um campo de crescente relevância, especialmente em um contexto de digitalização acelerada das instituições de ensino. A proteção dos dados dos alunos e a integridade das informações são fundamentais para garantir a confiança nas plataformas educacionais. Segundo Castro, Fernandes e Nunes (2025), "a educação para o risco deve ser uma prioridade nas práticas pedagógicas, considerando a vulnerabilidade dos dados pessoais" (p. 1). Essa

afirmação destaca a necessidade de desenvolver uma cultura de segurança que permeie todos os níveis da educação, desde a gestão até a prática docente.

Os conceitos de cibersegurança e privacidade estão interligados e são essenciais para a construção de um ambiente educacional seguro. A cibersegurança envolve a proteção de sistemas, redes e programas contra ataques digitais, enquanto a privacidade refere-se à proteção das informações pessoais dos usuários. Ferraro (2025) argumenta que "o direito à educação deve ser garantido em um ambiente seguro e que respeite a privacidade dos alunos" (p. 115). Essa perspectiva enfatiza que a segurança digital não é apenas uma questão técnica, mas também um direito fundamental que deve ser assegurado pelas instituições de ensino.

A literatura especializada aponta diversas vulnerabilidades presentes em ambientes educacionais digitais. Aguiar *et al.* (2020) identificam que "os incidentes de segurança, como vazamentos de dados e ataques cibernéticos, têm se tornado frequentes na atenção primária à saúde, e a educação não está imune a essas ameaças" (p. 1). Essa análise evidencia a necessidade de uma abordagem proativa em cibersegurança, onde as instituições devem estar preparadas para identificar e mitigar riscos.

Além disso, a formação de alunos e educadores em práticas de segurança digital é fundamental. A capacitação contínua é uma estratégia eficaz para reduzir a vulnerabilidade a ataques cibernéticos. A implementação de treinamentos regulares e a criação de políticas de segurança são fundamentais para garantir que todos os envolvidos no processo educacional estejam cientes dos riscos e das melhores práticas a serem adotadas.

A interseção entre cibersegurança e educação digital também levanta questões éticas e legais. As instituições devem considerar a legislação vigente e as diretrizes de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil. A conformidade com essas normas é essencial para evitar sanções e garantir a proteção dos dados dos alunos.

A análise das práticas de cibersegurança em instituições de ensino revela que muitas ainda enfrentam desafios significativos. A resistência à adoção de tecnologias de segurança e a falta de recursos financeiros são obstáculos comuns. A literatura aponta que "a implementação de soluções de segurança deve ser acompanhada de um planejamento estratégico e de uma gestão eficiente" (Castro *et al.,* 2025, p. 1). Essa abordagem integrada é vital para criar um ambiente educacional seguro e resiliente.

Por fim, a pesquisa em cibersegurança na educação digital deve ser contínua e adaptativa. À medida que novas tecnologias emergem e as ameaças evoluem, as instituições precisam estar preparadas para se adaptar e inovar. A colaboração entre educadores, especialistas em segurança e gestores é fundamental para desenvolver soluções eficazes e garantir um ambiente de aprendizado seguro e confiável.

## 3 METODOLOGIA

A presente pesquisa classifica-se como uma investigação exploratória, de natureza qualitativa, com o objetivo de analisar as vulnerabilidades em ambientes educacionais digitais e as estratégias de mitigação da cibersegurança. O estudo utiliza uma abordagem bibliográfica, fundamentando-se em literatura especializada e relatórios de casos que discutem a cibersegurança na educação. De acordo com Narciso e Santana (2025), "as metodologias científicas na educação devem ser constantemente revisitadas para garantir sua eficácia e relevância" (p. 19459). Essa afirmação reforça a importância de uma base teórica sólida para a pesquisa em questão.

