

SEGURANÇA VIRTUAL NAS ESCOLAS: É POSSÍVEL?

Flávio Renato de Aguiar Lopes¹.

¹Must University, Boca Raton, Florida (EUA).

<http://lattes.cnpq.br/2503165941882101>

RESUMO: Este capítulo discute a segurança virtual nas escolas a partir da necessidade de formação crítica, ética e pedagógica para o uso da internet na educação básica. Parte-se da constatação de que crianças e adolescentes utilizam tecnologias digitais em diferentes espaços da vida cotidiana, o que amplia oportunidades de aprendizagem, comunicação e autoria, mas também aumenta riscos relacionados à exposição de dados, golpes, desinformação, cyberbullying e contatos inadequados em ambientes virtuais. Com base em pesquisa bibliográfica, o texto analisa a relação entre cidadania digital, segurança da informação, alfabetização digital, letramento digital e formação docente. A discussão considera a Base Nacional Comum Curricular, estudos sobre tecnologias digitais na educação e uma experiência pedagógica voltada à conscientização sobre riscos em rede. Conclui-se que não é possível eliminar completamente os riscos do ambiente digital, mas a escola pode reduzi-los por meio de planejamento, capacitação de professores, participação estudantil, orientação às famílias e ações permanentes de educação para o uso responsável da internet.

PALAVRAS-CHAVE: Segurança virtual. Segurança digital. Cidadania digital. Internet. Escola. BNCC. TICs.

VIRTUAL SECURITY IN SCHOOLS: IS IT POSSIBLE?

ABSTRACT: This chapter discusses virtual security in schools based on the need for critical, ethical and pedagogical education for internet use in basic education. It starts from the understanding that children and adolescents use digital technologies in different areas of everyday life, which expands learning, communication and authorship opportunities, but also increases risks related to data exposure, scams, misinformation, cyberbullying and inappropriate contact in virtual environments. Based on bibliographic research, the text analyzes the relationship between digital citizenship, information security, digital literacy and teacher education. The discussion considers the Brazilian National Common Curricular Base, studies on digital technologies in education and a pedagogical experience focused on awareness of online risks. It concludes that it is not possible to completely eliminate risks

in the digital environment, but schools can reduce them through planning, teacher training, student participation, family guidance and permanent educational actions for responsible internet use.

KEY-WORDS: Virtual security. Digital security. Digital citizenship. Internet. School. BNCC. ICTs.

INTRODUÇÃO

Apresença das tecnologias da informação e comunicação no cotidiano escolar tornou-se uma realidade incontornável. Estudantes utilizam celulares, computadores, plataformas digitais, redes sociais, jogos on-line e diferentes aplicativos em situações de estudo, lazer, sociabilidade e produção de conteúdo. Ao mesmo tempo em que esses recursos ampliam o acesso ao conhecimento e criam novas possibilidades pedagógicas, eles também expõem crianças e adolescentes a riscos que não podem ser ignorados pela escola.

Nos últimos anos, tornaram-se frequentes as preocupações relacionadas à exposição de jovens na internet, ao cyberbullying, ao vazamento de dados sensíveis, aos golpes digitais, à circulação de imagens sem autorização, ao contato com desconhecidos e à participação em comunidades virtuais que podem estimular comportamentos violentos ou prejudiciais. Esses problemas não pertencem apenas à esfera familiar ou individual, pois atravessam diretamente a vida escolar. A escola, como espaço de formação humana, precisa discutir a internet não apenas como ferramenta técnica, mas também como ambiente social, cultural, ético e político.

Essa discussão está diretamente ligada ao conceito de cidadania digital. Ribble (2015) compreende a cidadania digital como um conjunto de conhecimentos, atitudes e responsabilidades necessários para o uso adequado das tecnologias. Entre seus elementos, a segurança digital ocupa posição central, pois envolve a capacidade de reconhecer riscos, proteger informações pessoais, agir de forma ética, respeitar direitos de outras pessoas e compreender que as ações realizadas no ambiente virtual geram consequências reais.

