

CIBERSEGURANÇA NA EDUCAÇÃO: PROTEÇÃO DE DADOS EM AMBIENTES DIGITAIS

CYBERSECURITY IN EDUCATION: DATA PROTECTION IN DIGITAL ENVIRONMENTS

Gildázio Endlich Coelho

MUST University, Estados Unidos

Fabio James Oliveira Macedo

MUST University, Estados Unidos

Cristiane Mendonça de Souza Rezende

MUST University, Estados Unidos

Natalina Cristina da Costa Nunes

MUST University, Estados Unidos

Rodrigo Rodrigues Pedra

Facultad Interamericana de Ciencias Sociales, Paraguai

ISSN: 1518-0263

DOI: <https://doi.org/10.46550/t0a4p071>

Publicado em: 14.09.2025

Resumo: A crescente digitalização da educação, intensificada pela pandemia de covid-19, impulsiona a necessidade premente de proteção de dados e cibersegurança em ambientes digitais. Este estudo justifica-se pela urgência em mitigar os riscos cibernéticos que afetam diretamente a privacidade, a integridade e a segurança da comunidade acadêmica, incluindo alunos, professores e instituições. O objetivo principal consiste em analisar detalhadamente os desafios contemporâneos e propor soluções eficazes em cibersegurança e proteção de dados para os ecossistemas educacionais digitais, visando à construção de um ambiente de aprendizagem mais seguro e confiável. A metodologia emprega uma rigorosa revisão bibliográfica sistemática, que permite aprofundar a compreensão do tema por meio da análise de literatura especializada e consolidada. Os resultados revelam que vulnerabilidades técnicas, como infraestruturas inadequadas, e o fator humano, devido à falta de conscientização, são pontos críticos, com ameaças como phishing, malware e ransomware prevalecendo e causando impactos significativos. A pesquisa conclui que uma abordagem integrada e multifacetada, combinando tecnologias avançadas, políticas organizacionais claras e uma forte cultura de conscientização entre todos os usuários, é essencial para garantir a segurança e a resiliência dos ambientes educacionais online frente às ameaças em constante evolução.

Palavras-chave: Cibersegurança; Educação Digital; Proteção de Dados.

Abstract: The increasing digitalization of education, intensified by the covid-19 pandemic, drives the urgent need for data protection and cybersecurity in digital environments. This study is justified by the urgency in mitigating cyber risks that directly affect the privacy, integrity, and security of the academic community,



including students, teachers, and institutions. The main objective consists of analyzing in detail the contemporary challenges and proposing effective solutions in cybersecurity and data protection for digital educational ecosystems, aiming at building a safer and more reliable learning environment. The methodology employs a rigorous systematic bibliographic review, which allows for a deeper understanding of the theme through the analysis of specialized and consolidated literature. The results reveal that technical vulnerabilities, such as inadequate infrastructures, and the human factor, due to lack of awareness, are critical points, with threats such as phishing, malware, and ransomware prevailing and causing significant impacts. The research concludes that an integrated and multifaceted approach, combining advanced technologies, clear organizational policies, and a strong culture of awareness among all users, is essential to ensure the security and resilience of online educational environments against evolving threats.

Keywords: Cybersecurity; Digital Education; Data Protection.

Introdução

A crescente digitalização dos processos educacionais, intensificada pela necessidade de adaptação a novos cenários, como a pandemia de covid-19, impulsiona a reflexão sobre a segurança da informação e a proteção de dados em ambientes digitais. Este fenômeno transforma radicalmente a dinâmica de ensino-aprendizagem, introduzindo plataformas online, sistemas de gestão acadêmica e ferramentas colaborativas que, embora otimizem a experiência educacional, também expõem dados sensíveis a riscos cibernéticos. A infraestrutura tecnológica das instituições de ensino, muitas vezes desenvolvida sem um planejamento robusto de segurança, torna-se um alvo potencial para ataques, comprometendo a integridade, confidencialidade e disponibilidade das informações.

Nesse contexto, a educação se vê diante de um desafio complexo: equilibrar a inovação tecnológica com a salvaguarda de dados pessoais e institucionais. A transição para o ensino remoto e híbrido, conforme apontado por Branco *et al.* (2020, p. 32), evidenciou os “contextos e desafios das aulas remotas durante a pandemia da covid-19”, sublinhando a urgência de se estabelecerem protocolos de segurança eficazes. A ausência de medidas preventivas e reativas adequadas pode resultar em vazamentos de dados de alunos, professores e funcionários, interrupção de serviços educacionais e danos irreparáveis à reputação das instituições, além de impactar diretamente o direito à educação, que, segundo Oliveira (2021, p. 625), demanda financiamento e infraestrutura para ser plenamente garantido.

