

# CIDADANIA DIGITAL: CAMINHOS PARA AMBIENTES EDUCACIONAIS SEGUROS E ÉTICOS

DIGITAL CITIZENSHIP: PATHWAYS TO SAFE AND ETHICAL EDUCATIONAL  
ENVIRONMENTS

Ciências Humanas • 21/01/2026

REGISTRO DOI: [10.5281/zenodo.18330881](https://doi.org/10.5281/zenodo.18330881)

Simone Oliveira Figueiredo<sup>1</sup>

Rivanei Moura de Figueiredo<sup>2</sup>

Ricardo Aparecido Tanaka<sup>3</sup>

## RESUMO

A crescente inserção das tecnologias digitais vem ampliando possibilidades pedagógicas e, simultaneamente, expondo instituições e usuários a novos riscos. No ambiente escolar e acadêmico, o uso intensivo das Tecnologias Digitais da Informação e Comunicação (TDICs) potencializa o acesso ao conhecimento, a gestão acadêmica e a interação pedagógica, mas também acarreta vulnerabilidades relacionadas à segurança da informação, à privacidade de dados e à saúde emocional dos estudantes. O presente artigo justifica-se pela necessidade de analisar criticamente a segurança digital no âmbito educacional, considerando sua relevância para a proteção de dados e para a formação cidadã em contextos digitais cada vez mais complexos. A pesquisa foi desenvolvida por meio de uma abordagem qualitativa, de caráter exploratório, fundamentada em levantamento. A metodologia permitiu compreender os principais riscos, vulnerabilidades e boas práticas relacionadas ao uso das tecnologias no contexto educacional. Os resultados indicam que a consolidação de uma cultura de segurança digital depende da articulação entre políticas institucionais, capacitação docente, conscientização discente e cumprimento da legislação vigente. Conclui-se que a promoção da cidadania digital e a observância da LGPD são elementos essenciais para a construção de ambientes educacionais mais seguros, éticos e inclusivos, capazes de assegurar a proteção de dados e o uso responsável das tecnologias na educação contemporânea.

**Palavras-chave:** Segurança digital; Cidadania digital; Proteção de dados; Ensino superior; LGPD.

## ABSTRACT

The growing integration of digital technologies has expanded

pedagogical possibilities while simultaneously exposing institutions and users to new risks. In school and academic environments, the intensive use of Digital Information and Communication Technologies (DICTs) enhances access to knowledge, academic management, and pedagogical interaction; however, it also generates vulnerabilities related to information security, data privacy, and students' emotional well-being. This article is justified by the need to critically analyze digital security in the educational context, considering its relevance to data protection and to the development of citizenship in increasingly complex digital environments. The research was conducted through a qualitative, exploratory approach, based on a literature review. This methodology made it possible to identify the main risks, vulnerabilities, and best practices related to the use of technologies in the educational context. The results indicate that the consolidation of a digital security culture depends on the articulation of institutional policies, teacher training, student awareness, and compliance with current legislation. It is concluded that the promotion of digital citizenship and compliance with the General Data Protection Law (LGPD) are essential elements for building safer, more ethical, and more inclusive educational environments, capable of ensuring data protection and the responsible use of technologies in contemporary education.

**Keywords:** Digital security; Digital citizenship; Data protection; Higher education; LGPD.

## 1. INTRODUÇÃO

A tecnologia está profundamente inserida no cotidiano contemporâneo, permeando praticamente todas as esferas da vida social. Desde o momento em que o indivíduo desperta até o instante em que se recolhe para o descanso, é difícil encontrar

situações completamente dissociadas de algum recurso tecnológico. Dispositivos como telefones celulares, computadores e meios de transporte ilustram a ubiquidade da tecnologia no dia a dia. Mesmo ambientes tradicionalmente domésticos, como a cozinha, foram transformados pela introdução de equipamentos que promovem praticidade e otimizam o tempo — a exemplo das panelas elétricas e outros utensílios automatizados

Essa presença constante, evidencia que a tecnologia se consolidou como um elemento importante para o funcionamento da vida moderna, trazendo benefícios relacionados à eficiência, comodidade e segurança. Contudo, ao transpor esse cenário para o campo educacional, torna-se imprescindível refletir criticamente sobre seu uso. O ambiente escolar, cada vez mais mediado pelas tecnologias digitais de informação e comunicação (TDICs) incluindo uso de plataformas digitais, armazenamento em nuvem e sistemas de gestão acadêmica, passou também a estar suscetível a riscos cibernéticos, como o vazamento de dados, ataques a sistemas institucionais, phishing, episódios de cyberbullying e outras exposições prejudiciais à saúde física e psicológica do usuário.