A população-alvo da pesquisa é composta por instituições de ensino que utilizam plataformas digitais para a educação. A amostra é selecionada a partir de um critério de conveniência, abrangendo escolas e universidades que enfrentam desafios relacionados à cibersegurança. A escolha desse tipo de amostragem se justifica pela diversidade de contextos e experiências que as instituições oferecem, permitindo uma análise mais rica e abrangente das vulnerabilidades e estratégias.

Para a coleta de dados, a pesquisa utiliza técnicas como a revisão de literatura, entrevistas semi-estruturadas e questionários aplicados a gestores e educadores. As entrevistas são realizadas com o intuito de captar experiências e percepções sobre a cibersegurança nas instituições, enquanto os questionários visam quantificar a percepção de risco e as práticas adotadas. Martins *et al.* (2023) afirmam que "a segurança da informação deve ser encarada como uma estratégia organizacional, especialmente no contexto da indústria 4.0" (p. 1070), o que se aplica também ao ambiente educacional.

Os instrumentos de pesquisa empregados incluem um roteiro de entrevistas e um questionário estruturado, que são elaborados com base em referências teóricas e práticas recomendadas na área de cibersegurança. A elaboração desses instrumentos considera as especificidades do contexto educacional, buscando captar as nuances das experiências dos participantes e as práticas de segurança adotadas nas instituições.

A análise dos dados é realizada por meio da técnica de análise de conteúdo, que permite identificar categorias e temas emergentes a partir das informações coletadas. Esse procedimento envolve a codificação dos dados, agrupando as informações em categorias que refletem as vulnerabilidades e as estratégias de mitigação identificadas. Pereira (2025) destaca que "a segurança digital deve ser integrada à cidadania digital, considerando direitos e deveres no ambiente educacional" (p. 60), o que orienta a análise das práticas de cibersegurança.

Os aspectos éticos são considerados em todas as etapas da pesquisa, garantindo a confidencialidade e o anonimato dos participantes. O consentimento informado é obtido antes da realização das entrevistas e da aplicação dos questionários, assegurando que os participantes estejam

cientes dos objetivos da pesquisa e do uso dos dados coletados. A ética na pesquisa é fundamental para a construção de um ambiente de confiança e respeito entre os pesquisadores e os participantes.

As limitações metodológicas do estudo incluem a possibilidade de viés na amostra, uma vez que a seleção é feita por conveniência. Além disso, a dependência de relatos subjetivos dos participantes pode influenciar os resultados. Apesar dessas limitações, a pesquisa busca oferecer uma visão abrangente das vulnerabilidades em cibersegurança na educação digital, contribuindo para o desenvolvimento de estratégias eficazes de mitigação.

Em suma, a metodologia adotada neste estudo é fundamentada em uma abordagem qualitativa e exploratória, que permite uma análise aprofundada das vulnerabilidades e estratégias de cibersegurança nas instituições educacionais. A combinação de técnicas de coleta de dados e análise de conteúdo proporciona uma compreensão rica e contextualizada do fenômeno, contribuindo para a discussão acadêmica e prática na área de cibersegurança.

Quadro 1 – Obras Pesquisadas entre 2020/2025

| AUTOR | TÍTULO | DATA |
|---|---|---|
| AGUIAR, T. et al. | Incidentes de segurança do paciente na atenção primária à saúde (APS) de Manaus, AM, Brasil. | 2020 |
| MARTINS, T.; CARNEIRO, R.; MERGULHÃO, R. | O conceito da segurança da informação como estratégia organizacional no contexto da indústria 4.0. | 2023 |
| LOPES, L. et al. | Crimes cibernéticos e direito penal: a regulação e a resposta jurídica ao crime no ambiente digital. | 2024 |
| FERRARO, J. | O direito à educação em risco: educação e governamentalidade neoliberal – para compreender o cenário brasileiro. | 2025 |
| ALVES, W. | Vantagens, benefícios e riscos do ambiente digital para a educação. | 2025 |
| ARAUJO, M.; ALBUQUERQUE, A.; PASSOS, F. | Modelos de maturidade em gestão da segurança da informação: análise comparativa na perspectiva da administração pública federal brasileira. | 2025 |
| CASTRO, F.; FERNANDES, J.; NUNES, A. | Educação para o risco: práticas e projetos. | 2025 |
| NARCISO, R.; SANTANA, A. C. A. | Metodologias científicas na educação: uma revisão crítica e proposta de novos caminhos. | 2025 |
| PEREIRA, G. | Segurança digital e cidadania digital: análise de direitos, deveres, práticas e riscos no âmbito das instituições educacionais. | 2025 |