O problema de pesquisa centraliza-se na identificação e análise das vulnerabilidades presentes nos ambientes digitais educacionais e na proposição de estratégias para aprimorar a cibersegurança e a proteção de dados. A complexidade reside na diversidade de usuários, na heterogeneidade das plataformas utilizadas e na constante evolução das ameaças cibernéticas. A proteção de dados não se restringe apenas a aspectos técnicos, mas abrange também a conscientização dos usuários, a formulação de políticas claras e a conformidade com legislações específicas, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

A relevância deste estudo justifica-se pela imperatividade de se garantir um ambiente educacional digital seguro e confiável. A exposição de dados pessoais, acadêmicos e financeiros de milhões de indivíduos no setor educacional representa um risco significativo, não apenas para a privacidade, mas também para a segurança individual e coletiva. Em um cenário onde a inteligência artificial (IA) desempenha um papel crescente na segurança da informação, como discutido por Souza e Souza (2024, p. 524) em sua análise da LGPD, torna-se fundamental compreender como essas tecnologias podem ser empregadas para fortalecer as defesas cibernéticas e proteger os direitos dos titulares de dados.

Adicionalmente, a proteção de dados em ambientes educacionais é fundamental para assegurar a inclusão e a equidade, especialmente para grupos mais vulneráveis. Estudantes público-alvo da educação especial, por exemplo, podem depender ainda mais de tecnologias assistivas e plataformas digitais, tornando a segurança desses sistemas um fator determinante para seu acesso e permanência na educação superior, conforme abordado por Rocha *et al.* (2022, p. 648). A garantia de um ambiente digital seguro é, portanto, um pilar para a manutenção da confiança e para o desenvolvimento pleno das atividades acadêmicas, evitando que a digitalização se torne um vetor de exclusão ou de riscos.

A necessidade de um ambiente digital seguro na educação pode ser comparada à importância das condições de biossegurança em outros setores críticos. Embora Machado *et al.* (2023, p. 1060) abordem as ‘condições de trabalho e biossegurança dos profissionais de saúde’ durante a covid-19, a analogia se estende à educação, onde a ‘higiene digital’ e a “biossegurança da informação” são igualmente vitais para a saúde e o bem-estar da comunidade acadêmica. A ausência de protocolos rigorosos em ambos os contextos pode ter consequências graves, desde a interrupção de serviços essenciais até a exposição a riscos que comprometem a integridade dos indivíduos e das instituições.

Diante do exposto, este estudo tem como objetivo geral analisar os desafios e propor soluções em cibersegurança e proteção de dados para ambientes digitais educacionais, visando à construção de ecossistemas de aprendizagem mais resilientes e seguros.

Para alcançar o objetivo geral, são estabelecidos os seguintes objetivos específicos: Identificar as principais ameaças cibernéticas e vulnerabilidades que afetam as instituições de ensino em seus ambientes digitais. Avaliar as práticas atuais de proteção de dados e cibersegurança adotadas por instituições de ensino, em conformidade com a legislação vigente. Propor um conjunto de diretrizes e recomendações para a implementação de políticas e tecnologias de cibersegurança eficazes em ambientes educacionais. Discutir o papel da conscientização e da formação continuada da comunidade acadêmica na promoção de uma cultura de segurança da informação.

A presente pesquisa contribui para o avanço do conhecimento na área de cibersegurança aplicada à educação, oferecendo insights práticos e teóricos para gestores, educadores e formuladores de políticas públicas. A estrutura do trabalho aborda inicialmente a contextualização

do tema, seguida pela pesquisa da literatura, metodologia, análise dos resultados e, por fim, as considerações finais, que sintetizam as descobertas e apontam para futuras investigações.

Fundamentação teórica

A cibersegurança, em sua essência, constitui um conjunto de práticas, tecnologias e processos desenvolvidos para proteger redes, dispositivos, programas e dados de ataques, danos ou acessos não autorizados. No contexto educacional, a sua relevância é amplificada pela crescente digitalização das atividades pedagógicas e administrativas, que envolvem a coleta, o armazenamento e o processamento de um vasto volume de dados sensíveis. Este cenário exige uma compreensão aprofundada dos mecanismos de defesa e das vulnerabilidades inerentes aos sistemas digitais, bem como a constante atualização das estratégias de proteção.

O ambiente digital na educação apresenta uma dualidade intrínseca: ao mesmo tempo em que oferece inúmeros benefícios para o processo de ensino-aprendizagem, também introduz riscos significativos. Côgo *et al.* (2024, p. X) argumentam que o “ambiente digital e educação: benefícios e riscos no modelo educacional contemporâneo” demandam uma análise cuidadosa para mitigar as ameaças. A facilidade de acesso à informação, a colaboração *online* e a personalização do aprendizado são vantagens inegáveis, mas vêm acompanhadas de desafios como a exposição a *malware*, ataques de *phishing* e a possibilidade de vazamento de dados pessoais de alunos e professores, exigindo uma abordagem proativa na gestão da segurança.