Diante desse contexto, o presente estudo tem como objetivo geral analisar medidas de segurança digital aplicáveis ao ambiente educacional, buscando compreender de que maneira é possível garantir a proteção de dados e a integridade das práticas pedagógicas mediadas pelas TDICs. Como objetivos específicos, pretende-se: (1) identificar os principais riscos e vulnerabilidades que afetam as instituições de ensino; (2) Cidadania Digital e LGPD e; (3) revisar boas práticas de segurança digital já adotadas no contexto educacional.

Para alcançar tais objetivos, este trabalho está estruturado em seções complementares. Inicialmente, apresenta-se uma fundamentação teórica, que discute os conceitos de segurança digital e sua relação com o ambiente educacional, bem como os principais riscos e desafios associados ao uso de tecnologias nesse contexto através da metodologia qualitativa pautada em referencial bibliográfico. Por fim, nas considerações finais, são apresentadas as conclusões e sugestões e ações voltadas ao fortalecimento da segurança digital na educação.

Além disso, a intensificação do uso das tecnologias digitais no contexto educacional foi significativamente acelerada nos últimos anos, especialmente em decorrência da expansão do ensino remoto e híbrido, impulsionada por situações emergenciais, como a pandemia da COVID-19. Esse cenário evidenciou, de forma ainda mais contundente, a dependência das instituições de ensino em relação às infraestruturas digitais para a continuidade das atividades pedagógicas e administrativas. Ao mesmo tempo, expôs fragilidades relacionadas à cultura de segurança da informação, à formação de docentes e discentes para o uso consciente e responsável das tecnologias, bem como à adequação das instituições às exigências legais e éticas relacionadas à proteção de dados pessoais. Assim, torna-se fundamental que a incorporação das TDICs na educação seja acompanhada por políticas institucionais consistentes de segurança digital, programas de conscientização e ações preventivas que promovam a cidadania digital, assegurando não apenas a continuidade dos processos educacionais, mas também a proteção dos sujeitos envolvidos e a confiabilidade dos ambientes digitais de aprendizagem.

## **2. SEGURANÇA DIGITAL NO ÂMBITO EDUCACIONAL**

A cibersegurança educacional compreende o conjunto de políticas, tecnologias e práticas voltadas à proteção de dados, sistemas e usuários no ambiente digital das instituições de ensino. Esse campo busca assegurar a integridade, a confidencialidade e a disponibilidade das informações acadêmicas e administrativas, prevenindo incidentes que possam comprometer a operação institucional.

Nos últimos anos, a cibersegurança tem se consolidado como uma das principais preocupações no contexto educacional, uma vez que escolas e universidades administram diariamente um volume expressivo de dados — incluindo informações pessoais, registros acadêmicos e dados financeiros de estudantes, docentes e colaboradores. Tal cenário evidencia a necessidade de estratégias robustas de proteção digital e de uma cultura institucional voltada à segurança da informação.

De acordo com Sêmola (2014) a segurança da informação é definida como um campo de conhecimento voltado à proteção dos ativos informacionais, buscando prevenir acessos não autorizados, modificações indevidas e a indisponibilidade dos dados.

A ausência de segurança no ambiente educacional acarreta riscos e vulnerabilidades com grande potencial de danos, uma vez que falhas no controle de acesso às bases de dados podem permitir invasões, vazamento de informações sensíveis e manipulação indevida de registros acadêmicos e financeiros. Esses incidentes não apenas comprometem a privacidade de estudantes, docentes e colaboradores, mas também podem afetar a continuidade das atividades institucionais, gerando prejuízos administrativos e reputacionais.