No Brasil, a Base Nacional Comum Curricular reforça a importância desse debate ao estabelecer, em sua quinta competência geral, que estudantes devem compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas práticas sociais e escolares (BRASIL, 2018). Tal orientação demonstra que o trabalho com tecnologias não deve limitar-se ao uso instrumental de equipamentos. É necessário promover alfabetização e letramento digital, permitindo que os estudantes aprendam a acessar, avaliar, produzir, compartilhar e proteger informações.

A questão central, portanto, não é simplesmente permitir ou proibir o uso da internet nas escolas. A pergunta mais adequada é: como utilizar os recursos digitais de forma pedagógica e, ao mesmo tempo, reduzir riscos? A resposta exige planejamento institucional, formação continuada de professores, participação dos estudantes, diálogo com as famílias

e ações permanentes de conscientização. Não se trata de prometer segurança absoluta, mas de construir uma cultura escolar de prevenção, responsabilidade e cuidado.

Diante desse cenário, este capítulo discute a importância da segurança virtual nas escolas, especialmente na educação básica. A reflexão considera a necessidade de capacitação docente, a formação para a cidadania digital, os desafios da alfabetização e do letramento digital e a possibilidade de desenvolver projetos pedagógicos que envolvam a comunidade escolar na redução dos riscos associados ao uso da internet.

OBJETIVO

O objetivo geral deste trabalho é discutir a importância da segurança virtual nas escolas, analisando como a instituição escolar pode contribuir para a redução dos riscos enfrentados por estudantes no uso da internet e das tecnologias digitais.

Como objetivos específicos, pretende-se: relacionar segurança digital e cidadania digital; apresentar a relevância da BNCC para a formação crítica e ética no uso das tecnologias; refletir sobre a necessidade de capacitação dos professores; discutir estratégias pedagógicas de prevenção e conscientização; e analisar os limites e as possibilidades de construção de uma cultura de segurança digital no ambiente escolar.

A proposta não é defender a eliminação das tecnologias do cotidiano educacional, mas compreender como elas podem ser utilizadas de modo mais seguro, responsável e significativo. Assim, o texto busca contribuir para que escolas, gestores e professores reconheçam a segurança virtual como parte do processo formativo dos estudantes.

METODOLOGIA

A metodologia utilizada neste capítulo é a pesquisa bibliográfica, desenvolvida por meio da leitura, seleção e análise de textos acadêmicos e documentos normativos que tratam de segurança digital, cidadania digital, tecnologias educacionais e práticas escolares em ambientes conectados.

Foram considerados, principalmente, os estudos de Ribble (2015), Carneiro, Figueiredo e Ladeira (2020) e Santos (2022), além da Base Nacional Comum Curricular (BRASIL, 2018). Essas referências permitem compreender tanto o papel da escola na formação para o uso crítico das tecnologias quanto a necessidade de ações concretas para minimizar riscos relacionados à vida digital dos estudantes.

A análise foi organizada de forma qualitativa, buscando interpretar conceitos e relacioná-los ao contexto escolar. O estudo não pretende medir quantitativamente a eficácia de ferramentas de segurança nem avaliar tecnicamente softwares de proteção, mas refletir sobre a dimensão pedagógica da segurança virtual. Nesse sentido, a preocupação principal é compreender como a escola pode ensinar estudantes a reconhecer riscos, adotar

comportamentos responsáveis, proteger dados pessoais e participar da cultura digital com ética e autonomia.

A escolha pela pesquisa bibliográfica justifica-se porque o tema exige fundamentação teórica e normativa. A segurança virtual nas escolas não depende apenas de equipamentos, filtros, antivírus ou bloqueios de acesso; ela exige formação, planejamento e práticas educativas permanentes. Por isso, o texto articula contribuições de autores da área educacional com orientações curriculares e experiências de intervenção pedagógica.

