

SEGURANÇA DIGITAL E A CIDADANIA DIGITAL NAS INSTITUIÇÕES EDUCACIONAIS

DIGITAL SECURITY AND DIGITAL CITIZENSHIP IN EDUCATIONAL INSTITUTIONS

Dilza Soares Vilas Boas

MUST University, Estados Unidos

Maria Aparecida dos Santos

MUST University, Estados Unidos

Deusli Maria de Melo

MUST University, Estados Unidos

Idelma Pereira de Basto Santos

MUST University, Estados Unidos

Luciani Marriel

MUST University, Estados Unidos

Girlene Gomes Sá

MUST University, Estados Unidos

Priscila Menezes Almeida

MUST University, Estados Unidos

ISSN: 1518-0263

DOI: <https://doi.org/10.46550/54cmtb76>

Accito em: 06.09.2026

Resumo: Este artigo foi elaborado a partir das referências bibliográficas, com reflexões fundamentadas na disciplina Tecnologia baseado no computador em sala de aula com discussões acerca da segurança digital é um tema cada vez mais relevante no contexto das instituições educacionais, onde a tecnologia é utilizada para apoiar o aprendizado e a comunicação. Na introdução será realizada uma abordagem sobre os desafios e oportunidades com a segurança digital - cidadania digital (direitos e deveres *online*): práticas e riscos no contexto das instituições educacionais. No desenvolvimento a partir das referências bibliográficas com discussões com relação a geral sobre a educação que é fundamental para promover a segurança digital e a cidadania digital com a tecnologia que pode ser uma ferramenta poderosa para promover a segurança digital e a cidadania digital. Além das políticas das instituições educacionais devem ter políticas claras e eficazes para promover a segurança digital e a cidadania digital. E por fim, a pesquisa possibilitou uma revisão detalhada sobre o tema, analisando diversos contextos e práticas, e reafirmando a relevância da segurança digital e a cidadania digital são temas importantes que devem ser abordados nas instituições educacionais. Com a utilização de práticas de segurança digital e cidadania digital, é possível promover um ambiente online seguro e respeitoso.

Palavras-chave: Educação digital. Direitos e deveres. Desafios. Privacidade. Riscos.

Abstract: This article was prepared based on bibliographic references, with reflections grounded in the discipline Computer-Based Technology in the Classroom, with discussions about digital security, which is an increasingly relevant topic in the context of educational institutions where technology is used to support learning and communication. The introduction will provide an approach on the challenges and opportunities related to digital security - digital citizenship (rights and duties online): practices and risks in the context of educational institutions. In the development section, based on bibliographic references, discussions will be made regarding general aspects of education, which are fundamental to promoting digital security and digital citizenship with technology that can be a powerful tool to promote digital security and digital citizenship. In addition, educational institutions should have clear and effective policies to promote digital security and digital citizenship. Finally, the research enabled a detailed review of the topic, analyzing various contexts and practices, and reaffirming the relevance of digital security and digital citizenship as important topics that should be addressed in educational institutions. By using digital security and digital citizenship practices, it is possible to promote a safe and respectful online environment.

Keywords: Digital education. Rights and duties. Challenges. Privacy. Risks.

Introdução

Esta pesquisa foi embasada nas referências bibliográficas de vários autores Reis (2021), Ferreira e Monteiro (2009), Melão (2011) entre outros que abordam o mesmo assunto sobre Segurança digital - cidadania digital (direitos e deveres *online*): práticas e riscos no contexto das instituições educacionais.

Segurança Digital e Cidadania Digital: Práticas e Riscos no Contexto das Instituições Educacionais, sendo um enfoque cada vez mais relevante no contexto das instituições educacionais, onde a tecnologia é utilizada para apoiar o aprendizado e a comunicação.

As práticas de segurança digital com o uso de senhas fortes ao utilizar senhas fortes e únicas para todas as contas online; autenticação de dois fatores ao utilizar autenticação de dois

fatores para adicionar uma camada extra de segurança às contas online; atualização de *software* que é bom manter o *software* atualizado para garantir que as vulnerabilidades sejam corrigidas. Além do cuidado com *links* e anexos, sendo bom ter cuidado ao clicar em links ou abrir anexos de fontes desconhecidas.