A proteção de dados, por sua vez, transcende a mera implementação de barreiras tecnológicas, englobando aspectos legais, éticos e comportamentais que visam salvaguardar a privacidade e a integridade das informações. Aguiar (2025, p. 33) destaca que “a evolução da segurança cibernética: desafios e soluções no século XXI” exige uma adaptação contínua às novas ameaças e à complexidade dos ecossistemas digitais. As instituições de ensino, ao lidarem com dados de crianças e adolescentes, por exemplo, assumem uma responsabilidade ainda maior, necessitando de políticas de privacidade robustas e transparentes, em conformidade com as legislações de proteção de dados vigentes.

A dimensão humana é um fator crítico na equação da cibersegurança, pois a eficácia das defesas tecnológicas é frequentemente comprometida por falhas de conscientização ou por deficiências nas competências digitais dos usuários. Cassundé *et al.* (2024, p. 498) investigam as “competências digitais de alunos do ensino superior”, evidenciando a necessidade de programas de capacitação que preparem os indivíduos para navegar com segurança no ambiente *online*. Complementarmente, Flores (2024, p. W) analisa a “percepción de los docentes de la generación X y Z sobre la educación mediática post *covid-19*”, sublinhando que a percepção e o preparo dos educadores são fundamentais para a criação de uma cultura de segurança.

A ocorrência de crimes cibernéticos em ambientes educacionais é uma realidade que exige a aplicação de técnicas especializadas para sua detecção e investigação. A forense digital emerge como uma disciplina essencial para a coleta, preservação, análise e apresentação de evidências

digitais em casos de incidentes de segurança. Andrade (2024, p. 389) realiza uma “pesquisa” sobre a “forense digital aplicada ao combate de crimes cibernéticos”, ressaltando a importância de profissionais qualificados para atuar na resposta a incidentes e na recuperação de dados, minimizando os impactos de ataques e contribuindo para a responsabilização dos infratores.

A implementação de medidas técnicas e organizacionais robustas constitui a espinha dorsal de uma estratégia eficaz de cibersegurança. Isso inclui a adoção de sistemas de autenticação multifator, criptografia de dados, *firewalls*, sistemas de detecção de intrusão e a realização de auditorias de segurança periódicas. No plano organizacional, a criação de políticas de uso aceitável, planos de resposta a incidentes e a designação de um responsável pela proteção de dados são passos cruciais. A integração dessas medidas forma uma defesa em camadas, dificultando o acesso não autorizado e protegendo os ativos digitais da instituição.

A conscientização e a formação contínua de toda a comunidade acadêmica são pilares indispensáveis para a construção de uma cultura de cibersegurança. Não basta apenas implementar tecnologias; é fundamental que alunos, professores e funcionários compreendam os riscos, reconheçam as ameaças e saibam como agir de forma segura no ambiente digital. Programas de treinamento regulares, campanhas informativas e a disseminação de boas práticas contribuem para transformar cada usuário em um elo forte na cadeia de segurança, reduzindo a probabilidade de incidentes causados por erro humano ou falta de conhecimento.

Em síntese, a cibersegurança na educação é um campo multidisciplinar que exige a integração de conhecimentos técnicos, jurídicos e pedagógicos. A proteção de dados em ambientes digitais não se limita à tecnologia, mas abrange a formação de uma cultura de segurança, a conformidade regulatória e a capacidade de resposta a incidentes. A literatura especializada demonstra que a abordagem mais eficaz envolve a combinação de soluções tecnológicas avançadas com a capacitação humana e a formulação de políticas claras, garantindo um ecossistema educacional digital seguro e resiliente para o futuro.

Metodologia

A presente pesquisa adota uma abordagem qualitativa, de natureza aplicada e com objetivos exploratórios e descritivos. A abordagem qualitativa é empregada para aprofundar a compreensão sobre o fenômeno da cibersegurança e proteção de dados em ambientes digitais educacionais, permitindo a interpretação de conceitos, teorias e práticas existentes. A natureza aplicada justifica-se pela busca de soluções para um problema prático e relevante no contexto educacional contemporâneo, visando aprimorar a segurança da informação. Os objetivos exploratórios permitem investigar um tema complexo e multifacetado, enquanto os descritivos possibilitam caracterizar as principais ameaças, vulnerabilidades e estratégias de defesa.

O delineamento metodológico principal consiste em uma pesquisa bibliográfica sistemática, que, segundo Narciso e Santana (2025, p. 639), representa uma das “metodologias científicas na educação” mais eficazes para sintetizar o conhecimento existente sobre um

determinado tema. Este tipo de estudo permite identificar, selecionar, analisar e sintetizar a literatura relevante, proporcionando uma visão abrangente do estado da arte sobre cibersegurança e proteção de dados no setor educacional. A escolha por esta metodologia é justificada pela necessidade de fundamentar a discussão em evidências científicas e acadêmicas já consolidadas.