FUNDAMENTAÇÃO TEÓRICA

Cidadania digital e segurança na cultura escolar

A cidadania digital pode ser entendida como a capacidade de participar de ambientes digitais de maneira ética, crítica, segura e responsável. Essa participação envolve direitos e deveres. Assim como no espaço físico, as ações realizadas no ambiente virtual produzem efeitos sobre outras pessoas, sobre instituições e sobre a própria identidade do usuário. Curtir, compartilhar, comentar, publicar imagens, armazenar senhas ou informar dados pessoais são práticas que precisam ser compreendidas como parte da vida social contemporânea.

No contexto escolar, a cidadania digital é especialmente relevante porque estudantes em idade de formação ainda estão construindo critérios de julgamento, convivência e responsabilidade. Muitos adolescentes dominam o uso operacional de dispositivos, mas isso não significa que compreendam os riscos associados a cada plataforma. Saber instalar aplicativos, enviar mensagens ou produzir vídeos não equivale a saber avaliar fontes, proteger dados, identificar golpes, reconhecer discursos de ódio ou agir adequadamente diante de situações de violência virtual.

A segurança digital, nessa perspectiva, não pode ser reduzida à proteção técnica dos computadores. Embora recursos como antivírus, senhas fortes, autenticação em duas etapas e controle de acesso sejam importantes, eles não substituem a formação dos sujeitos. Santos (2022) destaca que, durante muito tempo, a segurança da informação foi tratada quase exclusivamente como um problema técnico. Porém, temas como privacidade, phishing, engenharia social e exposição de dados mostram que o usuário também precisa ser educado para reconhecer riscos e tomar decisões responsáveis.

A escola, portanto, precisa incorporar a segurança virtual à sua cultura institucional. Isso significa tratar o assunto de modo permanente, e não apenas em situações de crise. Campanhas pontuais podem ser importantes, mas tornam-se insuficientes quando não estão articuladas a projetos pedagógicos, formação docente, normas de convivência, orientação às famílias e acompanhamento dos estudantes. A cultura de segurança é construída quando a comunidade escolar compreende que o uso da internet exige cuidado, ética e corresponsabilidade.

BNCC, alfabetização digital e letramento digital

A Base Nacional Comum Curricular reconhece que as tecnologias digitais modificaram as formas de trabalhar, comunicar, relacionar-se e aprender. Ao estabelecer a competência geral relacionada às tecnologias digitais, a BNCC orienta que os estudantes desenvolvam a capacidade de compreender, utilizar e criar recursos digitais de modo crítico, significativo, reflexivo e ético (BRASIL, 2018). Essa formulação é importante porque desloca o foco do simples manuseio técnico para a formação integral do estudante.

A alfabetização digital pode ser compreendida como o processo pelo qual o estudante aprende a utilizar ferramentas, dispositivos e ambientes digitais. Envolve ações como acessar plataformas, pesquisar conteúdos, elaborar documentos, utilizar aplicativos, participar de atividades on-line e compreender funcionalidades básicas dos recursos tecnológicos. Já o letramento digital aprofunda essa formação, pois envolve interpretação crítica, avaliação de fontes, produção responsável de informações, compreensão de linguagens digitais e reflexão sobre os impactos sociais da tecnologia.

Quando a escola trabalha apenas a alfabetização digital, corre o risco de formar usuários tecnicamente habilitados, mas pouco preparados para lidar com dilemas éticos e riscos de segurança. Por isso, a segurança virtual precisa integrar o letramento digital. Estudantes devem aprender, por exemplo, a diferenciar sites confiáveis de páginas fraudulentas, reconhecer tentativas de phishing, proteger senhas, evitar exposição excessiva de dados, respeitar direitos autorais, denunciar situações de violência e compreender a permanência dos rastros digitais.

