Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Educação para a Cidadania e Segurança Digital no Ensino Fundamental: letramento e proposta de práticas pedagógicas alinhados à BNCC de Computação

Annelise Schulz dos Santos

Monografia apresentada como requisito parcial
para conclusão do Curso de Computação — Licenciatura

Orientador
Prof. Dr. Jorge Henrique Cabral Fernandes

Brasília
2024

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Educação para a Cidadania e Segurança Digital no Ensino Fundamental: letramento e proposta de práticas pedagógicas alinhados à BNCC de Computação

Annelise Schulz dos Santos

Monografia apresentada como requisito parcial
para conclusão do Curso de Computação — Licenciatura

Prof. Dr. Jorge Henrique Cabral Fernandes (Orientador)
CIC/UnB

Prof. Dr. Jonathan Rosa Moreira
CIC/UnB

Prof. Joao Jose Costa Gondim
FT/UnB

Prof. Dr. Jorge Henrique Cabral Fernandes
Coordenador do Curso de Computação — Licenciatura

Brasília, 7 de outubro de 2024

Dedicatória

Dedico este trabalho à minha mãe, que sempre me ensinou que a caneta é mais leve que a enxada. Sua sabedoria, dedicação e sacrifício para me proporcionar uma educação de qualidade, oferecendo tudo que podia e até o que não podia, foram fundamentais para minha formação como ser humano e como profissional. Sem seu apoio incondicional, este caminho não teria sido possível. Sua força, resiliência e amor foram a base sobre a qual construí este sonho.

Aproveito também para expressar minha gratidão a todos que, de alguma forma, contribuíram para a realização deste trabalho. Aos meus professores, que compartilharam seus conhecimentos e orientações valiosas; aos colegas de curso, pelo apoio mútuo durante a jornada acadêmica; e à minha família, por acreditarem no meu potencial e me encorajarem a persistir, mesmo diante das dificuldades.

Este trabalho é fruto de uma caminhada coletiva, marcada por desafios e aprendizados, e sou profundamente grata por todas as mãos estendidas ao longo dessa trajetória.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

Este trabalho tem como objetivo desenvolver uma proposta pedagógica voltada para o ensino de segurança digital nos anos iniciais do ensino fundamental, de acordo com as diretrizes da Base Nacional Comum Curricular (BNCC). O eixo de Cultura Digital, com foco na segurança e responsabilidade no uso de tecnologias computacionais, é explorado por meio de atividades didáticas que capacitam professores a ensinarem conceitos como privacidade digital, proteção de dados, direitos autorais e ética digital. A partir de uma abordagem teórica fundamentada na aprendizagem significativa, o trabalho busca empoderar os educadores com o letramento digital necessário para que possam atuar de maneira crítica e reflexiva no desenvolvimento da cidadania digital de seus alunos. A metodologia proposta envolve a criação de materiais que facilitam o ensino e promovem uma interação prática entre os alunos e os conteúdos abordados, promovendo uma educação voltada para os desafios do mundo digital. Com isso, pretende-se contribuir para a formação de uma geração mais consciente e responsável em relação ao uso da tecnologia.

Palavras-chave: Segurança Digital, Cidadania Digital, Competências Digitais, Ensino de Computação, BNCC

Abstract

This study aims to develop a pedagogical proposal focused on teaching digital security in elementary school, in accordance with the guidelines of the National Common Curricular Base (BNCC). The Digital Culture axis, emphasizing security and responsibility in the use of computational technologies, is explored through didactic activities that equip teachers to teach concepts such as privacy, data protection, copyright, and digital ethics. Based on a theoretical approach grounded in meaningful learning, the work seeks to empower educators with the necessary digital literacy so that they can act critically and reflectively in fostering their students' digital citizenship. The proposed methodology involves creating materials that facilitate teaching and promote practical interaction between students and the addressed content, aiming to provide an education focused on the challenges of the digital world. Thus, this study intends to contribute to the formation of a more conscious and responsible generation regarding the use of technology.

Keywords: Digital Security, Digital Citizenship, Digital Competencies, Computing Education, BNCC

Sumário

Glossário

ameaças cibernéticas Qualquer ação ou evento potencial que possa comprometer a integridade, a disponibilidade ou a confidencialidade de informações e sistemas em um ambiente digital. Exemplos incluem ataques de malware, phishing.

antivírus Programa de software desenvolvido para detectar, prevenir e remover vírus e outros tipos de malware dos dispositivos, promovendo a proteção dos sistemas contra ameaças cibernéticas.

ataques cibernéticos Ações maliciosas realizadas para interromper, danificar ou roubar informações e sistemas de indivíduos ou organizações. São exemplares de ataques cibernéticos o phishing, o ransomware e a invasão de redes.

autenticação multifatorial Mecanismo de segurança que exige múltiplas formas de verificação (como senha e código SMS) para autenticar a identidade do usuário, aumentando a segurança no acesso a sistemas e plataformas.

cookies de navegação Pequenos arquivos armazenados no navegador que mantêm informações sobre o usuário e suas interações em sites, usados para personalizar experiências online e melhorar o rastreamento de dados de navegação.

crimes cibernéticos Atividades ilegais realizadas no ambiente digital, como roubo de identidade, fraudes financeiras, invasão de sistemas, disseminação de malware e violação de direitos autorais.

criptografia Técnica de segurança que transforma dados em um formato codificado, acessível apenas por quem possui uma chave de decriptação, sendo essencial para proteger informações sensíveis contra acessos não autorizados.

cyberbullying Ato de intimidação, humilhação ou agressão de uma pessoa a outra no ambiente online, com o uso de redes sociais, aplicativos de mensagens e outros meios digitais.

discurso de ódio Manifestação de ideias, comportamentos ou conteúdos que promovem discriminação, preconceito ou hostilidade contra grupos específicos, muitas vezes disseminado nas plataformas digitais e redes sociais.

e-commerce Comércio eletrônico realizado pela internet, permitindo a compra e venda de produtos e serviços em plataformas digitais, com transações financeiras online.

endereço IP Identificação numérica exclusiva atribuída a cada dispositivo conectado à internet, usada para localizar e identificar o dispositivo na rede.

fake news Informações falsas ou enganosas que são deliberadamente divulgadas como se fossem verdadeiras, geralmente com o objetivo de influenciar a opinião pública ou enganar o público.

firewalls Sistema de segurança que monitora e controla o tráfego de entrada e saída de uma rede, criando uma barreira entre redes confiáveis e não confiáveis para proteger dados e sistemas de ataques.

hacking Atividade de explorar vulnerabilidades em sistemas e redes digitais, que pode ser usada para propósitos mal-intencionados (invasão de sistemas) ou para promover melhorias de segurança (hacking ético).

informações sensíveis Dados que requerem proteção especial devido à sua natureza confidencial, como informações financeiras, dados médicos, senhas e informações pessoais.

Internet das Coisas (IoT) Conexão de dispositivos físicos, como eletrodomésticos e sensores, à internet, permitindo a coleta e troca de dados entre esses dispositivos para otimizar processos e funcionalidades.

malware Qualquer software malicioso, como vírus, spyware ou ransomware, que visa infectar, danificar ou roubar informações de sistemas e dispositivos.

monitoramento de rede Processo de rastrear e analisar atividades e dados em uma rede para detectar e responder a problemas de segurança ou desempenho, garantindo a integridade e a segurança dos dados.

nativos digitais Indivíduos que nasceram e cresceram em um mundo conectado à internet, familiarizados com tecnologias digitais e muitas vezes com habilidades intuitivas para navegar e usar dispositivos eletrônicos.

phishing Técnica de fraude online em que o golpista tenta enganar a vítima para que compartilhe informações confidenciais, como senhas e dados bancários, geralmente por meio de e-mails ou mensagens falsas.

pirataria digital Ato de copiar, distribuir ou acessar ilegalmente conteúdos digitais protegidos por direitos autorais, como músicas, filmes, softwares e jogos.

ransomware Tipo de malware que bloqueia o acesso ao sistema ou aos dados da vítima, exigindo pagamento de resgate para restaurar o acesso.

software Conjunto de programas e instruções que executam operações específicas em um computador ou dispositivo eletrônico, sendo o principal recurso para o funcionamento de aplicações e sistemas.

vulnerabilidades em software Falhas ou brechas em programas e sistemas que podem ser exploradas por hackers para comprometer a segurança e acessar informações ou sistemas de forma não autorizada.

vírus Tipo de malware que se replica e se espalha em sistemas, corrompendo ou danificando arquivos e programas, e frequentemente exigindo a intervenção de um anti-vírus para ser eliminado.

Capítulo 1

Introdução

A crescente digitalização da sociedade trouxe uma série de transformações profundas em diversos setores, incluindo o educacional. O uso de tecnologias computacionais se tornou parte integral da vida cotidiana, desde a comunicação e o acesso à informação até a organização do trabalho e a interação social. Nesse contexto, a escola desempenha um papel central na formação de cidadãos que não apenas utilizam essas tecnologias, mas que também compreendem os riscos e responsabilidades envolvidos. A Base Nacional Comum Curricular (BNCC), em sua versão mais recente, reconhece a importância de preparar os alunos para um mundo cada vez mais digital, incluindo competências relacionadas à segurança e ao uso responsável de tecnologias.

