SEGURANÇA E PRIVACIDADE EM AMBIENTES DIGITAIS EDUCACIONAIS[1]

SECURITY AND PRIVACY IN DIGITAL EDUCATIONAL ENVIRONMENTS

Renato Araújo da Silva[2]
Lourival Queiroz Alcântara Junior[3]

RESUMO: Este estudo debruçou-se sobre a importância do fomento da segurança e privacidade em ambientes digitais educacionais, um tema que se destaca diante da crescente digitalização do ensino. A pesquisa foi motivada pela necessidade de proteger dados pessoais de alunos e professores contra vulnerabilidades digitais, equilibrando segurança e flexibilidade para promover uma educação digital segura e eficaz. O principal objetivo foi analisar a pertinência de reforçar medidas de segurança e privacidade em contextos educacionais online, considerando as regulamentações como a Lei Geral de Proteção de Dados (LGPD). Utilizando uma metodologia qualitativa de revisão bibliográfica, o estudo explorou dissertações, teses e artigos recentes para mapear o estado da arte e identificar lacunas e oportunidades no campo. Os resultados indicaram a necessidade crucial de políticas robustas que protejam os dados sem restringir o acesso e a partilha de informações pedagógicas em igual medida. Sugere-se que futuras pesquisas explorem o impacto dessas políticas na inovação pedagógica.

Palavras-chave: **s**egurança digital; privacidade; educação à distância; LGPD.

ABSTRACT: This study focused on the importance of promoting security and privacy in digital educational environments, a topic that stands out in the face of the growing digitalization of education. The research was motivated by the need to protect personal data of students and teachers against digital vulnerabilities, balancing security and flexibility to promote safe and effective digital education. The main objective was to analyze the relevance of strengthening security and privacy measures in online educational contexts, considering regulations such as the General Data Protection Law (LGPD). Using a qualitative methodology of bibliographic review, the study explored dissertations, theses, and recent articles to map the state of the art and identify gaps and opportunities in the field. The results indicated a crucial need for robust policies that protect data without equally restricting access and sharing of pedagogical information. Future research is suggested to explore the impact of these policies on pedagogical innovation.

Keywords: digital security; privacy; distance education; LGPD.

Data de apresentação: 28/03/2025.

---

1 Artigo apresentado ao curso Informática na Educação do Instituto Federal do Amapá como requisito para a obtenção do título de Pós-graduação

2 Acadêmico do curso de Pós-graduação em Informática na Educação.

3 Orientador, Mestre em Educação Docente do Instituto Federal do Amapá. Email: professorlourival@ifap.edu.br.

1 INTRODUÇÃO

O estudo em foco aborda a importância do fomento da segurança e da privacidade em ambientes digitais educacionais, um tema que ganha relevância no contexto atual de crescente digitalização do ensino. Com a expansão do acesso à educação à distância, impulsionada por fatores como a pandemia de COVID-19 e o avanço tecnológico, surge a necessidade imperativa de proteger os dados pessoais de alunos e professores contra vulnerabilidades digitais (Antunes Neto; Quintino; Corrêa, 2021).

Esta pesquisa é justificada pela urgência em desenvolver e implementar políticas robustas de segurança que não apenas cumpram com regulamentações como a Lei Geral de Proteção de Dados (LGPD), mas que também garantam um ambiente seguro e confiável para o aprendizado. O risco de exposição a ataques cibernéticos e violações de dados pode ter implicações profundas, afetando desde a integridade pessoal dos envolvidos até a qualidade do processo educacional. Por isto que este estudo visa identificar até que ponto o reforço dessas medidas é fundamental para o ambiente educacional digital, ponderando entre a proteção necessária e a flexibilidade essencial para a inovação pedagógica e a colaboração (Alves *et al*., 2023). Através deste equilíbrio, busca-se promover uma educação digital que seja tanto segura quanto eficaz, alinhando segurança com avanço educacional.