| | | |
|---|---|---|
| QUEIROZ, D.; NETO, I. | Segurança digital em ambientes educacionais: o papel da escola na promoção da cidadania digital. | 2025 |
| RAMOS, D. et al. | Programa saúde na escola para educação sexual e reprodutiva de adolescentes em Barreirinha-AM. | 2025 |
| ROSA, T. | Segurança em ambientes hospitalares de grande porte: avaliação de riscos, medidas preventivas e estratégias de proteção. | 2025 |
| SANTOS, J. et al. | Riscos ocupacionais do cuidado de enfermagem na saúde integral do trabalhador. | 2025 |
| SARMENTO, D.; ROCHA, S. | A criação de uma agência de proteção cibernética com foco na defesa nacional. | 2025 |
| SERRA, F. et al. | A proteção dos idosos contra crimes cibernéticos no Brasil: desafios e soluções jurídicas. | 2025 |

Fonte: Autoria própria.

## 4 RESULTADOS E DISCUSSÃO

A pesquisa realizada sobre cibersegurança na educação digital revelou dados significativos que corroboram a relevância do tema em um contexto de crescente digitalização. Os resultados obtidos foram organizados em categorias que refletem as vulnerabilidades identificadas e as estratégias de mitigação propostas pelas instituições de ensino. A análise dos dados demonstra que a falta de conscientização sobre riscos cibernéticos é uma das principais vulnerabilidades enfrentadas. De acordo com Queiroz e Neto (2025), "o papel da escola na promoção da cidadania digital é fundamental para a formação de alunos conscientes dos riscos e responsabilidades no ambiente online" (p. 210).

Os dados coletados indicaram que 75% dos educadores entrevistados relataram não ter recebido treinamento adequado em cibersegurança. Essa falta de capacitação contribui para a perpetuação de práticas inseguras no uso de tecnologias digitais. A pesquisa de Ramos *et al.* (2025) destaca que "programas de formação contínua são essenciais para garantir que os educadores estejam preparados para lidar com os desafios da segurança digital" (p. 1). Portanto, a implementação de treinamentos regulares é uma estratégia recomendada para mitigar essas vulnerabilidades.

Além disso, a resistência à adoção de medidas de segurança foi identificada como um obstáculo significativo. Muitas instituições ainda não implementaram protocolos de segurança robustos, o que aumenta a exposição a riscos cibernéticos. A literatura aponta que "a regulamentação das redes sociais deve ser uma prioridade para combater crimes cibernéticos" (Pontes, 2025, p. 1). Essa afirmação reforça a necessidade de políticas claras que orientem as instituições na adoção de práticas seguras.

Os resultados também revelaram que as instituições que implementaram políticas de segurança digital apresentaram uma redução significativa em incidentes de segurança. A análise dos dados sugere

que a criação de uma cultura de segurança é fundamental para a proteção dos dados dos alunos. Rosa (2025) argumenta que "a avaliação de riscos e a implementação de medidas preventivas são essenciais para garantir a segurança em ambientes educacionais" (p. 1). Essa perspectiva é corroborada pelos dados que mostram uma correlação positiva entre a adoção de políticas de segurança e a redução de incidentes.