## **2.1. Riscos e Vulnerabilidades**

### **2.1.1. Riscos**

Na perspectiva educacional contemporânea, torna-se imperativo reconhecer que o papel das instituições de ensino ultrapassa a mera transmissão de conteúdos disciplinares. Nesse viés, os envolvidos no processo de ensino-aprendizagem devem inculcar no estudante a necessidade de atuar de forma crítica, autônoma e cidadã em um contexto permeado pelas tecnologias digitais. Essa autonomia implica não apenas a capacidade de utilizar os recursos tecnológicos de maneira eficiente, mas também a compreensão das responsabilidades e das consequências decorrentes de seu uso. Nesse sentido, incentivar a busca ativa por informações deve ser acompanhado da formação para a consciência dos riscos, das vulnerabilidades e dos desafios éticos que emergem do ambiente tecnológico.

De acordo com Santos (2022), embora as Tecnologias da Informação e Comunicação (TICs) promovam, de forma indireta, o desenvolvimento social e cultural, seu avanço também tem sido utilizado para práticas nocivas, como roubo de dados, perseguições, uso indevido de imagens e cyberbullying. A autora aponta que esses problemas estão, em grande parte, ligados à falta de ingerência dos usuários, que, por não saberem como se comportar nesse novo contexto digital, acabam se tornando facilmente manipuláveis e / ou manipuladores.

As Tecnologias da Informação e Comunicação (TICs), embora promovam o acesso facilitado ao conhecimento e agilizem o processo de ensino-aprendizagem, também ampliam os riscos

relacionados à coleta, manipulação e uso indevido de dados pessoais. Por meio de algoritmos, é possível delinear perfis de usuários e influenciar comportamentos de forma sutil, tornando-os mais suscetíveis à exposição e à desinformação. Essa condição favorece o contato com conteúdos falsos e práticas fraudulentas, dificultando a distinção entre informações verídicas e enganosas, o que pode acarretar desde danos mínimos até consequências graves e duradouras.

Entre os principais riscos associados ao uso das TICs estão a invasão de privacidade, o cyberbullying e o pu, a propagação de fake news, a dependência digital, a exposição a conteúdos impróprios e a manipulação comportamental.

De acordo com Andrade “O cyberbullying acaba por ser um problema difícil de erradicar, comparativamente ao bullying, uma vez que aquele possibilita que o agressor se esconda no anonimato proporcionado pela internet ou telemóvel devido à acessibilidade da vítima, que se encontra exposta a várias humilhações constantes. ” (Andrade, 2012, p. 2).

Nessa perspectiva, Pereira e Pinto (2018) destacam a relevância de um projeto pedagógico voltado não apenas para a identificação de práticas de cyberbullying, mas também para a compreensão dos procedimentos legais necessários à coleta de provas válidas. Tal proposta busca orientar os estudantes quanto às formas adequadas de reconhecer essas situações e aos caminhos institucionais e jurídicos disponíveis para a busca de apoio e resolução do problema.

Outrossim, O ambiente digital também apresenta riscos crescentes, como o phishing e o malware. O primeiro refere-se a fraudes que

enganam o usuário para obter informações pessoais por meio de mensagens falsas, enquanto o segundo diz respeito a softwares maliciosos criados para danificar ou invadir sistemas. Tais ameaças reforçam a necessidade de alfabetização digital e de práticas de segurança cibernética que promovam um uso mais consciente e protegido desses males.

Nesse cenário, evidencia-se que a discussão sobre os riscos associados às Tecnologias da Informação e Comunicação no contexto educacional não pode ser dissociada da necessidade de estruturar ações pedagógicas, institucionais e formativas voltadas à prevenção e à conscientização. A exposição a práticas como cyberbullying, phishing, disseminação de desinformação e uso indevido de dados pessoais revela que o ambiente digital, embora promissor, demanda mediações educativas sistemáticas e contínuas. Assim, torna-se imprescindível que as instituições de ensino incorporem a segurança digital como eixo transversal de seus projetos pedagógicos, articulando conteúdos curriculares, práticas educativas e políticas institucionais. Essa abordagem integrada cria condições para que estudantes e educadores desenvolvam competências críticas e éticas no uso das tecnologias, ao mesmo tempo em que prepara o terreno conceitual para a análise das vulnerabilidades, da legislação vigente e das estratégias de proteção digital, temas que serão aprofundados nas seções subsequentes do presente trabalho.