Nessa perspectiva, aqui se busca responder a seguinte questão de pesquisa: Quais são os principais desafios na implementação de medidas de segurança e privacidade em ambientes digitais educacionais e como a adequação à LGPD pode impactar a inovação pedagógica e a inclusão digital? A priori, considera-se que a promoção intensiva da segurança e privacidade em ambientes digitais educacionais é crucial para garantir a proteção eficaz dos dados pessoais de alunos e professores, minimizando o risco de violações que podem impactar negativamente a integridade acadêmica e psicológica dos envolvidos, e, consequentemente, melhorar a adesão e a eficiência dos processos educacionais (Almeida *et al*., 2024). Embora a segurança e privacidade sejam importantes, seu fomento excessivo em ambientes educacionais digitais pode resultar em restrições severas ao acesso e à partilha de informações pedagógicas, potencialmente limitando a inovação educacional e a colaboração necessária para um aprendizado efetivo e inclusivo (Araujo, 2022).

Por sua vez, este estudo tem como objetivo analisar os desafios e oportunidades na implementação de políticas de segurança e privacidade em ambientes digitais educacionais, com ênfase na conformidade com a LGPD e no impacto dessas medidas na inovação pedagógica. Para abordar adequadamente a questão da segurança e privacidade em ambientes digitais educacionais, é crucial avaliar a prática atual de proteção de dados no Brasil. Este estudo deve considerar os desafios enfrentados pela educação à distância, incluindo as soluções e tecnologias disponíveis para mitigar riscos. Explorando tanto a legislação quanto as ferramentas tecnológicas, será possível identificar lacunas e oportunidades para fortalecer a segurança dos dados e, consequentemente, a eficácia do ensino digital (Araújo Filho; Silva; Santos Filho, 2024).

A pesquisa adotou uma abordagem qualitativa baseada em revisão bibliográfica, utilizando dissertações, teses e artigos científicos disponíveis em bases como o Portal da CAPES e o Google Acadêmico. Para a seleção dos materiais, foram utilizados os descritores 'segurança digital na educação', 'privacidade de dados na educação' e 'LGPD no ensino', priorizando publicações de 2021 a 2024. O critério de exclusão abrangeu estudos que não abordam diretamente a interseção entre segurança digital e práticas educacionais. Tal abordagem tem como objetivo mapear o estado da arte das discussões sobre educação inclusiva e tecnologias emergentes, promovendo uma análise crítica e reflexiva sobre as práticas existentes e as lacunas no campo.

Os critérios de inclusão adotados foram: artigos, dissertações e teses que abordassem diretamente a interseção entre segurança digital, práticas educacionais e a aplicação da LGPD no Brasil; além de estudos que discutissem os desafios práticos enfrentados por instituições educacionais. Por outro lado, foram excluídos estudos que não apresentaram relação direta com o tema central ou que tratassem exclusivamente de contextos internacionais sem aplicabilidade ao cenário brasileiro.

Escolher o método de revisão bibliográfica sistemática justifica-se pela necessidade de consolidar um panorama abrangente das discussões acadêmicas mais recentes. Essa abordagem permite identificar lacunas no conhecimento existente e oferecer uma análise crítica sobre os desafios e oportunidades no campo da segurança digital em ambientes educacionais.

Os materiais selecionados foram analisados por meio de uma análise de conteúdo temática, conforme o método proposto por Bardin (2016). Essa técnica possibilitou identificar padrões recorrentes, desafios específicos enfrentados pelas instituições educacionais brasileiras e propostas para a implementação eficaz da LGPD. As categorias principais emergentes incluíram: infraestrutura tecnológica nas instituições educacionais; capacitação profissional para segurança digital; impactos da LGPD na inovação pedagógica; relação entre segurança digital e inclusão educacional.

Com essa metodologia detalhada, busca-se garantir maior rigor acadêmico ao estudo, promovendo transparência e reprodutibilidade. Além disso, ao focar no contexto brasileiro, a pesquisa contribui diretamente para o debate sobre como as instituições podem equilibrar inovação pedagógica com conformidade regulatória.

Como se constata, este estudo busca não apenas destacar a necessidade de aprimoramento das políticas de segurança e privacidade em ambientes digitais educacionais, mas também propor uma reflexão sobre como equilibrar a proteção de dados com a inovação pedagógica. Espera-se oferecer contribuições significativas para a prática educacional digital, promovendo um ambiente de aprendizagem seguro e propício ao desenvolvimento integral dos estudantes.