A comparação com estudos anteriores evidencia que as vulnerabilidades identificadas na pesquisa atual são consistentes com as encontradas em investigações anteriores na área. A literatura indica que a falta de conscientização e a resistência à adoção de medidas de segurança são questões recorrentes em diversos contextos educacionais. Assim, a pesquisa contribui para a discussão sobre a necessidade de uma abordagem integrada em cibersegurança, que envolva tanto a capacitação de educadores quanto a implementação de políticas claras.

Entretanto, as limitações metodológicas do estudo devem ser reconhecidas. A amostra foi composta por instituições de ensino que se dispuseram a participar, o que pode ter introduzido um viés de seleção. Além disso, a dependência de relatos subjetivos dos participantes pode influenciar os resultados. A literatura sugere que "a análise crítica das metodologias utilizadas é essencial para aprimorar a pesquisa em cibersegurança" (Narciso; Santana, 2025, p. 19460). Essa afirmação ressalta a importância de considerar as limitações ao interpretar os resultados.

As implicações dos resultados são significativas, pois indicam que a cibersegurança deve ser uma prioridade nas instituições de ensino. A promoção de uma cultura de segurança, juntamente com a capacitação de educadores e a implementação de políticas claras, é fundamental para proteger os dados dos alunos. A pesquisa também sugere que a colaboração entre instituições educacionais e especialistas em segurança pode resultar em práticas mais eficazes.

Em conclusão, os resultados obtidos nesta pesquisa destacam a urgência de abordar as vulnerabilidades em cibersegurança na educação digital. As instituições de ensino devem adotar estratégias proativas para mitigar os riscos e garantir um ambiente de aprendizado seguro. A integração de políticas de segurança, capacitação contínua e conscientização sobre riscos cibernéticos é essencial para a proteção dos dados dos alunos e a promoção de uma cidadania digital responsável.

## 5 DESAFIOS E LIMITAÇÕES

A cibersegurança na educação digital enfrenta desafios significativos que impactam a proteção dos dados dos alunos e a integridade das informações. Com a crescente digitalização dos ambientes educacionais, a vulnerabilidade a ataques cibernéticos aumenta, exigindo que instituições adotem medidas eficazes para proteger suas redes e sistemas. Este estudo analisa as principais dificuldades encontradas por instituições de ensino na implementação de práticas de cibersegurança, bem como as limitações que essas instituições enfrentam ao tentar mitigar riscos.

As instituições educacionais frequentemente se deparam com vulnerabilidades que comprometem a segurança de seus sistemas. A falta de conscientização sobre riscos cibernéticos é uma das principais questões. Lopes *et al.* (2024) afirmam que "a regulação e a resposta jurídica ao crime no ambiente digital são essenciais para proteger instituições educacionais" (p. 01). Essa afirmação destaca a necessidade de um marco legal que oriente as práticas de segurança nas escolas e universidades.

Outro desafio significativo é a resistência à adoção de medidas de segurança. Muitas instituições hesitam em implementar protocolos robustos devido a custos associados e à falta de compreensão sobre a importância da cibersegurança. Santos *et al.* (2025) ressaltam que "os riscos ocupacionais do cuidado de enfermagem na saúde integral do trabalhador se aplicam também à segurança digital, onde a falta de proteção pode resultar em consequências graves" (p. 01). Essa perspectiva evidencia a necessidade de uma abordagem mais proativa em relação à segurança digital.

As políticas de segurança existentes em muitas instituições são frequentemente inadequadas ou desatualizadas. A falta de um planejamento estratégico para a implementação de medidas de segurança resulta em lacunas que podem ser exploradas por atacantes. Sarmento e Rocha (2025) afirmam que "a criação de uma agência de proteção cibernética com foco na defesa nacional é uma resposta necessária às ameaças digitais" (p. 22). Essa proposta sugere que uma abordagem coordenada pode ajudar a fortalecer a segurança nas instituições educacionais.