Dentro do eixo de Cultura Digital, a BNCC destaca a "Segurança e Responsabilidade no Uso de Tecnologia Computacional"[1] como um objeto de conhecimento essencial. A proposta da BNCC reflete uma preocupação com a privacidade, a proteção de dados pessoais e a cidadania digital, compreendendo que os jovens de hoje são nativos digitais e, portanto, estão constantemente expostos a situações que exigem conhecimento sobre ética, segurança e responsabilidade na internet. Com isso, o papel dos educadores passa a ser não apenas o de transmitir conhecimento técnico, mas também de desenvolver nos alunos uma consciência crítica em relação ao ambiente digital.

Dessa forma, o presente trabalho tem como objetivo central elaborar uma proposta de material pedagógico que auxilie professores do ensino fundamental a ensinarem conceitos de segurança digital conforme as diretrizes da BNCC. A ênfase está no empoderamento dos educadores, de modo que eles sejam capazes de não apenas dominar os conteúdos técnicos, mas também promover um letramento digital que favoreça o desenvolvimento de uma cidadania digital crítica e responsável entre seus alunos. A abordagem teórica adotada neste trabalho está pautada na pedagogia significativa, que visa promover o aprendizado por meio de conexões diretas entre o conhecimento transmitido e a vivência cotidiana dos alunos, de maneira a tornar a experiência de aprendizado mais rica e contextualizada.

A estrutura do trabalho divide-se em capítulos que abordam o conceito de cidadania digital, a importância do letramento digital dos professores para o ensino de segurança computacional, uma análise aprofundada da BNCC de Computação, bem como a proposta de atividades didáticas voltadas para o ensino fundamental. Cada capítulo busca explorar as nuances de ensinar segurança digital em um contexto educacional dinâmico, oferecendo aos professores ferramentas e reflexões teóricas para que possam se tornar agentes ativos na formação de uma geração mais consciente e preparada para os desafios digitais contemporâneos.

Capítulo 2

Cidadania Digital

A cidadania digital, em sua essência, refere-se ao uso responsável, ético e seguro das tecnologias digitais por parte dos indivíduos, instituições e governos. Com a crescente digitalização de todos os aspectos da vida contemporânea, desde o ensino até o comércio, tornou-se essencial que os usuários estejam cientes de seus direitos e deveres no ambiente digital. Nunes e Lehfeld [2] afirmam que a cidadania digital envolve mais do que o simples acesso à internet ou o uso de dispositivos; trata-se de como os cidadãos se comportam e interagem neste espaço, respeitando os direitos dos outros e cumprindo suas obrigações enquanto usuários da tecnologia. Nesse contexto, o papel dos indivíduos, dos educadores e do governo torna-se fundamental para a promoção de uma cultura de cidadania digital.

2.1 O papel dos indivíduos

Os indivíduos são os protagonistas da cidadania digital. Conforme Ribble [3], o comportamento ético online depende da compreensão de direitos e responsabilidades, como a proteção da privacidade e o respeito às normas de conduta digital. Isso inclui ações como evitar a disseminação de informações falsas (fake news), respeitar os direitos autorais e agir de forma respeitosa nas interações online. A proteção dos dados pessoais também é uma das principais preocupações no contexto digital atual, e os usuários precisam estar atentos aos riscos envolvidos ao compartilhar informações sensíveis em plataformas digitais. Segundo Nunes e Lehfeld [2], o conhecimento sobre segurança digital é uma habilidade crucial que deve ser desenvolvida continuamente, à medida que novas ameaças cibernéticas surgem.

2.2 O Papel do Governo

O governo, como regulador e promotor de políticas públicas, tem a responsabilidade de garantir um ambiente digital seguro e acessível para todos os cidadãos. A Lei Geral de Proteção de Dados (LGPD), sancionada no Brasil em 2018, é um exemplo claro de como a legislação pode proteger os direitos dos cidadãos no ambiente digital. Segundo Nunes e Lehfeld [2], a LGPD estabelece regras claras sobre como os dados pessoais devem ser coletados, armazenados e utilizados, garantindo que os indivíduos tenham controle sobre suas informações. Além disso, o governo é responsável por desenvolver políticas de inclusão digital, assegurando que todos os cidadãos, independentemente de sua condição socioeconômica, tenham acesso às tecnologias digitais e possam exercer sua cidadania de forma plena.

2.3 O Papel dos Educadores

Os educadores desempenham um papel crucial na formação de cidadãos digitais conscientes. A UNESCO (2017) [4] destaca que o ensino da cidadania digital deve ser incorporado desde os primeiros anos de escolaridade, preparando os alunos para os desafios e oportunidades da era digital. Ribble [3] desenvolveu o conceito dos Nove Elementos da Cidadania Digital, que funcionam como uma estrutura abrangente para guiar o ensino e a prática da cidadania digital nas escolas. Esses elementos são:

1. **Acesso Digital:** Garantir que todos tenham acesso igual às tecnologias digitais. A inclusão digital é essencial para que todos possam exercer sua cidadania online.
2. **Comércio Digital:** O uso seguro e responsável do e-commerce, compreendendo os direitos dos consumidores e a segurança nas transações online.
3. **Comunicação Digital:** Compreender as diferentes formas de comunicação online e como utilizá-las de forma ética e apropriada.
4. **Literacia Digital:** Desenvolver a capacidade de localizar, entender e usar a informação de forma eficaz no ambiente digital.
5. **Etiqueta Digital:** Conduzir-se de maneira respeitosa nas interações online, evitando comportamentos como cyberbullying ou discurso de ódio.
6. **Lei Digital:** Entender as legislações e regras que regem o uso da tecnologia e as implicações legais de violá-las.

7. **Direitos e Responsabilidades Digitais:** Reconhecer que os direitos de privacidade e liberdade de expressão são acompanhados de responsabilidades no uso da internet.

8. **Saúde e Bem-Estar Digital:** Proteger-se dos riscos físicos e psicológicos associados ao uso excessivo de tecnologia, como cansaço visual ou dependência digital.

9. **Segurança Digital:** Proteger a si mesmo e os outros de ameaças como vírus, fraudes e invasões de privacidade.

Esses elementos são fundamentais para o desenvolvimento de práticas pedagógicas que integram a cidadania digital ao currículo escolar, conforme apontado por Teixeira e Lima [5]. O papel dos professores é criar um ambiente em que os alunos possam não só entender, mas aplicar esses conceitos em sua vida cotidiana, promovendo uma cultura de segurança e ética no uso das tecnologias digitais.

A cidadania digital envolve o comportamento responsável e ético de todos os usuários da tecnologia, incluindo indivíduos, educadores e o governo. Os Nove Elementos da Cidadania Digital fornecem uma estrutura sólida para guiar o desenvolvimento dessas práticas, desde o respeito à privacidade até a promoção da inclusão digital. Ao educar os alunos sobre esses princípios e ao criar políticas públicas que garantam a segurança e os direitos dos cidadãos no ambiente digital, podemos promover uma sociedade mais equitativa, informada e preparada para os desafios da era digital.

2.4 Competências digitais para professores

A era digital exige que os professores possuam competências digitais robustas, não apenas para integrar tecnologias em suas práticas pedagógicas, mas também para orientar os alunos no uso seguro e ético das tecnologias. As competências digitais dos educadores tornam-se essenciais para lidar com os desafios emergentes no ambiente escolar, especialmente no que se refere à cidadania digital e à segurança da informação. Nesse contexto, a preparação docente deve ir além do domínio técnico, abrangendo a capacidade de ensinar os alunos a navegar de forma crítica e responsável no mundo digital. Como aponta Teixeira e Lima [5], a formação de professores precisa incorporar elementos de cidadania digital, de modo a garantir que os educadores estejam aptos a promover o uso consciente e seguro das tecnologias dentro e fora da sala de aula.

Ademais, a Lei Geral de Proteção de Dados (LGPD) introduziu novos desafios e responsabilidades para as instituições de ensino e para os professores. A necessidade de conscientizar os alunos sobre os riscos associados ao compartilhamento de informações

online e o respeito aos direitos digitais exige que os docentes desenvolvam uma abordagem pedagógica que contemple o ensino de segurança digital. Ribble [3] argumenta que, ao capacitar os professores para ensinar as nove competências da cidadania digital, as escolas podem preparar melhor os alunos para lidar com os desafios e oportunidades do mundo digital, garantindo que estejam equipados para enfrentar as demandas da sociedade contemporânea.

Com a crescente digitalização da sociedade, as competências digitais dos professores tornaram-se um elemento central no desenvolvimento de práticas pedagógicas eficazes. Esse conjunto de habilidades é essencial não apenas para integrar tecnologias digitais ao processo de ensino-aprendizagem, mas também para promover a emancipação crítica dos alunos no uso dessas ferramentas. Em um cenário onde o ambiente virtual está cada vez mais presente, os educadores enfrentam o desafio de adaptar suas práticas, adquirindo fluência digital que lhes permita usar esses recursos de forma intencional e pedagógica.