2 A PROTEÇÃO DE DADOS DIGITAIS NO BRASIL

A proteção de dados digitais no Brasil, especialmente em ambientes educacionais, tornou-se um tema central nas discussões sobre segurança e privacidade na era digital. A Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 2018, representa um marco legal que estabelece diretrizes claras para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais (Bezerra *et al*., 2024). Este contexto legislativo é crucial para entender a importância da proteção de dados em instituições de ensino, onde a quantidade e a sensibilidade dos dados processados exigem uma atenção redobrada.

As instituições de ensino enfrentam desafios críticos na proteção de dados, pois lidam com informações altamente sensíveis, incluindo registros acadêmicos e dados pessoais de alunos e funcionários. A falta de investimentos em infraestrutura tecnológica e a baixa capacitação dos profissionais da educação na gestão da segurança digital aumentam a vulnerabilidade a ataques cibernéticos. Conforme estudos recentes (CUNHA, 2023), a ausência de protocolos padronizados de segurança e a dependência de plataformas terceirizadas sem conformidade integral com a LGPD representam riscos adicionais. A crescente adoção de tecnologias como sistemas de aprendizado online e aplicativos educacionais complica ainda mais a gestão desses dados, ampliando tanto o escopo quanto a complexidade das responsabilidades das instituições de ensino. Neste contexto, a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil torna-se crucial (Bin, 2023). Mais do que uma exigência legal, é uma necessidade prática para assegurar a proteção dos direitos individuais e promover um ambiente educacional que seja ao mesmo tempo seguro e inclusivo.

Nesse cenário, a implementação efetiva da LGPD nas instituições de ensino exige uma abordagem multifacetada que envolva a revisão e a atualização das políticas internas, a adoção de medidas técnicas de segurança e a capacitação contínua dos profissionais da educação. A conscientização sobre a importância da proteção de dados deve ser disseminada em todos os níveis da instituição, desde a alta gestão até os alunos, fomentando uma cultura de privacidade e segurança. Segundo Moraes e Silva (2024), a implementação da LGPD não deve ser vista como um mero cumprimento de obrigações legais, mas como uma oportunidade para fortalecer a reputação da instituição, aumentar a confiança dos alunos e familiares e promover a inovação pedagógica. Afinal, um ambiente educacional seguro e transparente é fundamental para o desenvolvimento integral dos estudantes e para a construção de uma sociedade mais justa e democrática.

Um dos desafios críticos que as instituições educacionais enfrentam hoje é a insuficiência de infraestrutura adequada para assegurar a segurança dos dados. Com recursos financeiros e técnicos muitas vezes restritos, essas instituições encontram-se vulneráveis a lacunas significativas na proteção de dados. Além disso, a falta de formação específica em segurança da informação entre educadores e administradores aumenta o risco de violações de dados. Estas falhas não só colocam em risco a privacidade e a segurança dos indivíduos envolvidos — alunos, professores e staff — mas também podem prejudicar gravemente a reputação das instituições (Cunha, 2023). Portanto, é essencial que as escolas e universidades invistam na capacitação de seu pessoal e na modernização de sua infraestrutura tecnológica para mitigar esses riscos, garantindo um ambiente seguro para a gestão e o manuseio de informações sensíveis.

A privacidade em ambientes educacionais digitais vai além da simples proteção contra acessos não autorizados ou vazamentos de dados. Tal fato envolve assegurar que os alunos e seus responsáveis estejam plenamente informados e tenham controle sobre a coleta e o uso de seus dados pessoais. A transparência nesta coleta e manipulação de dados é fundamental para estabelecer e manter uma relação de confiança entre estudantes, pais e as instituições educacionais. Este relacionamento transparente não apenas fortalece a segurança, mas também cria um ambiente propício ao desenvolvimento acadêmico e pessoal. Instituições que priorizam essa abertura sobre como os dados são utilizados demonstram um compromisso com a ética e com o respeito à individualidade e privacidade de cada indivíduo (Duque, 2022). Por isso, é crucial que as políticas de privacidade sejam claramente comunicadas e rigorosamente aplicadas, garantindo um espaço educacional que apoie tanto o crescimento quanto a segurança dos envolvidos.