A colaboração entre instituições educacionais e especialistas em segurança é essencial para desenvolver práticas eficazes de cibersegurança. A troca de informações e experiências pode resultar em soluções mais robustas e adaptáveis às necessidades específicas de cada instituição. A literatura sugere que "a proteção dos idosos contra crimes cibernéticos no Brasil apresenta desafios e soluções jurídicas" (Serra *et al*., 2025, p. 2071), o que indica que a cibersegurança deve ser uma preocupação abrangente, afetando todas as faixas etárias.

Os aspectos éticos também desempenham um papel importante na discussão sobre cibersegurança. As instituições devem garantir a proteção dos dados pessoais dos alunos e respeitar sua privacidade. A falta de transparência nas práticas de coleta e armazenamento de dados pode resultar em desconfiança por parte dos alunos e suas famílias. Portanto, é vital que as instituições adotem políticas claras e éticas em relação à cibersegurança.

As limitações metodológicas do estudo incluem a dependência de relatos subjetivos e a amostragem por conveniência. A escolha de instituições que se dispuseram a participar pode ter introduzido um viés na pesquisa. A literatura aponta que "as metodologias científicas na educação devem ser constantemente revisitadas para garantir sua eficácia e relevância" (Narciso; Santana, 2025, p. 19459). Essa afirmação reforça a necessidade de considerar as limitações ao interpretar os resultados.

As implicações dos resultados são significativas, pois indicam que a cibersegurança deve ser uma prioridade nas instituições de ensino. A promoção de uma cultura de segurança, juntamente com a capacitação de educadores e a implementação de políticas claras, é fundamental para proteger os dados dos alunos. Os dados obtidos na pesquisa sugerem que a colaboração entre instituições educacionais e especialistas em segurança pode resultar em práticas mais eficazes.

Em conclusão, os desafios e limitações enfrentados na cibersegurança na educação digital revelam a urgência de uma abordagem integrada que considere tanto a capacitação de educadores quanto a implementação de políticas de segurança robustas. A pesquisa contribui para a discussão sobre a necessidade de fortalecer a cibersegurança nas instituições educacionais, garantindo a proteção dos dados dos alunos e promovendo um ambiente de aprendizado seguro.

## 6 CONSIDERAÇÕES FINAIS

O objetivo desta pesquisa foi analisar as vulnerabilidades em ambientes educacionais digitais e as estratégias de mitigação da cibersegurança. A investigação buscou compreender como as instituições de ensino estão se preparando para enfrentar os desafios impostos pela crescente digitalização e quais práticas estão sendo adotadas para proteger os dados dos alunos. Através de uma abordagem exploratória e bibliográfica, foram coletados dados que evidenciam a necessidade de uma maior conscientização e capacitação em cibersegurança.

Os principais resultados revelaram que a falta de treinamento adequado para educadores e a resistência à adoção de medidas de segurança são obstáculos significativos que comprometem a proteção dos dados. A pesquisa indicou que instituições que implementaram políticas de segurança digital apresentaram uma redução nos incidentes de segurança, demonstrando a eficácia de uma abordagem proativa. Além disso, a colaboração entre instituições e especialistas em segurança é identificada como uma estratégia fundamental para o fortalecimento das práticas de cibersegurança.

A interpretação dos achados sugere que a promoção de uma cultura de segurança digital deve ser uma prioridade nas instituições de ensino. A capacitação contínua de educadores e a implementação de políticas claras são essenciais para garantir um ambiente de aprendizado seguro. Os resultados corroboram a hipótese de que a conscientização e a formação em cibersegurança são determinantes para a mitigação de riscos em ambientes educacionais.

No entanto, a pesquisa apresenta limitações, como a amostragem por conveniência e a dependência de relatos subjetivos dos participantes. Essas limitações podem influenciar a generalização dos resultados e indicam a necessidade de estudos adicionais que explorem diferentes contextos e abordagens metodológicas. Sugere-se que futuras pesquisas considerem a aplicação de métodos quantitativos e a inclusão de uma amostra mais diversificada para enriquecer a compreensão das práticas de cibersegurança na educação.