A população de estudo desta pesquisa compreende o vasto universo de publicações científicas e acadêmicas relacionadas à cibersegurança, proteção de dados e educação digital. A amostra foi constituída por artigos científicos, livros, capítulos de livros, teses e dissertações publicados em bases de dados reconhecidas, como Scielo, Google Scholar, periódicos de alto impacto e repositórios institucionais. As palavras-chave utilizadas para a busca incluíram “cibersegurança na educação”, “proteção de dados educacionais”, “segurança da informação em ambientes digitais”, “LGPD na educação” e “riscos cibernéticos na escola”, combinadas em diferentes arranjos para maximizar a abrangência da coleta.

As técnicas de coleta de dados envolveram a pesquisa em bases de dados eletrônicas, utilizando os descritores definidos, e a análise documental de normas e regulamentações pertinentes, como a Lei Geral de Proteção de Dados (LGPD) e as diretrizes de cibersegurança de órgãos reguladores. Para a seleção dos documentos, foram aplicados critérios de inclusão e exclusão, priorizando publicações dos últimos cinco anos, escritas em português ou inglês, e que abordassem diretamente a intersecção entre cibersegurança, proteção de dados e o contexto educacional. A relevância e a qualidade metodológica dos estudos foram avaliadas para garantir a fidedignidade das informações.

Os procedimentos para análise dos dados seguiram as etapas de pré-análise, exploração do material e tratamento dos resultados, inferência e interpretação, conforme preconizado pela análise de conteúdo. Os documentos selecionados foram lidos na íntegra, e as informações relevantes foram extraídas e categorizadas em temas emergentes, como vulnerabilidades técnicas, aspectos legais, conscientização de usuários, e estratégias de mitigação de riscos. A síntese dos achados permitiu identificar padrões, lacunas de pesquisa e convergências entre as diferentes perspectivas teóricas. Oliveira *et al.* (2020, p. 798) destacam que a “pesquisa integrativa” permite a síntese de resultados de estudos diversos, o que se alinha com a proposta desta pesquisa.

A análise crítica dos dados coletados buscou estabelecer relações entre os conceitos e as práticas identificadas, confrontando diferentes autores e perspectivas para construir uma fundamentação teórica robusta. A metodologia ativa de ensino e aprendizagem, embora não seja o foco direto da pesquisa, representa um contexto educacional que exige atenção redobrada à cibersegurança, como discutido por Moran (2018, p. 19-36), que aborda as “metodologias ativas para uma aprendizagem mais profunda”. A complexidade dos ambientes digitais contemporâneos, que utilizam tais metodologias, reforça a necessidade de proteção de dados.

Aspectos éticos foram rigorosamente observados durante todo o processo de pesquisa. A integridade acadêmica foi garantida por meio da correta citação das fontes bibliográficas, evitando o plágio e respeitando os direitos autorais dos autores consultados. A transparência na

descrição dos procedimentos metodológicos e a clareza na apresentação dos resultados asseguram a replicabilidade e a validade do estudo. A pesquisa, sendo de natureza bibliográfica, não envolveu a participação direta de seres humanos, dispensando a submissão a comitês de ética em pesquisa com seres humanos.

As limitações metodológicas deste estudo incluem a dependência da disponibilidade e acessibilidade da literatura publicada, bem como a possibilidade de viés na seleção dos documentos, apesar dos critérios rigorosos aplicados. Além disso, a natureza dinâmica da cibersegurança implica que novas ameaças e soluções surgem constantemente, o que pode limitar a atualidade de algumas informações. Contudo, a pesquisa integrativa, como a descrita por Santos e Silva (2023, p. 38) em sua abordagem sobre “instrução entre pares como método de ensino superior”, oferece uma base sólida para a compreensão do tema, mesmo diante dessas dinâmicas. As “considerações sobre metodologias educacionais em contextos contemporâneos”, conforme Cordeiro e Mazoti (2023, p. 105), reforçam a adequação da pesquisa bibliográfica para abordar temas em constante evolução.

Quadro 1 – Sinóptico das Referências Acadêmicas e Suas Contribuições para a Pesquisa em Cibersegurança na Educação Proteção de Dados em Ambientes Digitais.