Conforme o modelo DigCompEdu, desenvolvido pela Comissão Europeia, as competências digitais docentes são organizadas em seis áreas principais: 1) envolvimento profissional, 2) uso de tecnologias e recursos digitais, 3) ensino e aprendizagem, 4) avaliação, 5) empoderamento dos estudantes e 6) promoção das competências digitais dos estudantes. Este modelo oferece uma estrutura de autoavaliação que possibilita aos professores identificar suas lacunas e estabelecer planos de desenvolvimento contínuo. O estudo apresentado no material aponta que, embora os professores brasileiros dos Anos Iniciais do Ensino Fundamental já utilizem algumas tecnologias digitais em suas práticas, muitos ainda se encontram no nível de "Integrador", o que demonstra a necessidade de maior aprofundamento e reflexividade nas metodologias digitais aplicadas em sala de aula [6]

Os dados revelados pelo estudo destacam que os professores possuem lacunas em áreas críticas, como a avaliação e o empoderamento dos alunos com o uso das tecnologias digitais. Apenas um pequeno número de professores demonstrou competências avançadas em participação e formação online, sugerindo que, embora haja interesse em aprimorar suas habilidades digitais, a formação inicial e continuada ainda é insuficiente para garantir o desenvolvimento pleno dessas competências [7]. Assim, é imprescindível que os cursos de formação docente contemplem, de forma mais abrangente e sistemática, a utilização pedagógica das tecnologias digitais, indo além do simples uso técnico e focando na criação de estratégias que promovam a aprendizagem colaborativa e crítica [8].

Além disso, o estudo aponta que as competências digitais dos professores devem estar alinhadas ao contexto social, econômico e cultural em que os alunos estão inseridos, promovendo um ensino que não só utiliza as ferramentas digitais, mas que também prepara os estudantes para navegar em uma sociedade hiperconectada [9]. As competências digitais não se limitam ao uso técnico, mas englobam uma série de habilidades que permitem aos

educadores fomentar o pensamento crítico e a responsabilidade digital entre os alunos, incentivando-os a se tornarem cidadãos mais conscientes e atuantes nas práticas digitais.

Essas competências, entretanto, não podem ser desenvolvidas de forma isolada. O estudo aponta para a necessidade de políticas públicas eficazes que promovam a inclusão digital nas escolas, garantindo o acesso à internet de qualidade e a dispositivos tecnológicos adequados, especialmente em regiões mais vulneráveis. Sem essas condições, a formação digital dos professores continuará limitada, impedindo que eles alcancem a fluência digital necessária para educar na sociedade da informação [10]. Diante desses desafios, fica claro que a formação continuada dos professores deve ser ampliada e aprofundada, com foco no desenvolvimento de competências digitais que atendam às demandas da era digital e contribuam para uma educação mais inclusiva e conectada.

Capítulo 3

Letramento digital de professores voltado para o ensino de segurança

Após a discussão sobre cidadania digital no primeiro capítulo, que explorou como a participação crítica e ética no ambiente online é um elemento crucial para o exercício pleno da cidadania, este capítulo amplia o foco para o letramento digital dos professores no ensino de segurança. O objetivo deste trabalho é empoderar educadores, não apenas com conhecimento técnico, mas também com a capacidade de transmitir esses conceitos de forma eficaz a seus alunos. O letramento digital é fundamental para que os professores se tornem agentes ativos na formação de estudantes conscientes, que saibam navegar de forma segura no ambiente digital. Para isso, é necessário que os educadores compreendam profundamente os conceitos relacionados à segurança digital, não apenas como usuários, mas como facilitadores de um aprendizado significativo e contextualizado sobre proteção de dados, privacidade e comportamento online seguro. Esse capítulo irá abordar os principais conceitos que norteiam as propostas de atividades a serem desenvolvidas em sala de aula.

3.1 Letramento digital

A necessidade de um indivíduo possuir letramento digital surgiu a partir da compreensão de que as fontes digitais podem gerar diferentes tipos de informações, como imagens e sons, além do texto. Dessa forma, uma nova forma de alfabetização tornou-se essencial para que essas novas formas de apresentação fossem interpretadas de maneira significativa. [11]

Maria Teresa Freitas, em seu artigo "Letramento digital e formação de professores"[12] expõe que a escola já não é vista como o único espaço legítimo de saber, e os professores devem reconhecer essa nova realidade em vez de adotar uma postura defensiva em relação

às tecnologias digitais. Os alunos de hoje, mais familiarizados com as mídias digitais, chegam às salas de aula com novas informações adquiridas através da internet e esperam que o professor desempenhe o papel de orientador, não apenas de transmissor de conhecimento. Assim, cabe ao professor transformar esse volume de informações em conhecimento significativo, exercendo seu papel como mediador e problematizador do saber. A formação de professores para atuar com nativos digitais requer, portanto, uma atualização constante, permitindo que eles mantenham um olhar crítico sobre as tecnologias e aproveitem as novas possibilidades que elas oferecem para promover uma aprendizagem colaborativa e compartilhada.

A autora faz uma rica discussão sobre as definições de letramento digital com base em diversos autores. As definições estão organizadas em categorias restritas e amplas, abordando tanto o uso funcional quanto os aspectos socioculturais do letramento digital.

Definições restritas: Essas definições enfatizam o uso instrumental da tecnologia, focando nas habilidades técnicas necessárias para acessar, avaliar e criar informações por meio de tecnologias digitais. Serim (2002) [13], define letramento digital como a capacidade de utilizar ferramentas tecnológicas e redes para acessar e gerenciar informações em uma sociedade do conhecimento. A Association of College & Research Libraries descreve o letramento digital como um conjunto de habilidades que permite aos indivíduos localizar, avaliar e usar a informação de forma eficaz.

Definições amplas: Estas vão além do uso técnico e incorporam os aspectos socioculturais do letramento digital. A autora destaca a complexidade crescente de identificar quem é letrado digitalmente, pois isso envolve não apenas habilidades funcionais, mas também um conhecimento crítico do uso da tecnologia. Selfe (1999)[14] define letramento digital como um conjunto de valores, práticas e habilidades que são situados social e culturalmente, e que envolvem leitura, escrita e comunicação dentro de ambientes eletrônicos. Gilster (1997)[15] adiciona a ideia de que o letramento digital envolve a habilidade de entender e usar informações em múltiplos formatos e de avaliar criticamente o conteúdo digital.

A autora então conclui que o letramento digital dos professores vai muito além do simples acesso ou domínio instrumental de ferramentas tecnológicas. Embora o acesso a computadores e à internet, assim como cursos básicos de informática educativa, sejam importantes, esses elementos isolados não garantem a integração eficaz das tecnologias digitais nas práticas pedagógicas. O que se espera dos educadores é que eles sejam capazes de transformar suas práticas, incorporando, de forma criativa e crítica, as linguagens e os gêneros digitais que já fazem parte do cotidiano dos alunos. O objetivo não é abandonar as práticas educativas tradicionais, mas somar a elas o uso inteligente e significativo das tecnologias digitais, atribuindo-lhes novos significados e funções no processo de ensino-

aprendizagem. Assim, o letramento digital, tanto para professores quanto para alunos, deve ultrapassar a simples instrumentalização da tecnologia, promovendo uma apropriação crítica e construtiva dessas ferramentas. [12]

3.2 Ética Digital

Ética digital refere-se ao conjunto de princípios e normas que orientam o comportamento humano em ambientes digitais, incluindo o uso responsável de tecnologias e a consideração das implicações morais de nossas ações online. Ela envolve temas como privacidade, proteção de dados, direitos autorais, discurso apropriado, e a utilização responsável de mídias digitais, sempre levando em conta o impacto dessas ações em outras pessoas e na sociedade.

A ética digital torna-se essencial à medida que as tecnologias digitais permeiam cada vez mais aspectos da vida cotidiana, educacional e profissional. A rápida expansão do uso da internet e das redes sociais trouxe à tona novas questões éticas, como a disseminação de fake news, o ciberbullying, a violação de privacidade e o uso não autorizado de conteúdos digitais. Conforme Tavani [16] aponta, a ética digital se insere no campo da "cibercultura", onde as questões éticas se diferem das que regem os comportamentos no mundo físico, exigindo uma nova compreensão dos direitos e deveres digitais.

A integração da ética digital nas práticas educativas é fundamental para capacitar alunos a navegar pelos ambientes digitais de maneira segura e consciente. Ribble (2015) [17] enfatiza a importância de ensinar cidadania digital, que inclui a compreensão ética do uso da tecnologia. Esse conceito é essencial não só para evitar comportamentos prejudiciais, como o ciberbullying ou a violação de direitos autorais, mas também para promover uma convivência digital mais segura e justa.