É crucial que as instituições educacionais implementem políticas robustas de proteção de dados, alinhadas às diretrizes da Lei Geral de Proteção de Dados (LGPD). Isto requer investimentos significativos em tecnologias de segurança, além da realização de auditorias regulares e do oferecimento de formação contínua para todos os envolvidos na gestão de dados. Adicionalmente, é essencial estabelecer uma colaboração efetiva entre o governo, as instituições de ensino e os profissionais de tecnologia da informação. Tal esforço conjunto visa desenvolver estratégias que reforcem a segurança digital, sem que isso prejudique a qualidade da oferta educacional (Gonçalves, 2023). Estas ações são fundamentais para criar um ambiente educacional seguro, onde a privacidade dos dados é garantida e a integridade do processo educativo é mantida.

A proteção de dados no contexto educacional brasileiro é uma questão multifacetada que exige uma abordagem integrada e orientada para o futuro (Maciel, 2022). O sucesso nesta área não será apenas uma medida de como os dados são protegidos, mas também de como a educação pode evoluir em um ambiente cada vez mais digital e interconectado, mantendo-se fiel aos princípios de segurança, privacidade e inclusão.

No contexto especifico da Universidade Federal do Amapá – UNIFAP, o processo de implementação da Lei Geral de Proteção de Dados – LGPD demonstra panorama de desafios significativos. Ainda que a instituição tenha designado um Encarregado de Dados, um avanço importante para a conformidade, essa informação precisa de publicidade na página oficial da UNIFAP, limitando o acesso da comunidade acadêmica, sociedade e órgãos fiscalizadores a este recurso essencial. Além disso, a UNIFAP ainda não implementou politicas fundamentais para a adequação à LGPD, como políticas de privacidade, segurança e cookies, o que a deixa vulnerável em termos de proteção de dados. Tais fatores mostram as dificuldades enfrentadas por algumas instituições de ensino superior em traduzir as exigências da LGPD em práticas eficazes, e a analise dessa situação especifica contribui para a compreensão das diferenças da implementação da Lei em Universidades da região Amazônia, ofertando percepções valiosas para outras instituições em situações semelhantes.

3 EDUCAÇÃO À DISTÂNCIA: DESAFIOS, SOLUÇÕES E TECNOLOGIAS

A educação à distância (EAD) tem se mostrado fundamental, adaptando-se às necessidades de flexibilidade e acessibilidade na educação contemporânea. Contudo, esse modelo enfrenta desafios notáveis, especialmente no que concerne à segurança e privacidade dos dados. Proteger informações pessoais e acadêmicas é crucial, dado o aumento de atividades online que expõem alunos e instituições a potenciais riscos cibernéticos (Narciso *et al*., 2024). Assim, garantir um ambiente digital seguro é essencial para sustentar a integridade e a confiança no sistema de EAD.

Na era digital, a proteção de informações tornou-se um componente crítico da educação, exigindo medidas rigorosas para assegurar tanto a privacidade dos estudantes quanto a integridade dos dados. Com a expansão da educação à distância, estabelecer um ambiente seguro e eficaz é imperativo. Isto envolve a implementação de protocolos de segurança robustos, como criptografia avançada e autenticação de dois fatores, para prevenir acessos não autorizados e vazamentos de dados (Nascimento *et al*., 2024). Manter essas defesas fortalece a confiança no processo educacional, essencial para a aprendizagem efetiva e para a manutenção da reputação institucional no ambiente digital.

A transformação digital em escolas e universidades trouxe consigo uma série de inovações tecnológicas destinadas a enriquecer o processo educacional. No entanto, esta evolução também resultou em novas vulnerabilidades. A introdução de ferramentas digitais variadas não só facilitou o acesso e a disseminação de informações, mas também expôs as instituições a riscos aumentados relacionados à segurança dos dados. Gerenciar essas vulnerabilidades tornou-se uma tarefa essencial, exigindo que as instituições adotem protocolos rigorosos para proteger a integridade e a confidencialidade das informações dos usuários (Nhancale *et al*., 2023). A segurança de dados robusta é agora uma prioridade para garantir que o ambiente educacional permaneça seguro e confiável para todos os envolvidos.