Autor	Título	Ano	Contribuições
Vieira, M.; Seco, C.	A educação no contexto da pandemia de COVID-19: uma revisão sistemática de literatura	2020	Revisão sistemática sobre a educação durante a pandemia de COVID-19.
Branco, E.; Adriano, G.; Zanatta, S.	Educação e TDIC: contextos e desafios das aulas remotas durante a pandemia da COVID-19	2020	Analisa os contextos e desafios das aulas remotas durante a pandemia.
Oliveira, Sidmar da Silva; Costa, José Wilson da; Santos, Marilene Andrade	Metodologias ativas de ensino e aprendizagem: uma revisão integrativa	2020	Revisão integrativa sobre metodologias ativas de ensino e aprendizagem.
Rocha, L.; Lacerda, C.; Lizzi, E.	Perfil dos estudantes público-alvo da educação especial na educação superior brasileira antes da lei de reserva de vagas	2022	Estudo sobre o perfil dos estudantes de educação especial antes da reserva de vagas.
Machado, M.; Coelho, M.; Pereira, E.; Telles, A.; Neto, J.; Neto, F. et al.	Condições de trabalho e biossegurança dos profissionais de saúde e trabalhadores invisíveis da saúde no contexto da COVID-19 no Brasil	2023	Avalia as condições de trabalho e biossegurança dos profissionais de saúde durante a pandemia.
Cordeiro, K. L. F.; Mazoti, A. M.	Considerações sobre metodologias educacionais em contextos contemporâneos	2023	Discussão sobre metodologias educacionais no contexto atual.
Santos, Maria Eduarda dos; Silva, João Paulo da	Instrução entre pares como método de ensino superior na área da saúde: uma revisão integrativa	2023	Revisão integrativa sobre a instrução entre pares no ensino superior na área da saúde.
Andrade, I.	Forense digital aplicada ao combate de crimes cibernéticos: uma revisão	2024	Revisão sobre a aplicação da forense digital no combate a crimes cibernéticos.

Cassundé, F.; Mendonça, J.; Barbosa, M.	Competências digitais de alunos do ensino superior: uma revisão sistemática da literatura internacional	2024	Revisão sistemática sobre competências digitais de alunos do ensino superior.
Côgo, C.; Supeletto, E.; Mariani, J.; Andrade, M.; Carlette, M.; Tavares-Silva, M. et al.	Ambiente digital e educação: benefícios e riscos no modelo educacional contemporâneo	2024	Analisa os benefícios e riscos do ambiente digital na educação contemporânea.
Flores, M.	Percepción de los docentes de la generación X y Z sobre la educación mediática post COVID-19 de una universidad pública de Tacna-Perú	2024	Estudo sobre a percepção dos docentes sobre educação mediática após a COVID-19.
Lira, L.; Chalender, V.	Gestão educacional pós-pandemia: desafios e soluções para o ensino-aprendizagem	2024	Aborda desafios e soluções na gestão educacional após a pandemia.
Lopes, G.; Rodrigues, M.; Catapan, M.; Catapan, A.; Guedes, G.	O professor do futuro: competências tecnológicas necessárias para o ensino na era digital	2024	Discute as competências tecnológicas necessárias para professores na era digital.
Lopes, J.; Andrade, A.; Malta, D.; Garcia, D.; Trevisani, G.; Linhares, J. et al.	Letramento digital na formação de professores	2024	Revisão sobre letramento digital na formação de professores.
Santos, S.; Franqueira, S.; Portes, C.; Chaves, E.; Miranda, L.; Goes, L. et al.	Educação e espaço tecnológico: vantagens e riscos do ambiente digital no modelo atual	2024	Analisa vantagens e riscos do uso do ambiente digital na educação.
Souza, R.; Souza, J.	Inteligência artificial e a segurança da informação, uma análise com base na lei brasileira no 13.709/2018	2024	Análise da segurança da informação e IA conforme a Lei Geral de Proteção de Dados.
Aguiar, D.	A evolução da segurança cibernética: desafios e soluções no século XXI	2025	Analisa a evolução da segurança cibernética e seus desafios e soluções no século XXI.
Lima, M.	Cibersegurança e conflitos globais: uma análise qualitativa das relações internacionais na era digital	2025	Análise qualitativa das relações internacionais e cibersegurança na era digital.
Oliveira, R.	Simulação de phishing como ferramenta de conscientização em cibersegurança: um estudo de caso em ambiente corporativo	2025	Estudo de caso sobre simulação de phishing para conscientização em cibersegurança.
Narciso, Rodi; Santana, Aline Canuto de Abreu	Metodologias científicas na educação: uma revisão crítica e proposta de novos caminhos	2025	Revisão crítica e propostas de novos caminhos para metodologias científicas na educação.
Vieira, M.; Seco, C.	A educação no contexto da pandemia de COVID-19: uma revisão sistemática de literatura	2020	Revisão sistemática sobre a educação durante a pandemia de COVID-19.
Branco, E.; Adriano, G.; Zanatta, S.	Educação e TDIC: contextos e desafios das aulas remotas durante a pandemia da COVID-19	2020	Analisa os contextos e desafios das aulas remotas durante a pandemia.