### **2.1.2. Vulnerabilidade**

De acordo com o CERT (2012) a vulnerabilidade consiste em falha ou fragilidade que, quando utilizada por um invasor, pode resultar na violação de medidas de proteção da informação. Identificar as

possíveis vulnerabilidades podem impedir falhas na segurança da informação.

No contexto das instituições de ensino, a segurança da informação é frequentemente comprometida por práticas e configurações inadequadas. O uso de senhas fracas ou reutilizadas por estudantes e docentes constitui uma vulnerabilidade crítica, pois facilita o acesso indevido a sistemas e dados institucionais.

A utilização de redes Wi-Fi desprotegidas, isto é, conexões sem criptografia ou autenticação robusta, também representa um risco relevante, possibilitando a interceptação de informações sensíveis. Outro fator é o uso de dispositivos pessoais não gerenciados, comum em ambientes que adotam a política BYOD (Bring Your Own Device) — prática que permite o uso de equipamentos próprios, como notebooks e smartphones, sem o controle direto da instituição.

Além disso, o uso de softwares desatualizados — sistemas operacionais e aplicativos sem atualizações ou patches de segurança — amplia a exposição a ataques cibernéticos. Por fim, a ausência de backups regulares reduz a capacidade de recuperação de dados e compromete a continuidade das atividades em caso de incidentes.

Adicionalmente, a falta de políticas institucionais claras e de programas sistemáticos de conscientização em segurança da informação contribui para o agravamento dessas vulnerabilidades no ambiente educacional. Muitas instituições de ensino ainda não dispõem de normas bem definidas sobre o uso adequado dos sistemas, a proteção de credenciais, o armazenamento de dados

sensíveis e a resposta a incidentes de segurança. Soma-se a isso a carência de capacitação contínua de docentes, técnicos e discentes quanto às boas práticas de segurança digital, o que favorece comportamentos de risco, como o compartilhamento indevido de informações, a abertura de links suspeitos e a instalação de aplicações não confiáveis. Dessa forma, a ausência de uma cultura institucional de segurança da informação amplia a superfície de ataque e compromete a proteção dos dados acadêmicos e administrativos, tornando imprescindível a adoção de estratégias preventivas, educativas e tecnológicas integradas.

## **2.2. Cidadania Digital e a LGPD**

A Lei Geral de Proteção de Dados (LGPD) — Lei nº 13.709/2018 — representa um marco regulatório fundamental no ordenamento jurídico brasileiro ao estabelecer princípios, direitos e deveres relacionados ao tratamento de dados pessoais, tanto no setor público quanto no privado. Seu surgimento está diretamente associado ao avanço acelerado das tecnologias da informação e comunicação, ao aumento exponencial da circulação de dados no ambiente digital e à necessidade de proteger os indivíduos diante de práticas abusivas, uso indevido de informações e violações à privacidade. A legislação define parâmetros rigorosos para a coleta, o armazenamento, o compartilhamento e a eliminação de dados pessoais, exigindo que essas operações sejam realizadas de forma lícita, transparente, segura e alinhada a finalidades legítimas, previamente informadas aos titulares dos dados.

O objetivo central da LGPD é assegurar que as informações pessoais sejam geridas de maneira ética e responsável, garantindo ao cidadão maior controle sobre seus próprios dados. Para isso, a lei

consagra direitos fundamentais, como o acesso às informações, a correção de dados incompletos ou incorretos, a revogação do consentimento e a possibilidade de eliminação de dados tratados de forma inadequada. Ao mesmo tempo, impõe obrigações às organizações, que passam a responder civil, administrativa e, em alguns casos, penalmente por falhas na proteção das informações sob sua responsabilidade. Dessa forma, a LGPD atua como um instrumento de equilíbrio entre inovação tecnológica e proteção da dignidade humana, reconhecendo os dados pessoais como uma extensão da personalidade do indivíduo.