3.3 Segurança

Segurança é um conceito fundamental em todas as áreas da vida e tem sido objeto de estudo e preocupação ao longo da história da humanidade. De acordo com o dicionário online Michaelis [18], temos pelo menos onze definições do termo na língua portuguesa. O uso do termo segurança no contexto desse estudo refere-se à proteção contra perigos, ameaças ou riscos que possam causar danos ou prejuízos a pessoas, lugares, organizações, sistemas ou recursos.

3.3.1 Segurança no mundo informacional, computacional e digital

Restringindo também o espaço de estudo, serão abordadas definições de segurança específicas que se relacionam ao mundo informacional, computacional e digital: segurança da informação e principalmente, cibersegurança. O termo cibersegurança é frequentemente usado como sinônimo de segurança da informação. No entanto, os autores Solms, Rossouw von e Johan van Niekerk em [19] argumentam que embora haja uma grande sobreposição entre esses dois conceitos, eles não são completamente iguais. A cibersegurança vai além da proteção dos dados para incluir também a proteção de outros ativos, como as pessoas. Na segurança da informação, o foco no fator humano está principalmente no papel das pessoas no processo de segurança. No entanto, na cibersegurança, esse fator ganha uma dimensão adicional, considerando os humanos como possíveis alvos de ataques cibernéticos ou até mesmo como participantes involuntários desses ataques. Os autores adicionam que essa perspectiva ética destaca a responsabilidade social de proteger grupos vulneráveis, como as crianças.

3.3.2 Segurança da informação

A Segurança da Informação refere-se ao conjunto de práticas, políticas e princípios que visam proteger a integridade, a confidencialidade e a disponibilidade dos dados e sistemas de informação [20]. Ela está diretamente relacionada à proteção contra ameaças, como acesso não autorizado, violações de dados e ataques cibernéticos. Seu objetivo é garantir que informações sensíveis sejam adequadamente armazenadas, acessadas e manipuladas de maneira segura, preservando sua autenticidade e evitando qualquer tipo de comprometimento.

Em um ambiente digital, a segurança da informação abrange diversas áreas, incluindo criptografia, autenticação, monitoramento de rede e a implementação de firewalls e antivírus [21]. Além disso, envolve a criação de políticas de segurança, treinamentos regulares para usuários e a aplicação de práticas de conformidade com legislações e regulamentações, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, que impõe padrões específicos para o tratamento e a proteção de dados pessoais.

Segundo Stallings e Brown [20], os três pilares da segurança da informação são: **Confidencialidade,** que assegura que apenas pessoas autorizadas possam acessar informações sensíveis; **Integridade**, que garante que os dados não sejam alterados de forma indevida; e **Disponibilidade**, que visa assegurar que as informações e sistemas estejam sempre acessíveis quando necessário. Com o crescente número de dispositivos conectados e o aumento das interações digitais, o papel da segurança da informação tornou-se ainda mais

crucial para a proteção de dados pessoais e corporativos, bem como para a manutenção da confiança no ambiente digital [22].

No contexto educacional, a segurança da informação desempenha um papel vital, já que escolas e professores frequentemente lidam com informações sensíveis de alunos e famílias. Proteger esses dados é uma responsabilidade fundamental que vai além das práticas tecnológicas, envolvendo também a conscientização e o treinamento de professores e alunos sobre boas práticas de segurança digital. Abordar como a segurança da informação pode ser integrada ao ensino da cidadania digital e das competências digitais torna-se essencial para formar uma nova geração mais consciente dos riscos e práticas de segurança online.

3.3.3 Segurança Cibernética

A Segurança Cibernética pode ser entendida como um campo multidisciplinar que envolve a aplicação de medidas técnicas, organizacionais e educacionais para proteger sistemas, redes, dispositivos e dados no ambiente digital contra ameaças e ataques cibernéticos. Ela abrange a prevenção, detecção e resposta a riscos que podem comprometer a integridade, confidencialidade e disponibilidade de informações. Segundo a União Internacional de Telecomunicações (ITU/ONU)[23], a segurança cibernética inclui o uso de ferramentas, políticas, abordagens de gestão de risco, treinamentos e tecnologias para proteger dispositivos computacionais, serviços, sistemas de telecomunicação, infraestrutura e a totalidade das informações que circulam no ambiente cibernético .

Diferente da segurança da informação, que se concentra principalmente na proteção dos dados em si, a segurança cibernética engloba também a proteção de infraestruturas críticas, redes e dispositivos interconectados, como a Internet das Coisas (IoT), em um cenário onde as ameaças cibernéticas estão se tornando mais sofisticadas e constantes. Segundo Singer e Friedman [24], a segurança cibernética abrange desde a proteção contra ataques cibernéticos em nível nacional até a defesa de dispositivos pessoais, cobrindo aspectos de guerra cibernética, espionagem, sabotagem e proteção de dados pessoais.

O crescimento do uso de tecnologias digitais em diversos setores, como educação, saúde e comércio, aumentou significativamente a exposição a ameaças cibernéticas. A European Union Agency for Cybersecurity (ENISA) [25] destaca que ataques como phishing, ransomware, malware e exploração de vulnerabilidades em software são algumas das principais ameaças enfrentadas globalmente, sendo necessárias estratégias que combinem tecnologias de segurança com a capacitação de usuários para lidar com esses riscos .

Além disso, a segurança cibernética é um componente essencial da cidadania digital. De acordo com Buchanan et al. [26], educar as pessoas sobre segurança cibernética envolve não apenas a implementação de medidas técnicas de proteção, mas também o desenvol-

vimento de uma cultura de responsabilidade digital, onde os indivíduos compreendem os riscos envolvidos em suas atividades online e adotam práticas seguras, como o uso de senhas fortes, a verificação de fontes e a proteção de dados pessoais . Isso é particularmente relevante no contexto educacional, onde professores e alunos estão cada vez mais expostos a riscos no ambiente digital. Assim, ao incorporar práticas de segurança cibernética no currículo escolar, pode-se empoderar os indivíduos a protegerem seus dados e dispositivos, promovendo um ambiente digital mais seguro e ético.

3.4 Privacidade Digital

Privacidade digital refere-se à proteção dos dados e informações pessoais que os indivíduos compartilham ou geram ao utilizar dispositivos conectados à internet. Na era da informação, o conceito de privacidade se expandiu para além dos limites físicos, envolvendo o controle sobre como os dados são coletados, utilizados, armazenados e compartilhados em ambientes digitais. Segundo Almeida e Silva [27], a privacidade digital é um direito fundamental que visa garantir que os dados pessoais não sejam utilizados de maneira inadequada ou sem o consentimento dos indivíduos. Essa questão tornou-se cada vez mais relevante com o crescimento da coleta massiva de dados e da vigilância em ambientes digitais, que colocam em risco o controle que o usuário tem sobre suas informações.

Nos ambientes educacionais, a privacidade digital tem um papel crucial, uma vez que o uso de dispositivos digitais e o compartilhamento de dados se tornam parte integrante do processo de ensino-aprendizagem. Greenleaf [28] ressalta que as escolas, além de serem responsáveis pela proteção dos dados dos alunos, também devem educar sobre os riscos associados ao uso inadequado de tecnologias. A privacidade digital, portanto, não se limita apenas à proteção de dados, mas também abrange a conscientização sobre o uso ético e seguro das informações no ambiente online[29].

O conceito de privacidade digital está intimamente ligado à noção de controle e consentimento. Conforme discutido por Costa e Souza [30], a privacidade digital envolve o direito de controlar o acesso e o uso de dados pessoais e a necessidade de consentimento explícito antes que esses dados possam ser coletados ou compartilhados. Assim, um dos desafios da privacidade digital está em garantir que os indivíduos compreendam os impactos do compartilhamento de informações online e como manter um controle adequado sobre seus dados.

A privacidade digital também se relaciona diretamente com a cidadania digital, discutida no capítulo anterior do presente trabalho. O empoderamento dos educadores, no contexto da segurança digital, passa por proporcionar aos alunos uma compreensão mais profunda sobre a importância de resguardar suas informações em ambientes on-

line, garantindo a proteção de seus dados pessoais, conforme proposto por Greenleaf [28]. Dessa forma, garantir que os professores sejam letrados digitalmente também implica em capacitá-los a ensinar a importância da privacidade digital aos seus alunos, promovendo uma navegação mais segura e ética.

3.5 Proteção de Informações Pessoais

O conceito de "Proteção de Informações Pessoais"está diretamente relacionado ao direito à privacidade e à gestão de dados em um ambiente digital. Ele diz respeito à salvaguarda de informações que identificam direta ou indiretamente uma pessoa, como nome, endereço, e-mail, dados financeiros e outras informações sensíveis que, se expostos ou manipulados indevidamente, podem trazer prejuízos aos indivíduos. A proteção de dados pessoais abrange tanto a coleta, armazenamento e processamento dessas informações, quanto o consentimento do indivíduo e a garantia de que seus dados não serão usados para finalidades não autorizadas.