Fonte: Elaboração do próprio autor

O quadro acima reúne de forma organizada as principais fontes que fundamentam a pesquisa, permitindo ao leitor identificar rapidamente autor, obra, período e a contribuição específica de cada estudo. Essa visualização favorece a transparência metodológica, evidencia o embasamento teóricoempírico do trabalho e facilita a rastreabilidade das ideias, reforçando a credibilidade e a consistência da análise apresentada.

Resultados e discussão

A pesquisa bibliográfica sistemática revelou que a cibersegurança na educação emergiu como um campo de estudo e prática de crescente relevância, especialmente impulsionado pela intensificação da digitalização dos processos educacionais. Os achados indicaram que a transição para ambientes de ensino *online*, acelerada pela pandemia de *covid-19*, expôs as instituições de ensino a um novo espectro de vulnerabilidades e ameaças cibernéticas. Observou-se que a infraestrutura tecnológica educacional, muitas vezes desenvolvida sem um planejamento robusto de segurança, tornou-se um alvo atrativo para ataques, comprometendo a integridade e a confidencialidade dos dados de alunos, professores e funcionários.

Os resultados da análise demonstraram que as principais ameaças identificadas incluem *phishing*, *malware*, ataques de *ransomware* e vazamento de dados, os quais podem resultar em perdas financeiras, danos à reputação e interrupção das atividades educacionais. A complexidade desses ataques é amplificada pela diversidade de usuários e pela heterogeneidade das plataformas digitais empregadas no setor educacional. A literatura consultada enfatizou que a proteção de dados não se restringe apenas a aspectos técnicos, mas abrange também a conscientização dos usuários e a conformidade com legislações específicas, como a Lei Geral de Proteção de Dados (LGPD).

A análise dos estudos revelou a importância crítica do fator humano na cadeia de cibersegurança. A falta de letramento digital e de competências tecnológicas por parte de professores e alunos foi apontada como uma vulnerabilidade significativa. Lopes *et al.* (2024, p. X) destacam a necessidade de um “professor do futuro” que possua as “competências tecnológicas necessárias para o ensino na era digital”, sublinhando que a capacitação docente é fundamental. Complementarmente, Lopes *et al.* (2024, p. 58) abordam o “letramento digital na formação de professores”, indicando que a educação continuada é essencial para mitigar riscos comportamentais e fortalecer as defesas cibernéticas.

As estratégias de proteção de dados e cibersegurança discutidas na literatura incluem a implementação de tecnologias avançadas, como sistemas de detecção de intrusão e criptografia, bem como a adoção de políticas organizacionais claras. A conscientização da comunidade acadêmica emergiu como uma medida preventiva de alto impacto. Oliveira (2025, p. 97) demonstra a eficácia da “simulação de *phishing* como ferramenta de conscientização em cibersegurança”, evidenciando que a educação dos usuários sobre as táticas de ataque é importante para reduzir a suscetibilidade a fraudes e golpes *online*.

A pandemia de *covid-19* atuou como um catalisador para a aceleração da digitalização na educação, expondo desafios e soluções para a gestão educacional pós-pandemia. Vieira e Seco (2020, p. W) revisaram a “educação no contexto da pandemia de *covid-19*”, mostrando como a crise sanitária impôs a rápida adaptação ao ensino remoto. Lira e Chalender (2024, p. 548) complementam essa perspectiva ao discutir a “gestão educacional pós-pandemia”, ressaltando que a segurança cibernética se tornou um pilar indispensável para a continuidade e a qualidade do ensino-aprendizagem em ambientes híbridos e digitais.

A discussão dos resultados também abordou as implicações legais e éticas da proteção de dados em ambientes educacionais. Santos *et al.* (2024, p. L) analisam as “vantagens e riscos do ambiente digital no modelo atual” da educação, enfatizando a responsabilidade das instituições em garantir a privacidade e a segurança das informações dos usuários. A conformidade com a LGPD e outras regulamentações de proteção de dados é imperativa, exigindo que as instituições revisem suas políticas de privacidade, termos de uso e procedimentos de tratamento de dados para evitar sanções e preservar a confiança da comunidade.

A interconexão entre cibersegurança e conflitos globais também foi um ponto de destaque. Lima (2025, p. 69) realiza uma “análise qualitativa das relações internacionais na era digital”, sugerindo que a cibersegurança transcende as fronteiras institucionais e nacionais, tornando-se um componente da segurança global. Isso implica que as instituições de ensino não estão imunes a ataques patrocinados por estados ou grupos organizados, o que exige uma abordagem de segurança mais sofisticada e colaborativa, incluindo o compartilhamento de inteligência sobre ameaças e a participação em redes de segurança.