Nesse cenário, a legislação se relaciona de forma direta e indissociável com o conceito de cidadania digital, entendido como a capacidade de exercer direitos e cumprir deveres no ambiente virtual de maneira consciente, ética e responsável. A cidadania digital vai além do simples uso das tecnologias, abrangendo a compreensão crítica dos impactos sociais, jurídicos e éticos das ações realizadas no meio digital. Entre suas práticas fundamentais estão o respeito à privacidade, à propriedade intelectual, à veracidade das informações e à segurança dos dados, bem como a adoção de comportamentos responsáveis no compartilhamento de conteúdos e na interação em plataformas digitais.

Ao operacionalizar esses princípios, a LGPD contribui de forma significativa para o fortalecimento da cidadania digital, ao estabelecer normas claras que orientam tanto os usuários quanto as organizações sobre o uso adequado das informações pessoais. A lei promove a transparência nas relações digitais, estimula a responsabilidade no tratamento de dados e reforça a necessidade de consentimento informado, permitindo que o indivíduo compreenda como, por que e por quem seus dados estão sendo

utilizados. Esse protagonismo do titular dos dados é essencial para o exercício pleno da cidadania no ambiente digital, pois transforma o cidadão em um agente ativo na proteção de sua própria privacidade.

No contexto educacional, a relação entre LGPD e cidadania digital torna-se ainda mais relevante, uma vez que instituições de ensino lidam diariamente com grande volume de dados pessoais de estudantes, professores, colaboradores e familiares. Informações acadêmicas, registros administrativos, dados sensíveis e conteúdos digitais exigem cuidados específicos quanto ao armazenamento, ao acesso e ao compartilhamento. A aplicação efetiva da LGPD nas escolas e instituições de ensino superior não se limita ao cumprimento legal, mas assume um papel pedagógico ao promover uma cultura de proteção de dados e de responsabilidade digital.

Assim, enquanto a cidadania digital orienta estudantes e educadores quanto ao uso ético, seguro e consciente das tecnologias, a LGPD fornece o arcabouço legal e normativo necessário para garantir a segurança, a confidencialidade e a transparência no tratamento das informações. A integração desses dois conceitos contribui para a formação de indivíduos críticos, conscientes de seus direitos e deveres no ambiente digital, capazes de atuar de forma responsável em uma sociedade cada vez mais orientada por dados. Dessa maneira, a adoção de práticas alinhadas à LGPD no ambiente educacional fortalece não apenas a conformidade jurídica das instituições, mas também o desenvolvimento de uma cultura digital ética, segura e cidadã.

## **2.3. Práticas de Segurança Digital Que Devem Ser Adotadas no Contexto Educacional**

No contexto educacional, as práticas de segurança digital têm se consolidado como parte essencial da formação para a cidadania digital, que implica compreender e exercer de forma ética os direitos e deveres no ambiente online. Essa abordagem envolve o respeito à privacidade, à propriedade intelectual e à responsabilidade no uso das tecnologias, aspectos enfatizados por Greenhow e Robelia (2009) ao destacarem a importância de preparar os indivíduos para uma participação consciente, segura e crítica no espaço digital.

Nesse sentido, as instituições de ensino, referente a adoção de práticas voltadas à segurança digital devem garantir:

1. Ambiente educacional protegido e consciente. As escolas devem investir em plataformas tecnológicas seguras e estabelecer protocolos claros de prevenção e resposta a situações de abuso ou violação on-line, assegurando a integridade física e emocional da comunidade escolar.
2. A capacitação docente em segurança digital é essencial para que educadores possam orientar os estudantes quanto ao uso ético e responsável das tecnologias.
3. As políticas institucionais também desempenham um papel decisivo, pois definem diretrizes e promovem uma cultura de proteção e respeito no meio digital.
4. Por fim, a cooperação entre família, escola e órgãos públicos é indispensável para o enfrentamento eficaz dos riscos

cibernéticos, fortalecendo a formação cidadã e a construção de um espaço virtual mais seguro e inclusivo.

Sobre essa ótica Valente e Almeida (2018) pontuam que a segurança digital deve ser compreendida como uma responsabilidade compartilhada, sustentada por ações e campanhas de conscientização que envolvam de forma integrada toda a comunidade escolar.