O primeiro grande desafio da educação à distância (EAD) é a segurança dos dados. Com a realização de aulas de forma virtual, uma imensa quantidade de dados pessoais e acadêmicos é transmitida diariamente através dos sistemas de informação. Isto eleva substancialmente o risco de ataques cibernéticos, como *phishing* e *ransomware*, especialmente se as medidas de proteção adotadas não forem suficientemente robustas (Souza *et al*., 2024). Portanto, as instituições de ensino devem investir significativamente em infraestruturas tecnológicas avançadas e em políticas de segurança da informação rigorosas. Medidas como a implementação de criptografia forte, autenticação de dois fatores e soluções completas de segurança cibernética são essenciais para assegurar a integridade e a disponibilidade dos dados (Novais *et al*., 2024). Estes investimentos são cruciais para criar um ambiente virtual de

aprendizagem seguro, protegendo tanto os alunos quanto as próprias instituições contra as crescentes ameaças digitais.

Na educação à distância (EAD), além da segurança, a privacidade representa um desafio significativo. A natureza deste modelo educacional, que frequentemente transpõe as fronteiras entre o espaço pessoal e o educacional, pois ocorre dentro do ambiente privado dos alunos, requer uma gestão cuidadosa da privacidade. As instituições devem assegurar que as plataformas e softwares empregados na entrega do conteúdo respeitem rigorosamente a privacidade dos usuários. Isto inclui evitar a coleta desnecessária de dados e proporcionar aos alunos controle total sobre suas próprias informações (Vaz, 2022). A conformidade com a Lei Geral de Proteção de Dados (LGPD) e a implementação de políticas de privacidade claras e transparentes são fundamentais para estabelecer e manter a confiança entre as instituições e a comunidade acadêmica (Oliveira, 2022; Praca, 2023). Estas medidas garantem que os alunos se sintam seguros e protegidos, permitindo que se concentrem totalmente em seu aprendizado sem preocupações adicionais sobre a segurança de suas informações pessoais.

No contexto da educação à distância (EAD), a tecnologia assume um papel crucial ao fornecer soluções para seus desafios intrínsecos. Plataformas de aprendizado online, como os Sistemas de Gestão de Aprendizagem (LMS), são fundamentais não apenas para facilitar a entrega de conteúdo educacional, mas também para monitorar o progresso dos alunos e gerenciar a interação efetiva entre professores e estudantes. A importância dessas plataformas vai além da funcionalidade básica; elas devem ser desenvolvidas sob o princípio de "*privacy by design*". Este conceito assegura que a segurança e a privacidade dos dados sejam componentes integrados ao design e à operação desde o início, prevenindo riscos de privacidade antes que se tornem problemas (Praxedes *et al*., 2023). Adotar tal abordagem é essencial para garantir que os direitos dos usuários sejam respeitados e protegidos, estabelecendo um ambiente de aprendizagem digital que seja não só eficiente, mas também seguro e confiável para todos os envolvidos.

A implementação de inteligência artificial (AI) na educação à distância (EAD) está revolucionando a maneira como o conteúdo é entregue e personalizado. A capacidade da AI de adaptar o ensino às necessidades individuais de cada aluno transforma a experiência educacional, tornando-a mais eficaz. Esta personalização não apenas atende melhor às variações de aprendizado de cada estudante, mas também maximiza o engajamento ao proporcionar feedback instantâneo. Este feedback, gerado em tempo real, permite que os alunos compreendam suas falhas e sucessos imediatamente, facilitando uma aprendizagem mais rápida e mais profunda (Reis *et al*., 2024). Estas melhorias na customização e na resposta educacional destacam o potencial da AI para significativamente enriquecer a EAD, tornando-a uma ferramenta cada vez mais poderosa na educação moderna.

A aplicação de inteligência artificial (AI) na educação à distância (EAD) oferece vantagens inegáveis, mas também exige uma gestão cuidadosa para prevenir possíveis desvantagens. A necessidade de monitorar e ajustar continuamente os algoritmos é essencial para evitar tendências que possam distorcer ou prejudicar as decisões educacionais automatizadas. Estas posturas podem surgir de imperfeições nos dados de treinamento ou na programação dos algoritmos. Portanto, é crucial que as decisões tomadas por sistemas de AI sejam transparentes e passíveis de revisão, garantindo que sejam justas e equitativas para todos os alunos (Santos, 2022). A integridade do processo de ensino depende dessa vigilância, assegurando que a tecnologia seja utilizada como uma ferramenta de apoio eficaz e inclusiva, que realmente beneficie toda a comunidade educacional envolvida na EAD.