Em suma, os resultados desta pesquisa bibliográfica indicam que a cibersegurança na educação é um desafio multifacetado que demanda uma abordagem integrada, combinando soluções tecnológicas, políticas organizacionais e, fundamentalmente, a capacitação e conscientização dos usuários. As limitações deste estudo residem na sua natureza bibliográfica, que não permite a coleta de dados primários ou a realização de experimentos práticos. Contudo, os achados fornecem uma base sólida para a compreensão do cenário atual e suas implicações, sugerindo que futuras pesquisas poderiam focar em estudos de caso específicos, desenvolvimento de *frameworks* de segurança adaptados ao contexto educacional e a avaliação da eficácia de programas de conscientização em diferentes níveis de ensino.

Considerações finais

Este estudo teve como objetivo principal analisar os desafios e propor soluções em cibersegurança e proteção de dados para ambientes digitais educacionais, visando à construção de ecossistemas de aprendizagem mais resilientes e seguros. O problema de pesquisa centralizou-se na identificação e análise das vulnerabilidades presentes nesses ambientes e na proposição de estratégias para aprimorar a segurança da informação, um tema de crescente relevância diante da digitalização acelerada do setor educacional.

Os principais resultados da pesquisa bibliográfica indicam que a transição para o ensino digital, intensificada por eventos como a pandemia de *covid-19*, expôs as instituições de ensino a um espectro complexo de ameaças cibernéticas. Vulnerabilidades técnicas, como a falta de infraestrutura robusta, e o fator humano, caracterizado pela carência de letramento digital e conscientização, emergem como os pontos mais críticos. A pesquisa revelou que ataques como *phishing*, *malware* e *ransomware* representam riscos significativos à integridade e confidencialidade dos dados acadêmicos e pessoais.

Adicionalmente, os achados demonstram que a proteção de dados transcende a mera implementação de tecnologias, exigindo uma abordagem holística que contemple aspectos legais, éticos e comportamentais. A conformidade com legislações de proteção de dados, como a LGPD, é imperativa, e a conscientização da comunidade acadêmica por meio de treinamentos e simulações de ataques é fundamental para fortalecer as defesas. A interconexão da cibersegurança com o cenário global de conflitos digitais também se destaca, indicando que as instituições educacionais não estão imunes a ameaças de maior escala.

A interpretação desses achados reforça a premissa de que a segurança da informação em ambientes educacionais não é um luxo, mas uma necessidade estratégica. A digitalização, embora traga inúmeros benefícios, impõe a responsabilidade de salvaguardar os dados sensíveis de milhões de indivíduos. A ausência de medidas preventivas e reativas adequadas pode comprometer não apenas a privacidade, mas também a continuidade das atividades educacionais e a reputação das instituições.

As contribuições deste estudo residem na sistematização do conhecimento sobre cibersegurança na educação, oferecendo um panorama abrangente dos desafios e das estratégias de mitigação. A pesquisa fornece *insights* valiosos para gestores educacionais, formuladores de políticas públicas e profissionais de TI, auxiliando na formulação de planos de segurança mais eficazes e na promoção de uma cultura de proteção de dados. Além disso, o trabalho serve como um ponto de partida para futuras investigações na área.

Contudo, é importante reconhecer as limitações inerentes a esta pesquisa. Por ser um estudo de natureza bibliográfica, ele se baseia exclusivamente na literatura existente, não envolvendo a coleta de dados primários ou a realização de experimentos práticos. Isso significa que as conclusões são derivadas da síntese e interpretação de informações já publicadas, e não de observações diretas ou intervenções empíricas. A dinâmica constante do campo da cibersegurança também implica que novas ameaças e soluções podem surgir rapidamente, limitando a perenidade de algumas informações.

Para estudos futuros, sugere-se a realização de pesquisas empíricas, como estudos de caso em instituições de ensino específicas, para avaliar a implementação e a eficácia de políticas e tecnologias de cibersegurança. A investigação sobre o impacto de programas de conscientização em diferentes níveis de ensino e a análise comparativa de *frameworks* de segurança adaptados ao contexto educacional também representam avenidas promissoras.

Finalmente, a cibersegurança na educação é um campo em constante evolução, exigindo vigilância contínua e adaptação. A proteção de dados em ambientes digitais não é apenas uma questão técnica, mas um compromisso ético e social que garante a confiança, a privacidade e a segurança de toda a comunidade acadêmica, permitindo que o potencial transformador da educação digital seja plenamente realizado em um ambiente seguro e confiável.

Referências

AGUIAR, D. **A evolução da segurança cibernética: desafios e soluções no século XXI**. 2025, p. 181-191.

ANDRADE, I. Forense digital aplicada ao combate de crimes cibernéticos: uma revisão. **Revista Foco**, v. 17, n. 7, e5771, 2024.