Diante das discussões apresentadas, observa-se que a segurança digital no âmbito educacional configura-se como um campo multifacetado, que envolve dimensões técnicas, pedagógicas, legais e sociais. A compreensão dos riscos e vulnerabilidades associados ao uso intensivo das Tecnologias da Informação e Comunicação, bem como a incorporação dos princípios da cidadania digital e da Lei Geral de Proteção de Dados, evidencia que a proteção do ambiente educacional extrapola a adoção isolada de ferramentas tecnológicas. Trata-se, sobretudo, da construção de uma cultura institucional pautada na responsabilidade compartilhada, na formação crítica dos sujeitos e na implementação de práticas contínuas de prevenção e conscientização. Nesse sentido, a segurança digital deve ser entendida como um elemento estruturante das práticas educacionais contemporâneas, capaz de sustentar ambientes de aprendizagem mais seguros, éticos e alinhados às exigências da sociedade digital.

### **3. CONSIDERAÇÕES FINAIS**

O presente estudo evidenciou que a segurança digital constitui um elemento indispensável para a proteção de dados pessoais e a promoção de práticas éticas no ambiente educacional. A análise

revelou que, embora as Tecnologias da Informação e Comunicação (TICs) ampliem as possibilidades de acesso ao conhecimento e facilitem a disseminação de informações, elas também expõem estudantes, docentes e instituições a riscos significativos, como cyberbullying, phishing, malware e vazamento de dados sensíveis.

A relação entre cidadania digital e a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) mostrou-se central para a construção de um ambiente escolar seguro e ético. A cidadania digital orienta indivíduos sobre direitos e deveres no espaço virtual, enquanto a LGPD fornece as bases legais e diretrizes para assegurar a integridade, confidencialidade e transparência no tratamento de informações pessoais. Assim, a implementação de políticas institucionais, plataformas seguras, capacitação docente e campanhas de conscientização revelou-se essencial para mitigar vulnerabilidades e fortalecer uma cultura de proteção digital.

Por fim, os resultados indicam que a consolidação de práticas de segurança digital no contexto educacional depende da cooperação integrada entre escolas, famílias e órgãos públicos, criando um ecossistema que favorece a formação crítica, ética e consciente dos estudantes. Dessa forma, assegurar o cumprimento da LGPD e promover a cidadania digital não apenas atende às exigências legais, mas também contribui para a construção de uma educação mais responsável, segura e inclusiva na era digital.

## **REFERÊNCIAS BIBLIOGRÁFICAS**

ANDRADE, L. C. F. (2012). Bullying e cyberbullying: Um estudo no contexto escolar particular cooperativo. Universidade da Madeira.

BRASIL. (2018). Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018). Diário Oficial da União.

CERT BRASIL. (2012). Cartilha de segurança para a Internet, versão 4.0. Comitê Gestor de Internet no Brasil.

GREENHOW, C., & ROBELIA, B. (2009). Informal learning and identity formation in the digital age.

SANTOS, C. (2022). Educação, práticas digitais e novos riscos em rede. In Anais do XXVIII Workshop de Informática na Escola (pp. 338–347). Sociedade Brasileira de Computação.

SÊMOLA, M. (2014). Gestão da segurança da informação: Uma visão executiva (2ª ed.). Elsevier.

VALENTE, J. A., & ALMEIDA, F. (2018). Educação e cidadania digital: Desafios no ambiente escolar. Editora Ciência & Educação.

---

<sup>1</sup> Graduação em Turismo – Universidade Plínio Leite, Pós Graduação Lato Sensu Pedagogia Empresarial – UCAM, Pós graduanda em psicopedagogia institucional e clínica – PROMINAS. Mestranda Must University Florida – USA – Master of Science in Emergent Technologies in Education E-mail: [acesse o artigo original para visualizar o e-mail.](#)

<sup>2</sup> Graduado em Matemática Faculdade Castelo Branco. Pós graduado em Matemática Faculdade de Filosofia Campo Grande – FEUC. Mestrando Must University Florida - Master of Science in Emergente Technologies in Education, E-mail: [acesse o artigo original para visualizar o e-mail.](#)

<sup>3</sup> Graduado em Ciências Econômicas e Ciência Contábeis pela FECAP. Especialista em Controladoria pela FECAP. Especialista em Gestão Empresarial – Executivo Internacional pela FGV. Mestrando em Administração de Empresas pela Must University. E-mail: [acesse o artigo original para visualizar o e-mail.](#)