Carneiro, Figueiredo e Ladeira (2020) defendem que as tecnologias digitais podem tornar o processo de ensino-aprendizagem mais significativo quando dialogam com a realidade dos estudantes. No entanto, para que isso ocorra, professores precisam estar preparados pedagógica e didaticamente. A presença da tecnologia na escola não garante, por si só, uma prática educativa de qualidade. É a mediação docente, orientada por objetivos claros, que transforma o recurso digital em oportunidade formativa.

Nesse sentido, a BNCC pode ser interpretada como um chamado para que a escola assuma papel ativo na formação digital dos estudantes. A segurança virtual não deve ser tratada como tema externo ao currículo, mas como componente transversal que dialoga com diferentes áreas do conhecimento. Língua Portuguesa pode trabalhar leitura crítica de informações on-line; História e Geografia podem discutir circulação de discursos e impactos sociais da tecnologia; Ciências pode abordar dados, saúde e bem-estar; matemática pode analisar estatísticas de segurança e uso da internet; e projetos interdisciplinares podem reunir diferentes perspectivas.

Capacitação docente e organização institucional

A capacitação dos professores é uma condição indispensável para que a escola consiga desenvolver ações efetivas de segurança virtual. Não se pode exigir que docentes orientem estudantes sobre riscos digitais sem que eles próprios tenham oportunidades de formação, estudo e atualização. Muitos professores foram formados em contextos nos quais a cultura digital ainda não ocupava o espaço que ocupa hoje, o que torna necessária a formação continuada.

Essa capacitação não deve limitar-se ao ensino de ferramentas. É importante que o professor conheça conceitos de cidadania digital, privacidade, proteção de dados, cyberbullying, desinformação, discurso de ódio, direitos autorais, exposição de imagem, segurança de senhas e uso pedagógico das plataformas. Também é necessário discutir procedimentos institucionais: como agir diante de denúncias, como orientar estudantes e famílias, quando acionar a gestão escolar e quais registros precisam ser feitos.

A organização institucional também é fundamental. A escola precisa construir normas claras para o uso de dispositivos e redes, sem cair em proibições generalizadas que ignorem o potencial educativo das tecnologias. Normas de convivência digital, termos de uso de laboratórios, orientação para uso de imagens, cuidado com dados de estudantes e protocolos para situações de cyberbullying são exemplos de medidas que podem orientar a comunidade escolar.

Outro ponto essencial é o envolvimento das famílias. Muitos riscos digitais ocorrem fora do horário escolar, mas chegam à escola por meio de conflitos, exposições, ameaças ou sofrimento emocional dos estudantes. Por isso, ações de formação para pais e responsáveis podem fortalecer a rede de proteção. A escola não substitui a responsabilidade familiar, mas pode criar espaços de diálogo e orientação, ajudando a comunidade a compreender que segurança virtual é uma responsabilidade compartilhada.

A capacitação docente, quando articulada à organização institucional, permite que a segurança digital deixe de ser uma preocupação individual de alguns professores e se torne um projeto coletivo. Essa mudança é importante porque os estudantes recebem mensagens mais coerentes quando toda a escola trabalha com princípios semelhantes. A construção de uma cultura de segurança depende justamente dessa continuidade entre gestão, professores, estudantes e famílias.

Estratégias pedagógicas para redução de riscos

A redução de riscos no uso da internet exige estratégias pedagógicas diversificadas. A escola pode realizar palestras, oficinas, campanhas, debates, estudos de caso, produção de cartazes, podcasts, vídeos, entrevistas, rodas de conversa e atividades interdisciplinares. O mais importante é que os estudantes não sejam apenas ouvintes passivos, mas participantes ativos da construção de conhecimentos sobre segurança digital.

Santos (2022) apresenta uma experiência pedagógica que demonstra a relevância de campanhas de conscientização com participação da comunidade escolar. Entre as ações descritas, destacam-se a produção de materiais informativos, a realização de entrevistas na rádio escolar, a elaboração de cursos específicos para professores, o desenvolvimento de chatbot para esclarecimento de dúvidas, publicações em redes sociais institucionais e oficinas voltadas ao uso seguro das tecnologias. A variedade de ações fortalece o alcance do projeto, pois permite que diferentes estudantes se envolvam de modos distintos.