A legislação internacional e nacional, como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, estabelecem princípios para assegurar que as entidades públicas e privadas adotem medidas adequadas para garantir a privacidade dos dados pessoais. Conforme Doneda [31] destaca, a proteção de dados pessoais transcende a simples ideia de privacidade, pois envolve também a capacidade de controlar as informações e o direito de saber como elas são utilizadas. Dessa forma, a proteção de dados pessoais é uma medida preventiva, que visa não apenas resguardar a privacidade, mas também prevenir possíveis abusos de poder ou exploração econômica dos dados, como apontado por Ruaro e Rodriguez [32].

Além disso, a proteção de dados está intrinsecamente ligada à ideia de autonomia do indivíduo no ambiente digital, na medida em que se refere à capacidade de gerenciar e controlar as informações que circulam sobre si próprio, conforme mencionado por Schaar [33]. No contexto educacional, essa proteção torna-se ainda mais relevante, considerando a quantidade de informações pessoais de alunos que são coletadas por instituições de ensino e o uso crescente de tecnologias digitais no processo de ensino-aprendizagem.

3.6 Segurança de Dispositivos

Segurança de dispositivos refere-se ao conjunto de práticas, políticas e tecnologias empregadas para proteger dispositivos eletrônicos, como computadores, smartphones e tablets, contra ameaças cibernéticas, acessos não autorizados e roubo de dados. Esse conceito envolve a aplicação de medidas para garantir a integridade, confidencialidade e disponibi-

lidade das informações armazenadas nos dispositivos, além de proteger as comunicações e operações realizadas por eles. A segurança de dispositivos se faz essencial em um ambiente digital cada vez mais complexo, no qual tanto indivíduos quanto organizações estão expostos a vulnerabilidades, como malware, ataques de phishing, e de hacking.

A proteção de dispositivos pode incluir o uso de software de segurança, como antivírus e firewalls, autenticação multifatorial, criptografia de dados, atualizações regulares de software e a adoção de boas práticas de uso, como não clicar em links suspeitos e evitar o uso de redes públicas desprotegidas. Segundo Karabatak et al. [34], a segurança de dispositivos é um componente vital para a proteção de dados pessoais e corporativos, garantindo que os usuários tenham controle sobre suas informações e reduzindo o risco de ataques cibernéticos. Além disso, Amrozi et al. [35] apontam que o aumento do uso de dispositivos móveis e a crescente conectividade tornaram essa questão ainda mais relevante, exigindo uma abordagem robusta para a segurança desses dispositivos em diversos contextos, como ambientes corporativos e educacionais.

Quando conectada ao ensino de cidadania digital, a conscientização sobre segurança de dispositivos capacita tanto professores quanto alunos a utilizarem a tecnologia de maneira responsável e segura, minimizando os riscos associados ao uso de dispositivos conectados à internet.

3.7 Rastros Digitais

"Rastros digitais"referem-se às informações que os indivíduos deixam para trás ao utilizar tecnologias digitais, como navegações na web, interações em redes sociais, compras online, e-mails, ou o uso de dispositivos conectados. Esses rastros são divididos em dois tipos principais: rastros ativos e rastros passivos. Rastros ativos são aqueles que o usuário cria de forma intencional, como publicar em redes sociais, enviar e-mails ou preencher formulários online. Já os rastros passivos são gerados automaticamente por sistemas, sem que o usuário esteja ciente, como endereço IP, cookies de navegação ou dados de localização geográfica [36].

A coleta e o uso de rastros digitais têm implicações importantes em termos de privacidade e segurança digital. Muitos serviços online utilizam essas informações para personalizar anúncios, aprimorar a experiência do usuário ou monitorar comportamentos, mas isso também pode representar riscos à privacidade, como a exposição de informações sensíveis sem o consentimento dos indivíduos [37]. Nesse contexto, torna-se essencial que os usuários de tecnologia estejam conscientes sobre os rastros digitais que deixam ao utilizar diferentes plataformas, sendo capazes de controlar o compartilhamento de dados

pessoais e compreender as implicações legais e éticas envolvidas, como apontam Pereira & Almeida [38].

Os rastros digitais são um tema central na educação para a cidadania digital e a segurança online, especialmente quando se trata de preparar crianças e jovens para navegarem de forma segura no ambiente virtual. No contexto educacional, é fundamental ensinar os alunos a gerenciar seus rastros digitais de maneira crítica e consciente, uma vez que essas pegadas podem ser usadas para rastrear comportamentos ou até mesmo comprometê-los em situações de segurança, como fraudes e roubo de identidade [39].

3.8 Alfabetização Midiática

"Alfabetização midiática", também conhecida como letramento midiático, é um conceito que se refere ao desenvolvimento de habilidades para acessar, analisar, avaliar e criar conteúdos em diferentes formas de mídia. Segundo Buckingham [40], essa competência envolve não apenas a capacidade de usar tecnologias e plataformas de mídia, mas também a compreensão crítica de como os conteúdos são produzidos, distribuídos e consumidos na sociedade. Alfabetizar-se midiaticamente implica em reconhecer os efeitos da mídia na formação de opiniões, comportamentos e na construção da realidade social, além de capacitar indivíduos a serem consumidores críticos e produtores ativos de conteúdo.

A alfabetização midiática tem como objetivo empoderar os indivíduos para que possam navegar no complexo ambiente midiático contemporâneo, distinguindo entre informações confiáveis e enganosas, como destaca Hobbs [41]. Em um mundo digital permeado por fake news, desinformação e manipulação de imagens e dados, a alfabetização midiática torna-se essencial para o exercício da cidadania. Ela prepara os indivíduos a questionarem a veracidade das informações, a entenderem as intenções por trás de certos discursos midiáticos e a utilizarem a mídia de forma ética e responsável. A introdução dessa alfabetização nas escolas tem sido recomendada por estudiosos como Jenkins [42], que defendem a integração de práticas educativas voltadas ao letramento midiático para preparar as novas gerações para o cenário digital.

3.9 Direitos Autorais

Os direitos autorais são um conjunto de normas jurídicas que visam proteger as obras intelectuais e criativas, garantindo ao criador ou autor o controle sobre o uso e a reprodução de sua obra. Esses direitos são reconhecidos mundialmente como fundamentais para incentivar a produção intelectual e artística, ao assegurar aos criadores o reconhecimento de sua autoria e a compensação pelo uso de suas criações. De acordo com o World

Intellectual Property Organization [43], os direitos autorais englobam não apenas obras literárias, artísticas e científicas, mas também conteúdos digitais, softwares, músicas, filmes, fotografias e até obras disponibilizadas em ambientes virtuais.

Conforme exposto por Silva [44], os direitos autorais garantem ao autor o poder de decisão sobre a reprodução, distribuição e exibição de sua obra, estabelecendo assim um equilíbrio entre o interesse público de acesso à cultura e o direito privado do criador. Uma das premissas centrais dos direitos autorais é a exclusividade que o autor detém sobre o uso de sua obra por um determinado período, após o qual ela pode entrar em domínio público, permitindo que qualquer pessoa a utilize sem a necessidade de autorização prévia.

Outro aspecto relevante dos direitos autorais, conforme Pontes [45], refere-se à proteção tanto dos direitos morais quanto dos direitos patrimoniais. Os direitos morais garantem ao autor a proteção contra modificações indevidas em sua obra, a atribuição correta de sua autoria e o direito de preservar a integridade do conteúdo. Já os direitos patrimoniais tratam da exploração econômica da obra, garantindo que o autor receba uma remuneração justa pelo uso comercial de sua criação.

No ambiente digital, os desafios associados à proteção dos direitos autorais têm se intensificado. As facilidades de compartilhamento, reprodução e disseminação de obras criativas na internet, muitas vezes sem o devido consentimento dos autores, levantam questões sobre a eficácia dos sistemas tradicionais de proteção. A pirataria digital e o uso indevido de conteúdos protegidos são problemas recorrentes que colocam em risco a remuneração e a sustentabilidade dos criadores. Nesse contexto, conforme abordado por Pereira [46], as ferramentas tecnológicas, como as licenças digitais e os sistemas de gestão de direitos digitais (DRM), surgem como mecanismos para mitigar os desafios e assegurar que os direitos autorais sejam respeitados no ambiente virtual.

Portanto, o respeito aos direitos autorais é crucial para garantir a continuidade da produção cultural e intelectual, e sua proteção no mundo digital requer uma conscientização dos usuários, especialmente no contexto educacional. Ensinar sobre direitos autorais nas escolas, como proposto por Melo (2020), ajuda a formar cidadãos conscientes do valor da criação artística e científica e de sua responsabilidade ao consumir e compartilhar conteúdos.

Ensinar sobre direitos autorais nas escolas é uma ação de extrema relevância no contexto educacional contemporâneo. Em um mundo cada vez mais digital e interconectado, os estudantes têm acesso facilitado a uma grande quantidade de materiais online, incluindo músicas, filmes e textos, muitos dos quais são protegidos por direitos autorais. Portanto, é crucial que os jovens aprendam desde cedo sobre as implicações legais e éticas relacionadas ao uso de materiais protegidos, de forma que eles não apenas respeitem os direitos dos criadores, mas também entendam o valor da produção intelectual [47].