Enquanto a EAD apresenta oportunidades significativas para expandir o acesso à educação, ela também exige uma abordagem consciente e estratégica para lidar com os desafios relacionados à segurança e privacidade (Santos *et al*., 2024). A chave para o sucesso na EAD será uma combinação de tecnologia avançada, políticas rigorosas e uma cultura de respeito pela

privacidade dos dados, assegurando assim um ambiente de aprendizado seguro e eficaz para todos os envolvidos.

4 CONSIDERAÇÕES FINAIS

A era digital transformou significativamente o cenário educacional, com a educação à distância (EAD) emergindo como uma modalidade cada vez mais prevalente. Esta transição foi acelerada por eventos globais como a pandemia de COVID-19, que obrigaram instituições de ensino a adotar rapidamente tecnologias digitais para continuar oferecendo educação de qualidade. No entanto, esse avanço trouxe consigo desafios significativos relacionados à segurança e privacidade dos dados, questões que se tornaram extremamente pertinentes no contexto educacional digital.

A proteção eficaz dos dados pessoais de alunos e professores era uma preocupação central, pois a exposição a violações e ataques cibernéticos poderia ter consequências devastadoras para a integridade pessoal e acadêmica dos envolvidos. A legislação, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, estabelecia diretrizes para o tratamento de dados pessoais, mas a aplicação prática dessas normas em ambientes educacionais digitais ainda enfrentava obstáculos significativos. Diante deste panorama, esta pesquisa visava explorar a fundo a importância do fomento da segurança e da privacidade em ambientes digitais educacionais. O estudo propôs analisar as medidas de proteção existentes, identificar as lacunas e desafios enfrentados pelas instituições de ensino e sugerir melhorias para fortalecer a segurança dos dados. Desta forma, buscava-se contribuir para a criação de um ambiente educacional mais seguro e propício ao desenvolvimento acadêmico, harmonizando as necessidades de proteção de dados com as demandas de um ensino inovador e acessível.

Perante isso, indaga-se mais uma vez: Nessa perspectiva, aqui se busca responder a seguinte questão de pesquisa: Quais são os principais desafios na implementação de medidas de segurança e privacidade em ambientes digitais educacionais e como a adequação à LGPD pode impactar a inovação pedagógica e a inclusão digital?

O fomento da segurança e da privacidade em ambientes digitais educacionais é de vital importância, constituindo um pilar fundamental para a eficácia e a integridade da educação na era digital. Com a crescente adoção de plataformas online para aprendizado e gestão educacional, a proteção de dados sensíveis se torna crucial. Violações de dados podem expor informações pessoais de alunos e professores, resultando em consequências negativas que vão desde o comprometimento da privacidade individual até repercussões legais para as instituições envolvidas. A segurança robusta impede acessos não autorizados e protege contra ameaças cibernéticas, enquanto políticas de privacidade transparentes e conformidade com normas como a Lei Geral de Proteção de Dados (LGPD) no Brasil fortalecem a confiança entre usuários e instituições educacionais. Este ambiente de confiança é essencial para que alunos e professores se sintam seguros ao compartilhar e acessar conteúdos educativos.

Diante da crescente digitalização do ensino, a segurança e a privacidade dos dados educacionais não devem ser vistas apenas como obrigações regulatórias, mas como elementos fundamentais para garantir um ambiente de aprendizado confiável e inclusivo. Este estudo evidencia a necessidade de investimentos em infraestrutura de segurança cibernética, na capacitação dos profissionais da educação e na adoção de práticas alinhadas ao conceito de *privacy by design*, assegurando que as medidas de proteção sejam incorporadas desde o planejamento das plataformas educacionais. Como perspectivas futuras, sugere-se a realização de estudos empíricos sobre o impacto da LGPD na inovação pedagógica e no acesso equitativo à educação digital.