A produção de materiais informativos é uma estratégia importante porque transforma os estudantes em autores. Ao pesquisar sobre golpes digitais, exposição de dados, senhas seguras ou cyberbullying, os alunos precisam selecionar informações, interpretar riscos e comunicar orientações de forma clara. Esse processo desenvolve competências de leitura, escrita, síntese, autoria e responsabilidade social.

Oficinas práticas também podem ser muito eficazes. Uma oficina sobre senhas, por exemplo, pode demonstrar a importância de combinações fortes, autenticação em duas etapas e cuidado com compartilhamentos. Uma atividade sobre privacidade pode analisar configurações de redes sociais e discutir quais informações não devem ser publicadas. Um estudo de caso sobre cyberbullying pode levar os estudantes a refletir sobre empatia, consequências legais, apoio às vítimas e canais de denúncia.

Outra possibilidade é integrar a segurança digital a projetos de protagonismo juvenil. Grupos de estudantes podem atuar como multiplicadores, produzindo campanhas, orientando colegas e colaborando na construção de normas de convivência digital. Essa estratégia tende a aumentar o engajamento, pois os próprios jovens participam da elaboração de linguagem e formatos próximos de sua realidade.

As ações pedagógicas, contudo, precisam evitar abordagens moralistas ou baseadas apenas no medo. Alertar sobre riscos é necessário, mas o objetivo não é afastar estudantes da tecnologia. O propósito é ensiná-los a usar a internet com autonomia, responsabilidade e senso crítico. A educação para a segurança digital deve equilibrar prevenção e potencialidade: reconhecer riscos, mas também valorizar o uso da rede para aprender, criar, colaborar e participar da vida social.

Segurança virtual nas escolas: possibilidades e limites

A pergunta que orienta este capítulo é se é possível alcançar segurança virtual nas escolas. A resposta exige cuidado. Se segurança for entendida como eliminação completa de riscos, a resposta é negativa. Nenhuma instituição consegue garantir risco zero no ambiente digital. Mesmo usuários experientes podem cair em golpes, ter dados expostos ou cometer erros de avaliação. Além disso, muitas interações digitais ocorrem fora do controle direto da escola.

Entretanto, se segurança for compreendida como redução de riscos, formação para o uso responsável e construção de práticas preventivas, a resposta é positiva. A escola pode contribuir significativamente para que estudantes compreendam os perigos da internet, adotem medidas de proteção, saibam pedir ajuda e desenvolvam postura ética nas interações digitais.

A primeira possibilidade está no planejamento pedagógico. Quando a segurança digital é incluída no currículo e nas práticas escolares, deixa de ser tema improvisado e passa a compor a formação dos estudantes. Projetos interdisciplinares, campanhas permanentes e atividades vinculadas às áreas do conhecimento ajudam a consolidar aprendizagens.

A segunda possibilidade está na formação de professores. Docentes capacitados conseguem identificar situações de risco, orientar estudantes, planejar atividades adequadas e dialogar com as famílias. A formação também reduz a insegurança dos educadores diante das tecnologias, permitindo que eles usem recursos digitais de forma mais intencional.

A terceira possibilidade está na participação estudantil. Quando os estudantes são envolvidos na criação de soluções, o tema ganha sentido concreto. Eles podem produzir materiais, propor regras de convivência, realizar pesquisas, divulgar orientações e atuar como multiplicadores. Essa participação fortalece o protagonismo e contribui para que a segurança digital seja percebida como responsabilidade coletiva.

A quarta possibilidade está na articulação entre escola e comunidade. Famílias, gestores, professores e estudantes precisam dialogar sobre limites, responsabilidades, direitos e deveres no ambiente virtual. A escola pode orientar, mas a proteção dos estudantes depende também do acompanhamento familiar e de políticas públicas que garantam acesso seguro, inclusão digital e formação continuada.