Os riscos de segurança digital como o *Phishing* que são golpes que visam obter informações confidenciais, como senhas ou números de cartão de crédito; o *Malware* que é *software* malicioso que pode danificar ou roubar informações; o *cyberbullying* com comportamento agressivo ou intimidador online que pode causar danos psicológicos. Além da privacidade com a exposição de informações pessoais online pode ser um risco para a privacidade.

Cidadania digital com direitos aos usuários têm direito à privacidade, à liberdade de expressão e à segurança *online*; os deveres dos usuários têm o dever de respeitar os direitos dos outros, de não compartilhar conteúdo ilegal ou prejudicial e de proteger suas informações pessoais.

Práticas de cidadania digital com respeito *online* ao tratar os outros com respeito e dignidade *online*; o compartilhamento responsável de informações de forma responsável e verificada. Bem como a proteção de privacidade e das informações pessoais e respeitar a privacidade dos outros.

Desafios e oportunidades com a educação é fundamental para promover a segurança digital e a cidadania digital; a tecnologia pode ser uma ferramenta poderosa para promover a segurança digital e a cidadania digital. Assim como as políticas nas instituições educacionais devem ter políticas claras e eficazes para promover a segurança digital e a cidadania digital.

A segurança digital e a cidadania digital são temas importantes que devem ser abordados nas instituições educacionais. Com a utilização de práticas de segurança digital e cidadania digital, é possível promover um ambiente online seguro e respeitoso.

Desenvolvimento

Este estudo adotou como metodologia a pesquisa bibliográfica para investigar a Segurança digital - cidadania digital (direitos e deveres *online*): práticas e riscos no contexto das instituições educacionais, com o objetivo de analisar e compreender que a segurança digital é uma abordagem cada vez mais relevante no contexto das instituições educacionais, onde a tecnologia é utilizada para apoiar o aprendizado e a comunicação, desenvolvida a partir da leitura e levantamentos apresentados em consulta de fontes secundárias e material de vários autores sobre um mesmo tema.

Segundo Fonseca (2002, p.32).

A pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto. Existem, porém, pesquisas científicas que se baseiam unicamente na pesquisa bibliográfica, procurando referências teóricas publicadas como objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta.

A pesquisa bibliográfica é uma técnica que consiste na busca e análise crítica da produção científica disponível sobre um determinado tema, utilizando-se de fontes para buscar as informações necessárias para responder ao problema de pesquisa e promover o aprofundamento da discussão.

A segurança e a cidadania digital nas instituições educacionais envolvem práticas éticas, proteção de dados e conscientização sobre os riscos do ambiente *online*. É essencial formar alunos e educadores para atuarem com responsabilidade e respeito no mundo digital.

Segurança digital nas escolas refere-se à proteção de dados pessoais, privacidade e integridade das informações no ambiente virtual. Nas instituições educacionais, isso incluem a proteção de redes e sistemas escolares contra invasões, vazamentos e ataques cibernéticos; o uso responsável de senhas e autenticação para acesso a plataformas educacionais; orientação sobre *phishing*, *fake news* e engenharia social, que podem afetar alunos e professores. Além das políticas claras de uso de dispositivos e internet, com regras sobre downloads, compartilhamento de arquivos e acesso a conteúdo. Essas práticas visam garantir um ambiente seguro para o aprendizado e a comunicação digital.

A cidadania digital direitos e deveres, pois envolve o exercício consciente e ético da participação online. No contexto educacional, isso significa que o direito à privacidade e à proteção de dados pessoais dos alunos e profissionais; o dever de respeitar os outros usuários, evitando *cyberbullying*, discurso de ódio e violação de direitos autorais; a participação ativa e crítica em ambientes digitais, como fóruns, redes sociais e plataformas de ensino. Bem como a inclusão digital, garantindo acesso equitativo às tecnologias e à internet para todos os estudantes.

A cidadania digital também está ligada à educação para a democracia, promovendo valores como respeito à diversidade, igualdade de oportunidades e atuação cívica *online* Anatel.