Em síntese, a jornada para a conformidade com a LGPD no setor educacional transcende a mera formalidade legal, representando um compromisso ético e estratégico com a segurança

e o bem-estar da comunidade acadêmica. A proteção de dados, quando integrada aos processos pedagógicos e administrativos, não apenas mitiga riscos, mas também fortalece a confiança dos alunos, familiares e colaboradores na instituição. Investir em segurança cibernética, capacitar os profissionais da educação e adotar práticas de *privacy by design* são passos essenciais para construir um futuro educacional digital mais seguro, inclusivo e inovador. Ao equilibrar a proteção de dados com a promoção da inovação e da inclusão, as instituições de ensino podem criar um ambiente de aprendizado que seja ao mesmo tempo seguro, estimulante e equitativo para todos.

REFERÊNCIAS

ALMEIDA, Vinícius Tadeu *et al*. A criação de um protocolo sobre a (in)segurança digital na escola. **Anais CIET: Horizonte**, 2024. Disponível em: https://ciet.ufscar.br/submissao/index.php/ciet/article/view/2613. Acesso em: 31 jan. 2025.

ALVES, Luciene *et al*. Cidadania digital na sala de aula: desafios e oportunidades da tecnologia educacional. **Revista Ilustração**, v. 4, n. 5, p. 157-163, 2023. Disponível em: https://journal.editorailustracao.com.br/index.php/ilustracao/article/view/209. Acesso em: 31 jan. 2025.

ANTUNES NETO, Jose Nogueira; QUINTINO, Amaro Sebastião de Souza; CORRÊA, Jackeline Barcelos. A invasão de hackers na gestão educacional: Um estudo sobre a preservação de dados no ensino remoto à luz da segurança digital. In: **Anais** do Encontro Virtual de Documentação em Software Livre e Congresso Internacional de Linguagem e Tecnologia Online, 2021, v. 10, n. 1. Disponível em: https://ciltec.textolivre.pro.br/index.php/CILTecOnline/article/view/734. Acesso em: 31 jan. 2025.

ARAUJO, Ronald Carvalho Ribeiro de. **Métodos de autenticação considerando aspectos de segurança, privacidade e experiência de uso:** a visão dos usuários finais. 2022. 101 f. Dissertação (Mestrado Profissional em Computação Aplicada) – Universidade de Brasília, Brasília, 2022. Disponível em: Repositório Institucional da Universidade de Brasília.

ARAÚJO FILHO, Roberto Mariano; SILVA, Robson Santos da; SANTOS FILHO, José Elias dos. Competências digitais em projetos pedagógicos da licenciatura em matemática a distância. **EaD em Foco**, v. 14, n. 1, e2393, 2024. Disponível em: https://eademfoco.cecierj.edu.br/index.php/Revista/article/view/2393. Acesso em: 31 jan. 2025.

BEZERRA, Erich Teles *et al*. O impacto das tecnologias emergentes na educação: transformações e desafios na era digital. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n. 7, p. 2992-3003, 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/14950. Acesso em: 31 jan. 2025.

BIN, Kaio Jia. **Modelo de captura de dados por internet das coisas e disponibilização dos mesmos para uso clínico e de pesquisa seguindo as leis de proteção de dados**. 2023. 44 f. Tese (Doutorado em Ciências Médicas) – Universidade de São Paulo, São Paulo, 2023. Disponível em: Faculdade de Medicina da Universidade de São Paulo.

CUNHA, Christiane Handa Carneiro da. **Barreiras e desafios da transformação digital em um centro de serviços compartilhados com base na teoria da contingência**. 2023. 51 f. Dissertação (Mestrado Profissional em Controladoria e Finanças) – Faculdade FIPECAFI, São Paulo, 2023.

DUQUE, Marcos André. **Gêmeo digital e blockchain**: A evolução do facility management no contexto da estratégia BIM. 2022. 136 f. Dissertação (Mestrado Profissional em Governança, Tecnologia e Inovação) – Universidade Católica de Brasília, Brasília, 2022. Disponível em: Biblioteca da Universidade Católica de Brasília.

GONCALVES, Caroline Luiz. **Saúde digital**: Um estudo exploratório e proposta de arquitetura de software. 2023. 166 f. Dissertação (Mestrado em Engenharia e Gestão da Inovação) – Universidade Federal do ABC, Santo André, 2023.