Entre os limites, destacam-se a desigualdade de acesso, a falta de infraestrutura, a ausência de formação docente, a sobrecarga das escolas e a velocidade das mudanças tecnológicas. Novas plataformas, aplicativos e formas de interação surgem rapidamente, exigindo atualização constante. Por isso, a segurança virtual não pode ser tratada como conteúdo fechado, mas como processo permanente de aprendizagem.

CONSIDERAÇÕES FINAIS

A segurança virtual nas escolas é uma necessidade urgente no contexto educacional contemporâneo. Crianças e adolescentes vivem em uma cultura digital marcada por oportunidades de aprendizagem, comunicação e criação, mas também por riscos relacionados à exposição de dados, cyberbullying, golpes, desinformação e interações inadequadas. Ignorar esse cenário significaria deixar os estudantes sem orientação diante de uma parte importante de sua vida social.

A discussão realizada mostrou que a escola pode contribuir para reduzir riscos, desde que compreenda a segurança digital como dimensão pedagógica da cidadania digital. Não

basta instalar ferramentas técnicas de proteção ou bloquear acessos. É necessário formar estudantes capazes de agir com autonomia, responsabilidade, ética e senso crítico no ambiente virtual.

A BNCC reforça essa responsabilidade ao indicar que os estudantes devem compreender, utilizar e criar tecnologias digitais de modo crítico, reflexivo e ético. Essa orientação exige alfabetização e letramento digital, formação continuada dos professores, planejamento institucional e envolvimento das famílias. A segurança virtual, portanto, deve ser tratada como tema transversal e permanente, articulado ao currículo e às práticas escolares.

Também foi possível observar que projetos pedagógicos participativos podem gerar resultados significativos. Campanhas, oficinas, materiais informativos, entrevistas, ações em redes sociais e participação dos estudantes como multiplicadores são estratégias capazes de ampliar a conscientização e fortalecer a cultura de prevenção. Essas ações não eliminam todos os riscos, mas ajudam a comunidade escolar a reconhecê-los e enfrentá-los com mais preparo.

Conclui-se que a segurança virtual nas escolas é possível quando entendida como redução de riscos e formação para o uso responsável da internet, e não como promessa de controle absoluto. O desafio é construir uma cultura escolar que una tecnologia, ética, cidadania, proteção e aprendizagem. Assim, a internet pode ser utilizada como ferramenta pedagógica relevante, sem que a escola deixe de reconhecer os cuidados necessários para proteger e orientar seus estudantes.

REFERÊNCIAS

BRASIL. Ministério da Educação. Base Nacional Comum Curricular. Brasília, DF: Ministério da Educação, 2018. Disponível em: <http://basenacionalcomum.mec.gov.br/implementacao/praticas/caderno-de-praticas/aprofundamentos/193-tecnologias-digitais-da-informacao-e-comunicacao-no-contexto-escolar-possibilidades>. Acesso em: 5 ago. 2023.

CARNEIRO, Auner Pereira; FIGUEIREDO, Ismérie Salles de Souza; LADEIRA, Thalles Azevedo. A importância das tecnologias digitais na Educação e seus desafios. Revista Educação Pública, Rio de Janeiro, v. 20, n. 35, 15 set. 2020. Disponível em: <https://educacaopublica.cecierj.edu.br/artigos/20/35/joseph-a-importancia-das-tecnologias-digitais-na-educacao-e-seus-desafios-a-educacao-na-era-da-informacao-e-da-cibercultura>. Acesso em: 5 ago. 2023.

RIBBLE, Mike. Digital citizenship in schools: nine elements all students should know. 3. ed. Eugene: International Society for Technology in Education, 2015.

SANTOS, C. Educação, práticas digitais e novos riscos em rede. In: WORKSHOP DE INFORMÁTICA NA ESCOLA, 28., 2022, Porto Alegre. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 338-347. DOI: 10.5753/wie.2022.225607.