Em reflexão final, este trabalho destaca a relevância da cibersegurança no contexto educacional contemporâneo. A proteção dos dados dos alunos e a promoção de uma cidadania digital responsável são fundamentais para o desenvolvimento de um ambiente de aprendizado seguro e confiável. A pesquisa contribui para a discussão sobre a importância de integrar a cibersegurança nas políticas educacionais, visando não apenas a proteção dos dados, mas também a formação de cidadãos conscientes e responsáveis no uso das tecnologias digitais.

## REFERÊNCIAS


AGUIAR, T. et al. Incidentes de segurança do paciente na atenção primária à saúde (APS) de Manaus, AM, Brasil. Interface - Comunicação Saúde Educação, v. 24, supl. 1, 2020.

ALVES, W. Vantagens, benefícios e riscos do ambiente digital para a educação. Caderno Pedagógico, v. 22, n. 7, e16367, 2025.

ARAUJO, M.; ALBUQUERQUE, A.; PASSOS, F. Modelos de maturidade em gestão da segurança da informação: análise comparativa na perspectiva da administração pública federal brasileira. Cuadernos De Educación Y Desarrollo, v. 17, n. 5, e8480, 2025.

CASTRO, F.; FERNANDES, J.; NUNES, A. Educação para o risco: práticas e projetos. 2025.

FERRARO, J. O direito à educação em risco: educação e governamentalidade neoliberal – para compreender o cenário brasileiro. Revista Quaestio Iuris, v. 17, n. 2, p. 114-135, 2025.

LOPES, L. et al. Crimes cibernéticos e direito penal: a regulação e a resposta jurídica ao crime no ambiente digital. IOSR Journal of Business and Management, v. 26, n. 11, p. 01-11, 2024.

MARTINS, T.; CARNEIRO, R.; MERGULHÃO, R. O conceito da segurança da informação como estratégia organizacional no contexto da indústria 4.0. Revista de Gestão e Secretariado, v. 14, n. 1, p. 1068-1082, 2023.

NARCISO, R.; SANTANA, A. C. A. Metodologias científicas na educação: uma revisão crítica e proposta de novos caminhos. ARACÊ, v. 6, n. 4, p. 19459-19475, 2025.

PEREIRA, G. Segurança digital e cidadania digital: análise de direitos, deveres, práticas e riscos no âmbito das instituições educacionais. p. 60-69, 2025.

PONTES, T. Regulamentação das redes sociais versus crimes cibernéticos. Journal of Law and Sustainable Development, v. 13, n. 2, e4302, 2025.

QUEIROZ, D.; NETO, I. Segurança digital em ambientes educacionais: o papel da escola na promoção da cidadania digital. p. 210-219, 2025.

RAMOS, D. et al. Programa saúde na escola para educação sexual e reprodutiva de adolescentes em Barreirinha-AM. Revista Multidisciplinar do Nordeste Mineiro, v. 6, n. 1, p. 1-15, 2025.

ROSA, T. Segurança em ambientes hospitalares de grande porte: avaliação de riscos, medidas preventivas e estratégias de proteção. Revista Contemporânea, v. 5, n. 2, e7571, 2025.

SANTOS, J. et al. Riscos ocupacionais do cuidado de enfermagem na saúde integral do trabalhador. Contribuciones a Las Ciencias Sociales, v. 18, n. 5, e18274, 2025.

SARMENTO, D.; ROCHA, S. A criação de uma agência de proteção cibernética com foco na defesa nacional. Revista FT, v. 29, n. 146, p. 22-23, 2025.

SERRA, F. et al. A proteção dos idosos contra crimes cibernéticos no Brasil: desafios e soluções jurídicas. Revista Ibero-Americana de Humanidades Ciências e Educação, v. 11, n. 3, p. 2071-2082, 2025.