Ao incluir o ensino de direitos autorais no currículo escolar, promove-se a educação para a cidadania digital, ajudando os alunos a desenvolverem uma postura ética em suas interações no ambiente digital. Eles passam a compreender que, ao violar os direitos autorais, não estão apenas infringindo uma lei, mas também desrespeitando o esforço criativo de indivíduos ou empresas. Isso é particularmente importante em um mundo onde o plágio e o compartilhamento não autorizado de conteúdos se tornaram práticas comuns entre os jovens [48]. Ao desenvolver essa consciência, os alunos estão mais bem preparados para navegar na internet de forma responsável, contribuindo para uma cultura de respeito à criação intelectual e ajudando a promover uma comunidade digital mais justa e equitativa.

Capítulo 4

Análise da proposta atual do desenvolvimento de competências e habilidades relacionadas com a segurança nos anos iniciais do Ensino Fundamental

4.1 Importância da educação da sociedade sobre os objetos de conhecimento relacionados à segurança

A segurança cibernética agora é uma preocupação globalmente reconhecida e relevante. De acordo com o Índice Global de Segurança Cibernética 2020, divulgado pela ONU [23], mais de 167 países divulgaram oficialmente algum tipo de documento estratégico detalhando sua posição oficial em relação ao ciberespaço, crimes cibernéticos e/ou segurança cibernética.

De acordo com a pesquisa TIC Domicílios 2023 [49], no Brasil 84% da população tem acesso a internet e na faixa etária de 10 a 15 anos, essa porcentagem sobe para 92% . Apesar de trazer inúmeros benefícios, a proliferação de dispositivos eletrônicos, aplicativos e plataformas online introduz uma série de riscos que devem ser cuidadosamente considerados.

Em um estudo publicado em 2024 sobre segurança online no ambiente educacional moderno [50], os autores utilizam a metodologia de revisão sistemática de literatura para justificar a importância de fomentar a conscientização sobre segurança online. Destacam-se alguns trechos abaixo sobre a relevância da apropriação dos conceitos de segurança

desde a educação mais básica para mitigar os riscos e construir um futuro mais seguro para todos:

- Livingstone & Helsper (2008) [51] ressaltam a importância de implementar programas de conscientização que abordem os riscos associados à privacidade online, ao ciberbullying e ao acesso a conteúdo inadequado. Essas iniciativas devem ser abrangentes, envolvendo estudantes, educadores e pais, reconhecendo que a segurança online é uma responsabilidade compartilhada.
- Além disso, é crucial desenvolver estratégias para promover a cidadania digital responsável. Ribble (2015) [17] introduz o conceito de cidadania digital, que engloba a compreensão do uso apropriado e responsável da tecnologia. A cidadania digital não se limita à mitigação de riscos, mas também inclui a capacidade de aproveitar as oportunidades oferecidas pelas tecnologias digitais de maneira ética e eficaz.
- Boyd (2020) [52] destaca a importância de compreender como os jovens interagem com as tecnologias digitais. Programas educacionais e de conscientização devem ser baseados em uma compreensão realista do uso da tecnologia pelos jovens, promovendo habilidades digitais relevantes para suas experiências cotidianas.
- Por fim, de acordo com a proposta de Buckingham (2007) [53] , a educação digital não deve se restringir apenas à aquisição de habilidades técnicas; ela também deve abranger a compreensão crítica dos meios de comunicação, a ética online e a consciência dos direitos digitais. Isso prepara os indivíduos não apenas para enfrentar os desafios do ambiente digital, mas também para se tornarem participantes ativos e bem informados na sociedade digital.

4.2 Legislação e Políticas de Segurança Digital na Educação

No contexto das políticas educacionais voltadas para a segurança digital, é imperativo que as instituições de ensino implementem medidas eficazes para proteger os dados e a privacidade dos alunos. Greenleaf (2014) [28] destaca que essas políticas devem ir além da mera conformidade com as leis de proteção de dados, exigindo a adoção de práticas robustas de segurança cibernética. Isso inclui a capacitação dos funcionários sobre a importância da segurança da informação e o estabelecimento de protocolos claros para lidar com eventuais violações de dados.

A UNESCO (2017) [4] sublinha a importância de educar os estudantes sobre seus direitos digitais, em especial no que tange à privacidade online, além de conscientizá-los sobre

suas responsabilidades no uso das tecnologias digitais. A formação dos alunos nessa área é crucial para que possam navegar de maneira segura e responsável no ambiente digital. Além disso, Lentini (2015) reforça a relevância de políticas educacionais que integrem a cidadania digital no currículo, abordando aspectos legais do uso da internet, como direitos autorais e ética digital, preparando os estudantes para os desafios da sociedade digital conectada.

Sampaio e Fernandes (2019) [29] ressaltam que os educadores possuem o dever de orientar os alunos no uso seguro e ético das tecnologias digitais, mas também têm o direito de receber formação contínua para se atualizarem sobre as melhores práticas de segurança digital. Dessa forma, a legislação e as políticas de segurança digital no âmbito educacional desempenham um papel essencial, não apenas na proteção de dados e privacidade, mas também na promoção de um ambiente de aprendizado seguro e responsável. As escolas devem, portanto, estar atentas às suas responsabilidades legais e éticas, trabalhando de forma ativa para educar alunos e educadores sobre os desafios e as oportunidades da era digital.

4.3 Base Nacional Comum Curricular (BNCC)

Homologada pelo Ministério da Educação, a Base Nacional Comum Curricular (BNCC) é uma norma nacional que propõe o desenvolvimento de determinadas competências e habilidades ao longo da jornada de um aluno na Educação Básica. Publicada em 2017 [1], levou em consideração artigos específicos da Constituição Federal e da Lei de Diretrizes e Bases da Educação Nacional (LDB) e diversas outras orientações de ordem legal e normativa. O Conselho Nacional de Educação desenvolveu então o trabalho de discussão e elaboração do documento mediante articulação e ampla participação de toda a comunidade educacional e sociedade brasileira.

A resolucao CNE/CP no 2, de 22 de dezembro de 2017 institui no Art. 1o e 2o a Base Nacional Comum Curricular (BNCC) como "documento de caráter normativo que define o conjunto orgânico e progressivo de aprendizagens essenciais no âmbito da Educação Básica escolar."Essas aprendizagens essenciais são definidas como "conhecimentos, habilidades, atitudes, valores e a capacidade de os mobilizar, articular e integrar, expressando-se em competências."O Art. 3o diz que "No âmbito da BNCC, competência é definida como a mobilização de conhecimentos (conceitos e procedimentos), habilidades (práticas cognitivas e socioemocionais), atitudes e valores, para resolver demandas complexas da vida cotidiana, do pleno exercício da cidadania e do mundo do trabalho."

De acordo com o O Art. 14, A BNCC está organizada em Áreas do Conhecimento: Linguagens, Matemática, Ciências da Natureza, Ciências Humanas e Ensino Religioso.

E, apesar da versão publicada nessa época não existir a área de Computação, já existiam conhecimentos, competências e habilidades envolvendo o conceito de segurança referenciados em algumas Áreas do Conhecimento, descritas a seguir:

Linguagens

Competência específica 6 Compreender e utilizar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares), para se comunicar por meio das diferentes linguagens e mídias, produzir conhecimentos, resolver problemas e desenvolver projetos autorais e coletivos.

Ciências da natureza

Competência específica 6 Utilizar diferentes linguagens e tecnologias digitais de informação e comunicação para se comunicar, acessar e disseminar informações, produzir conhecimentos e resolver problemas das Ciências da Natureza de forma crítica, significativa, reflexiva e ética.

Ciências Humanas

Não temos uma competência específica, mas a BNCC da área de Ciências Humanas prevê que sejam enfatizadas as aprendizagens dos estudantes relativas ao desafio de dialogar com o outro e com as novas tecnologias. Considerando que as novas tecnologias exercem influência, às vezes negativa, outras vezes positiva, no conjunto das relações sociais, é necessário assegurar aos estudantes a análise e o uso consciente e crítico dessas tecnologias, observando seus objetivos circunstanciais e suas finalidades a médio e longo prazos, explorando suas potencialidades e evidenciando seus limites na configuração do mundo contemporâneo.

4.4 BNCC de Computação

4.4.1 Histórico

O parecer sobre a resolução de 2017 acima citada, no Capítulo V (Das Disposições Finais e Transitórias), artigo 22 determina que "O CNE elaborará normas específicas sobre computação". Em resposta a essa determinação e em resposta à Indicação CNE/CEB no 3/2019, formou-se uma comissão para elaborar a BNCC de Computação. Além da comissão, houve a contribuição de entidades como a Sociedade Brasileira de Computação (SBC), o Ministério da Educação (MEC) e o Conselho Nacional de Secretários de

Educação (CONSED), além da realização de eventos como o "Seminário Internacional sobre Computação na Educação Básica"e a participação da CEB no CSforAll Summit, visando discutir desafios e perspectivas para a implementação de políticas educacionais de computação no Brasil e no exterior.