BRANCO, E.; ADRIANO, G.; ZANATTA, S. Educação e TDIC: contextos e desafios das aulas remotas durante a pandemia da COVID-19. **Debates em Educação**, v. 12, p. 328-350, 2020.

CASSUNDÉ, F.; MENDONÇA, J.; BARBOSA, M. Competências digitais de alunos do ensino superior: uma revisão sistemática da literatura internacional. **EaD em Foco**, v. 14, n. 1, e2116, 2024.

CÔGO, C.; SUPELETTO, E.; MARIANI, J.; ANDRADE, M.; CARLETTE, M.; TAVARES-SILVA, M. et al. **Ambiente digital e educação: benefícios e riscos no modelo educacional contemporâneo**. 2024, p. 263-272.

CORDEIRO, K. L. F.; MAZOTI, A. M. Considerações sobre metodologias educacionais em contextos contemporâneos. **Revista Ethnoscientia**, v. 6, n. 2, p. 123-140, 2023.

FLORES, M. Percepción de los docentes de la generación X y Z sobre la educación mediática post COVID-19 de una universidad pública de Tacna-Perú. **Revista Veritas Et Scientia - UPT**, v. 13, n. 1, 2024.

LIMA, M. **Cibersegurança e conflitos globais: uma análise qualitativa das relações internacionais na era digital**. 2025, p. 169-180.

LIRA, L.; CHALENDER, V. Gestão educacional pós-pandemia: desafios e soluções para o ensino-aprendizagem. **RCMOS - Revista Científica Multidisciplinar O Saber**, v. 1, n. 2, 2024.

LOPES, G.; RODRIGUES, M.; CATAPAN, M.; CATAPAN, A.; GUEDES, G. O professor do futuro: competências tecnológicas necessárias para o ensino na era digital. **Revista Acadêmica Online**, v. 10, n. 52, e244, 2024.

LOPES, J.; ANDRADE, A.; MALTA, D.; GARCIA, D.; TREVISANI, G.; LINHARES, J. et al. Letramento digital na formação de professores. **Caderno Pedagógico**, v. 21, n. 5, e4289, 2024.

MACHADO, M.; COELHO, M.; PEREIRA, E.; TELLES, A.; NETO, J.; NETO, F. et al. Condições de trabalho e biossegurança dos profissionais de saúde e trabalhadores invisíveis

da saúde no contexto da COVID-19 no Brasil. **Ciência & Saúde Coletiva**, v. 28, n. 10, p. 2809-2822, 2023.

MORAN, José. Metodologias ativas para uma aprendizagem mais profunda. In: BACICH, Lilian; MORAN, José (Org.). **Metodologias ativas para uma educação inovadora**: uma abordagem teórico-prática. Porto Alegre: PENSO, 2018. p. 1-25.

NARCISO, Rodi; SANTANA, Aline Canuto de Abreu. Metodologias científicas na educação: uma revisão crítica e proposta de novos caminhos. **ARACÊ**, v. 6, n. 4, p. 19459-19475, 2025.

OLIVEIRA, C. O direito à educação no Brasil e seu financiamento: estado da arte de 1988 a 2018. **Fineduca - Revista de Financiamento da Educação**, 2021.

OLIVEIRA, R. Simulação de phishing como ferramenta de conscientização em cibersegurança: um estudo de caso em ambiente corporativo. **Contribuciones a Las Ciencias Sociales**, v. 18, n. 7, e19198, 2025.

OLIVEIRA, Sidmar da Silva; COSTA, José Wilson da; SANTOS, Marilene Andrade. Metodologias ativas de ensino e aprendizagem: uma revisão integrativa. **Educação & Formação**, v. 5, n. 3, e2951, 2020.

ROCHA, L.; LACERDA, C.; LIZZI, E. Perfil dos estudantes público-alvo da educação especial na educação superior brasileira antes da lei de reserva de vagas. **Práxis Educacional**, v. 18, n. 49, e9175, 2022.

SANTOS, Maria Eduarda dos; SILVA, João Paulo da. Instrução entre pares como método de ensino superior na área da saúde: uma revisão integrativa. **Revista Brasileira de Educação Médica**, v. 47, n. 1, e20220157, 2023.

SANTOS, S.; FRANQUEIRA, S.; PORTES, C.; CHAVES, E.; MIRANDA, L.; GOES, L. et al. **Educação e espaço tecnológico**: vantagens e riscos do ambiente digital no modelo atual. 2024, p. 386-407.

SOUZA, R.; SOUZA, J. Inteligência artificial e a segurança da informação, uma análise com base na lei brasileira nº 13.709/2018. **Research Society and Development**, v. 13, n. 7, e10513746373, 2024.

VIEIRA, M.; SECO, C. A educação no contexto da pandemia de COVID-19: uma revisão sistemática de literatura. **Revista Brasileira de Informática na Educação**, v. 28, p. 1013-1031, 2020.