Os riscos e desafios em que as instituições enfrentam diversos riscos no ambiente digital com a exposição indevida de dados escolares e pessoais por falta de controle ou conhecimento; o *cyberbullying* entre alunos, que pode afetar o bem-estar e o desempenho escolar; a desinformação e uso inadequado de redes sociais, prejudicando o ambiente educativo. Além da falta de formação dos educadores sobre práticas seguras e cidadania digital.

Boas práticas para mitigar esses riscos, é recomendável capacitar professores, gestores e alunos sobre segurança e ética digital; implementar políticas de uso de tecnologia com foco em proteção e respeito; promover projetos pedagógicos que abordem cidadania digital e segurança *online*. Bem como utilizar ferramentas de controle e monitoramento com transparência e consentimento.

Segurança digital e cidadania digital (direitos e deveres *online*) nas instituições educacionais: práticas, riscos e referências úteis.

Conceitos-chave sobre segurança digital: proteger dados, sistemas e pessoas (confidencialidade, integridade e disponibilidade). ISO 27001 chama isso de “SGSI” — um sistema de gestão com controles organizacionais, humanos, físicos e tecnológicos baseados em risco.

A cidadania digital: uso ético, seguro e responsável da tecnologia (direitos, deveres, participação e pensamento crítico). Diretrizes atuais da UNESCO focam em empoderar educadores e alunos para agir de forma ética e resiliente *online*.

Direitos e deveres *online* (contexto escolar) com os direitos do aluno/servidor/família com a privacidade e proteção de dados (transparência, acesso, retificação, limitação, portabilidade,

oposição, apagamento quando cabível). No espaço europeu/UK: GDPR/UK GDPR + leis nacionais; escolas precisam nomear/envolver um Encarregado/DPO e ter políticas claras.

O ambiente seguro (prevenção de assédio, discurso de ódio e discriminação). As diretrizes de cidadania digital da UNESCO ligam segurança digital a inclusão e bem-estar. Os deveres da instituição e da comunidade escolar ao minimizar coleta de dados, informar finalidades, gerenciar consentimento (especialmente para menores), aplicar controles de acesso e registrar incidentes. Órgãos espanhóis (AEPD) e britânicos (GOV.UK/ICO) mantêm guias específicos para centros educativos.

Principais riscos no contexto educacional como *Phishing*/engenharia social; *ransomware*; vazamentos por má configuração de plataformas de colaboração; *cyberbullying*/sextorção; *deepfakes* e vigilância/biometria desproporcionais (especial atenção a dados sensíveis de crianças). Casos recentes mostram escrutínio sobre uso de biometria e falhas em plataformas escolares.

Práticas recomendadas (o que implementar na escola) com governança e conformidade ao *bomear* DPO; mapa de dados; base legal; PIA/DPIA para novos sistemas; contratos com operadores; plano de resposta a incidentes; registros de tratamento. (Modelos/roteiros oficiais para escolas no GOV.UK/ICO e AEPD).

Controles técnicos essenciais com MFA para contas de *staff*/alunos; princípio do menor privilégio; gestão de patches; *backups* 3-2-1; criptografia em repouso e em trânsito; listas de permissões em drives e *VLEs*; *logs* e alertas. Esses controles alinham-se a ISO 27001 e ao NIST CSF 2.0 (funções: Governar, Identificar, Proteger, Detectar, Responder, Recuperar).

Políticas e processos com AUP/Política de uso aceitável para alunos e colaboradores; política de senhas/MFA; política de dispositivos (BYOD/MDM); política de fotografia/biometria; gestão de fornecedores (edtech). Modelos e checklists setoriais: GOV.UK toolkit; SWGfL.

Capacitação contínua com programa de cidadania digital por faixa etária (currículo gratuito da *Common Sense UK*).

Na era digital atualmente, a tecnologia desempenha um papel cada vez mais importante na formação da cidadania e no contexto educacional. A interseção entre cidadania, educação e tecnologia apresenta novas oportunidades e desafios que precisam ser compreendidos e explorados.