O documento foi aprovado em 17 de fevereiro de 2022, com a publicação do Parecer CNE/CEB nº 2/2022, – Normas sobre Computação na Educação Básica – Complemento à Base Nacional Comum Curricular (BNCC).

4.4.2 Ensino de computação no Brasil

O Parecer CNE/CEB nº 2/2022 destaca o histórico do ensino da computação na educação básica, desde a década de 1960 até os dias atuais, abordando a evolução das discussões e práticas nesse campo. A partir da criação da linguagem Logo e da proposta do Construcionismo por Papert, Solomon e Feurzeig, surgiram reflexões sobre a introdução da computação no ensino, culminando na expressão "Letramento Computacional"proposta por DiSessa e no conceito de "Pensamento Computacional"discutido por Wing e outros [54]. No Brasil, o ensino da computação começou a ser desenvolvido em universidades como UFSC, UFRGS, UFRJ, UNICAMP e USP na década de 1970, com experimentos e desenvolvimento de softwares educacionais. Essas iniciativas foram impulsionadas por eventos como a I Conferência Nacional de Tecnologia Aplicada ao Ensino Superior e o I Seminário Nacional de Informática na Educação, que proporcionaram a troca de experiências entre pesquisadores nacionais e internacionais.

Além disso, o documento menciona políticas e programas implementados pelo governo brasileiro, como o Projeto EDUCOM e o Programa Nacional de Informática Educativa (PRONINFE), que visavam promover o uso educacional da informática nas escolas públicas. Destaca-se a criação do Programa Nacional de Informática na Educação (ProInfo) e do Projeto de Informática na Educação Especial (PROINESP), evidenciando esforços para a inclusão digital e a formação de professores. Por fim, são apresentadas diferentes abordagens para a introdução da computação na educação básica, incluindo o Construcionismo, o Pensamento Computacional, as demandas do mercado e a equidade e inclusão, destacando a importância do desenvolvimento do pensamento computacional para os estudantes.

4.4.3 Licenciatura em Computação no Brasil

A Resolucao CNE/CP nº 2, de 22 de dezembro de 2017 aborda a emergência e o desenvolvimento dos Cursos de Licenciatura em Computação no Brasil, destacando sua importância diante do crescente impacto da computação no desenvolvimento econômico e

educacional. Com o contexto da pandemia de Covid-19 e a necessidade de educação mediada por tecnologias digitais, a sociedade brasileira reconhece a demanda por profissionais capacitados para lecionar computação na Educação Básica. Iniciativas como a criação de um Grupo de Trabalho pela Sociedade Brasileira de Computação para elaborar um Currículo de Referência e a posterior homologação desse currículo durante o Congresso da SBC são citadas. A Resolução do CNE em 2016 estabeleceu as Diretrizes Curriculares Nacionais para os cursos de graduação na área da Computação, incluindo a Licenciatura em Computação, alinhando-se com a legislação educacional vigente.

O documento destaca a importância dos licenciados em Computação dominarem conceitos fundamentais da área, explorarem o pensamento computacional e colaborarem com outros docentes na construção de narrativas pedagógicas eficazes. Enfatiza-se também a necessidade desses profissionais para enfrentar os desafios da digitalização da educação e garantir a continuidade e o sucesso da Educação Básica no Brasil, ressaltando sua contribuição para o desenvolvimento das habilidades e competências previstas na BNCC.

4.4.4 Computação na educação básica

Nesse tópico, aborda-se a centralidade da computação na contemporaneidade e seu impacto na educação e na sociedade como um todo. Destaca-se a necessidade de desenvolver habilidades fundamentais da era digital, como pensamento crítico, resolução de problemas, criatividade e ética, por meio da integração da computação na educação. Além disso, ressalta-se a importância de formar cidadãos preparados para o pleno desenvolvimento da cidadania e para o mundo do trabalho, considerando o atual cenário informacional. A Ciência da Computação é apresentada como uma disciplina essencial para compreender e lidar com um um futuro cada vez mais digitalizado e complexo e com os desafios da Quarta Revolução Industrial, influenciando não apenas o setor econômico, mas também as relações sociais, culturais e educacionais. O relatório do Fórum Econômico Mundial sobre as escolas do futuro destaca a importância de habilidades como cidadania global, inovação, habilidades digitais e aprendizagem colaborativa para direcionar os estudantes para essa próxima revolução.

As recomendações de organismos internacionais, como a OCDE, UNESCO e UNICEF, são mencionadas para enfatizar a necessidade urgente de incluir fundamentos de tecnologias digitais nos sistemas educacionais. A inclusão de questões computacionais no Programa Internacional de Avaliação de Estudantes (Pisa) e a elaboração de diretrizes de ensino de computação na Educação Básica pela Sociedade Brasileira de Computação evidenciam a relevância crescente da computação na educação brasileira.

Portanto, a formação em computação é considerada crucial para capacitar os estudantes a compreender, criar e utilizar tecnologias digitais de forma crítica, ética e responsável, preparando-os para os desafios do mundo contemporâneo.

4.4.5 Implementação da Computação na educação básica

Essa seção do texto da BNCC ressalta a importância da inclusão do ensino de Computação na educação básica, destacando que países que adotaram essa prática geralmente começaram nos Anos Finais do Ensino Fundamental ou no Ensino Médio, cerca de uma década atrás (Duncan, Bell, 2015). No contexto brasileiro, é enfatizada a necessidade de políticas públicas que garantam o acesso à Computação a todos os estudantes, respeitando as diversas peculiaridades e desigualdades presentes na educação pública (Siqueira, 2020). A implementação efetiva da Computação na Educação Básica requer a consideração de diversos parâmetros, como formação de professores, desenvolvimento de currículo, disponibilização de recursos didáticos compatíveis e gestão do processo de implementação. Além disso, destaca-se a importância da avaliação formativa e somativa para verificar os resultados e realizar ajustes necessários. A formação contínua dos professores é fundamental, podendo ser realizada por meio de cursos online, visando ampliar o número de docentes capacitados (INEP, 2019; CSTA, 2022). A BNCC oferece orientações quanto às competências e habilidades a serem desenvolvidas em cada etapa da Educação Básica, inclusive na Educação Infantil, onde são ressaltados temas como segurança online, destacando a importância de adaptar os conhecimentos técnicos necessários à idade dos alunos. No Ensino Fundamental, sugere-se uma implementação gradual, considerando as especificidades de cada segmento, e no Ensino Médio, a implementação também deve ocorrer de forma progressiva. Recomenda-se a criação de uma estrutura operacional pelo MEC para acompanhar a implementação da política, abrangendo formação de professores, recursos didáticos, assessoramento aos sistemas de ensino e avaliação do processo (BNCC, 2020).

4.4.6 Legislação

A legislação educacional brasileira, representada pela Constituição Federal de 1988, a Lei de Diretrizes e Bases da Educação Nacional (LDB) e as Diretrizes Curriculares Nacionais (DCNs), estabelece princípios fundamentais para a promoção da educação básica e do desenvolvimento integral dos estudantes. Esses documentos enfatizam a importância da inclusão de habilidades computacionais desde a Educação Básica, alinhando-se com as recomendações de organismos internacionais.

Os princípios constitucionais destacam a necessidade de preparar os cidadãos para o pleno exercício da cidadania e para o mundo do trabalho, incluindo o desenvolvimento

científico e tecnológico. A LDB e as DCNs reforçam essa perspectiva, estabelecendo objetivos claros para a educação básica, como a formação comum indispensável para a cidadania e o desenvolvimento de competências para a vida pessoal e profissional.

A inclusão de habilidades computacionais é vista como essencial para alcançar esses objetivos, pois a ciência da computação permeia diversos aspectos da vida contemporânea. Além de proporcionar o desenvolvimento de habilidades de resolução de problemas e pensamento crítico, o ensino de computação também promove a compreensão do mundo digital e seu impacto na sociedade.

A transversalidade da computação na proposta curricular, desde a Educação Infantil até o Ensino Médio, é enfatizada como uma forma de garantir uma formação integral e alinhada com as demandas do século XXI. Os Itinerários Formativos no Ensino Médio destacam a importância de incluir conteúdos relacionados à matemática e suas tecnologias, como programação, robótica e inteligência artificial, para preparar os estudantes para os desafios do mundo contemporâneo.

Em suma, a legislação e as diretrizes educacionais brasileiras reconhecem a importância da inclusão de habilidades computacionais na educação básica, visando preparar os estudantes para uma sociedade cada vez mais digital e tecnológica. Essa abordagem busca promover não apenas o desenvolvimento de competências técnicas, mas também o pensamento crítico, a criatividade e a cidadania ativa.

4.5 Segurança na BNCC de Computação

Dentre todas as habilidades descritas na BNCC de computação, aqui iremos destacar por etapa as que pertencem ao eixo de cultura digital, tendo a segurança e a responsabilidade no uso da tecnologia computacional como objetos do conhecimento. A habilidade, sua explicação e exemplos explicitados abaixo estão exatamente como se encontram no documento oficial.