MACIEL, Moises. **O direito fundamental à segurança cibernética como pressuposto da governança nas cidades digitais brasileiras**. 2022. 392 f. Tese (Doutorado em Função Social do Direito) – Faculdade Autônoma de Direito, São Paulo, 2022.

NARCISO, Rodi *et al*. Ética e privacidade na educação digital: os desafios éticos e de privacidade no uso de tecnologias digitais. **Revista Foco**, v. 17, n. 1, e4123, 2024. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/4123. Acesso em: 31 jan. 2025.

NASCIMENTO, Edinardo Aguiar do *et al*. Educação digital: riscos e desafios nas instituições escolares. **Revista Tópicos**, v. 2, n. 10, p. 1-17, 2024. Disponível em: https://revistatopicos.com.br/artigos/educacao-digital-riscos-e-desafios-nas-instituicoes-escolares. Acesso em: 31 jan. 2025.

NHANCALE, Cláudio Ângelo *et al*. Educação para a cidadania digital: o papel do professor universitário no contexto atual. **Remunom**, v. 7, n. 1, 2023. Disponível em: http://revista.unipacto.com.br/index.php/multidisciplinar/article/view/1462. Acesso em: 31 jan. 2025.

NOVAIS, Alessandra Ferreira Salgado *et al*. Promovendo segurança online no ambiente educacional moderno. **Revista Foco**, v. 17, n. 1, e4113, 2024. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/4113. Acesso em: 31 jan. 2025.

OLIVEIRA, Caio Vasconcelos. **Reflexos da Lei Geral de Proteção de Dados no setor médico hospitalar**: Uma abordagem no contexto da responsabilidade civil. 2022. 173 f.

Dissertação (Mestrado Profissional em Saúde e Educação) – Universidade de Ribeirão Preto, Ribeirão Preto, 2022.

PRACA, Marcella Leonel Viotti Leite. **Novos contornos da privacidade e intimidade em meio à sociedade da informação**: Limites para compartilhamento de dados pessoais de influenciadores digitais. 2023. Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP-SP), São Paulo, 2023.

PRAXEDES, Germano Fonseca *et al*. Desafios éticos e oportunidades na educação digital e cidadania. **Revista Amor Mundi**, v. 4, n. 7, p. 87-94, 2023. Disponível em: https://pdfs.semanticscholar.org/3109/9f0c53df7d61aa1b4af20663ddfd4b0a6ba2.pdf. Acesso em: 31 jan. 2025.

REIS, Sálvio Roberto Freitas *et al*. Desafios da LGPD quanto à privacidade em ambientes educacionais: um mapeamento sistemático. **Revista de Gestão e Secretariado**, v. 15, n. 3, e3292, 2024. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/view/3292. Acesso em: 31 jan. 2025.

SANTOS, Cynara Maria da Silva. **Tecnologias digitais móveis como dispositivo de inclusão digital do idoso**. 2022. 150 f. Tese (Doutorado em Educação) – Universidade Tiradentes, Aracaju, 2022.

SANTOS, Silvana Maria Aparecida Viana *et al*. Educação e espaço tecnológico: vantagens e riscos do ambiente digital no modelo atual. **Revista Políticas Públicas & Cidades**, v. 13, n. 2, e1242, 2024. Disponível em: https://journalppc.com/RPPC/article/view/1242. Acesso em: 31 jan. 2025.

SOUZA, Rosimar Rodrigues *et al*. Tecnologias digitais nas instituições de ensino: práticas de uso e segurança on-line. **Revista Ilustração**, v. 5, n. 1, p. 119-128, 2024. Disponível em: https://journal.editorailustracao.com.br/index.php/ilustracao/article/view/255. Acesso em: 31 jan. 2025.

VAZ, Mariana Weba Lobato. **A responsabilidade civil dos agentes de tratamento, empresas e plataformas digitais frente a violação de dados pessoais e incidentes de segurança**: Um diálogo entre as Lei nº 13.709/2018, 12.965/2014 e 8.078/1990. 2022. 151 f. Dissertação (Mestrado Profissional em Direito, Mercado, Compliance e Segurança Humana) – Faculdade CERS, Recife, 2022.