Nesse contexto, quando se aborda sobre a interseção entre cidadania, educação e tecnologia, é questionado sobre como essas três ferramentas se conectam e se influenciam. A educação é o pilar central no processo de formação de cidadãos conscientes, engajados e capazes de participar ativamente na sociedade. No entanto, com o advento das tecnologias digitais, a natureza da educação está em constante transformação.

Além disso, outros obstáculos institucionais são observados, como por exemplo: entendimento e compreensão de que a cidadania digital é uma competência a ser desenvolvida

nas escolas; reestruturação curricular, tornando-o mais flexível e atualizado frente as evoluções sociais e tecnológicas; atualização dos currículos formativos dos docentes que frequentemente negligenciam a temática referente a cidadania digital; discussão e reflexão por toda a comunidade escolar sobre as práticas de ensino que apresentam riscos e vulnerabilidades digitais.

Considerações finais

A partir da revisão integrativa da literatura foi possível identificar quais estratégias poderão ser executadas para trabalhar a cidadania digital no contexto educacional. Percebe-se que o ambiente educacional é responsável pela formação cidadã, social e pedagógica dos alunos, e assim, deverá prepara-lo para os desafios que este encontrará no convívio em uma sociedade contemporânea globalizada, tecnológica, interativa e conectada. Além disso, precisará entender as transformações que os próprios processos educativos sofreram diante da incorporação das tecnologias digitais da informação e comunicação.

As instituições de ensino deverão promover debates com exposição de casos verídicos para demonstração sobre a responsabilidade do bom uso da tecnologia. Utilizar a cidadania digital juntamente com as boas práticas digitais e a segurança da informação serão primordiais para promover um diálogo de aproximação e não de condenação aos seus alunos, porém, é relevante que os alunos sejam levados a ter a sensibilidade e a clareza quanto a responsabilidade que ele tem ao utilizar essa ferramenta, trazendo também os pais a participar mais amplamente deste diálogo, quando alunos menores de idade. Precisarão analisar e identificar quais pontos são mais relevantes a serem trabalhados dentro dos processos educativos, como por exemplo, as questões de privacidade, direitos autorais e uso ético das redes sociais. Deverá haver a

percepção que as tecnologias digitais estão constantemente evoluindo, sendo acompanhados dos riscos digitais, e a escola deverá ter um canal de comunicação aberto com a comunidade escolar para discussão de boas práticas digitais e atitudes protetivas frente as vulnerabilidades digitais. É percebido um grande desafio para as escolas e todas as redes de ensino: o de geração de uma cultura de paz e antiviolença digital, oportunizando aos alunos se desenvolverem em um ambiente saudável e capazes de se tornarem cidadãos críticos e participativos na sociedade em que estiverem inseridos. Isso, é o que se espera da educação.

Referências

- Base Nacional Comum Curricular [BNCC]. (2018). Ministério da Educação. Disponível em <http://basenacionalcomum.mec.gov.br/>. Acessado em 20 de out. de 2025.
- Belloni, M. L. (1999). Educação a distância (2ª ed.). São Paulo, SP: Editora Autores Associados.
- Ferreira, P., & Monteiro, A. F. (2009). Riscos de Utilização das TIC. EDUSER: Revista

de Educação. Vol.1. ISSN 1645-4774.

Lei nº 12.965, de 23 de abril de 2014. (2014). Marco Civil da Internet. Brasília, DF: Diário Oficial da União. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 11 de out. de 2025.

Netto, C. M. (2018b). Comunicação na era digital. [e-book] Flórida: Must University.

Netto, C. M. (2018c). Segurança on-line. [e-book] Flórida: Must University.

Netto, C. M. (2018a). Sociedade da informação e do conhecimento e a educação. [e-book] Flórida: Must University.

Melão, D. H. M. R. (2011). Da página ao(s) ecrã(s): tecnologia, educação e cidadania digital no século XXI. Educação, Formação & Tecnologias. Revista EFT: <http://eft.educom.pt> 89. 4(2), 89-107.

Reis, A. F. C. (2021). Tecnologia Digital na Educação Infantil: potencialidade e cuidados. Paripiranga.