4.5.1 1o Ano - Ensino Fundamental

Habilidade: Conhecer as possibilidades de uso seguro das tecnologias computacionais para proteção dos dados pessoais e para garantir a própria segurança.

Explicação da habilidade: Esta habilidade propõe que o aluno possa refletir sobre a importância de resguardar dados pessoais como nome, endereço, idade, onde estuda, quando da utilização de tecnologias como celular, tablets, em que não se pode compartilhar essas informações com qualquer pessoa.

Exemplos: Professor poderá fazer um jogo de imagens de dispositivos como celular, tablet, computador dentre outros em que os alunos precisam apresentar o que as pessoas

fazem com essas tecnologias. Assim, o professor poderá destacar os cuidados quando usamos esses dispositivos.

4.5.2 2o Ano - Ensino Fundamental

Habilidade: Reconhecer os cuidados com a segurança no uso de dispositivos computacionais.

Explicação da habilidade: Nesta habilidade temos a perspectiva de trazer um panorama sobre os cuidados com a segurança ao usar dispositivos como celular, tablets, computadores dentre outros (roubo de dados em dispositivos físicos, rastro de dados online quando da utilização de jogos por exemplo etc.).

Exemplos: O professor poderá criar um portfólio com alguns cuidados ao jogar nos dispositivos como celular, tablets.

4.5.3 3o Ano - Ensino Fundamental

Habilidade: Reconhecer o potencial impacto do compartilhamento de informações pessoais ou de seus pares em meio digital.

Explicação da habilidade: A proposta nesta habilidade é que o aluno possa identificar alguns dos principais impactos de compartilhar informações pessoais com colegas ou pessoas em meio digital, como por exemplo endereço, nomes das pessoas da família, onde estuda, onde mora. Essas informações podem ser utilizadas por pessoas de forma mal-intencionadas, quando os alunos trocam informações online por celular, computador ou até mesmo quando estão jogando na internet.

Exemplos: O professor poderá apresentar um caso em que foram utilizados dados roubados de pessoas, solicitando aos alunos que destaquem o que pode ter acontecido para que os dados pudessem ter sido roubados. Poderá ainda, a partir do que foi levantado pelos alunos, criar um painel com imagens dos dispositivos computacionais como tablets, celular, computador, apontando em cada um os impactos de acordo com o que mais se utiliza nesses dispositivos.

4.5.4 4o Ano - Ensino Fundamental

Habilidade I: Demonstrar postura ética nas atividades de coleta, transferência, guarda e uso de dados.

Explicação da habilidade I: Propõe-se que o aluno reflita sobre aspectos éticos relacionados a manipulação de dados, como por exemplo quando assiste e faz download, compartilha uma imagem, dentre outros.

Exemplos: Construção de um painel, a partir das imagens de tecnologias como o celular e computador, em que os alunos poderão destacar ações importantes de quando se manipula um dado como imagem, música, vídeo, informação, como verificar as permissões, autoria, dentre outros.

Habilidade II: Reconhecer a importância de verificar a confiabilidade das fontes de informações obtidas na Internet.

Explicação da habilidade II: Nesta habilidade espera-se que os alunos possam reconhecer que, ao se obter informações na Internet, é preciso identificar as suas fontes e se elas são seguras e a informação é confiável.

Exemplos: O professor poderá organizar casos em que se precisa de determinadas informações e ao se deparar com elas, se verifica que muitas dessas informações estão equivocadas, comparando páginas que tratam do mesmo tema, mas com informações diferentes como por exemplo em uma biografia.

4.5.5 5o Ano - Ensino Fundamental

Habilidade I: Acessar as informações na Internet de forma crítica para distinguir os conteúdos confiáveis de não confiáveis.

Explicação da habilidade I: Nesta habilidade é importante que os alunos possam refletir e acessar informações em buscas na Internet criticamente, identificando características de conteúdos prejudiciais, informações confiáveis, notícias falsas.

Exemplos: O professor pode propor um estudo comparativo entre sites de jornais oficiais e blogs para falar sobre as fontes de informação, considerando sua confiabilidade.

Habilidade II: Usar informações considerando aplicações e limites dos direitos autorais em diferentes mídias digitais.

Explicação da habilidade II: O objetivo desta habilidade é que o aluno possa utilizar informações e dados na Internet reconhecendo os direitos autorais, como por exemplo de uma música, um filme, um livro, e os cuidados em seu compartilhamento e uso pessoal.

Exemplos: O aluno poderá criar um portfólio com imagens de personagens de desenhos animados em que ele poderá citar as fontes e propor um formato em que considera todos os direitos autorais

Capítulo 5

Proposta de atividades para letramento em segurança digital no Ensino Fundamental

Essas são as ideias iniciais de atividades para cada habilidade destacada na BNCC para cada ano do ensino fundamental, todas as habilidades estão no mesmo eixo e objeto de conhecimento e todas as atividades seguem o mesmo padrão, explicitado abaixo:

5.1 Estrutura das atividades

Eixo: Cultura Digital

Objeto de conhecimento: Segurança e responsabilidade no uso de tecnologia computacional

Habilidade: Descrição da habilidade como está na BNCC.

Explicação da habilidade: Explicação da habilidade como está na BNCC.

Atividade: **Objetivo:** O que quer se ensinar ou capacitar. **Material necessário:** Materiais para desenvolvimento da atividade. **Diagnóstico inicial:** Momento em que o professor faz uma análise se os alunos possuem os conhecimentos prévios necessários pra cada atividade, tendo assim um ponto de partida inicial. **Atividade em si:** Passo a passo descrevendo a atividade e o que deverá ser feito.

Reflexão em grupo: Momento de reflexão final para avaliação da eficiência e eficácia da atividade.

Material complementar: Proposta de material para reforçar o conteúdo visto em sala e incentivar o aluno a levar as discussões também para dentro de sua casa.

5.2 Justificativa para atividades offline e sem uso de computadores

A escolha por desenvolver atividades offline e sem o uso de computadores nas aulas de segurança digital parte de uma análise da realidade socioeconômica e educacional brasileira. O Brasil, sendo um país de grandes desigualdades regionais, enfrenta sérios desafios no que diz respeito à infraestrutura tecnológica nas escolas públicas. De acordo com o Cetic.br, cerca de 34% das escolas públicas urbanas e uma porcentagem ainda maior nas áreas rurais não possuem acesso adequado à internet ou enfrentam limitações no uso de dispositivos tecnológicos [49]. Além disso, muitas escolas têm apenas um número reduzido de computadores funcionais, o que impede o uso pleno de recursos digitais em sala de aula. [55]

Nesse contexto, atividades lúdicas e pedagógicas offline são uma alternativa eficaz para garantir que a educação em segurança digital seja acessível a todos os estudantes, independentemente de sua condição social ou de infraestrutura tecnológica disponível. Essas atividades oferecem aos alunos uma oportunidade de aprender sobre segurança digital, proteção de dados pessoais e comportamento online seguro, sem depender de recursos que podem não estar disponíveis na maioria das escolas públicas.

Outro ponto importante é que o uso de metodologias ativas e jogos interativos, que não exigem acesso à internet ou dispositivos digitais, promove uma maior inclusão e equidade no ensino. Tais metodologias, baseadas em teorias como a Aprendizagem Significativa de Ausubel [56] e as propostas construtivistas de Piaget e Vygotsky, permitem que o aprendizado seja centrado na experiência concreta dos alunos, oferecendo um ambiente colaborativo e reflexivo [57] [58].

Além disso, ao desenvolver atividades que podem ser realizadas sem computadores, os professores têm mais liberdade para adaptar o conteúdo às necessidades específicas da turma, incluindo aqueles que têm pouca ou nenhuma experiência com tecnologia. Isso permite que a segurança digital seja introduzida de forma prática e contextualizada, garantindo que todos os alunos possam participar ativamente das atividades e compreender os conceitos fundamentais sem barreiras tecnológicas.

Portanto, a implementação de atividades offline é uma escolha pedagógica consciente que visa democratizar o acesso ao ensino de segurança digital, promovendo uma educação inclusiva e adaptada às realidades de um país tão diverso como o Brasil. Essa abordagem garante que a BNCC possa ser implementada com sucesso em diferentes contextos, sem deixar para trás estudantes que não têm acesso a dispositivos tecnológicos ou à internet.

5.3 1º Ano

Habilidade: Conhecer as possibilidades de uso seguro das tecnologias computacionais para proteção dos dados pessoais e para garantir a própria segurança.

Explicação da habilidade: Esta habilidade propõe que o aluno possa refletir sobre a importância de resguardar dados pessoais como nome, endereço, idade, onde estuda, quando da utilização de tecnologias como celular, tablets, em que não se pode compartilhar essas informações com qualquer pessoa.

5.3.1 Atividade: Jogo "Pode ou não pode?"

Objetivo: Ensinar as crianças a reconhecerem informações pessoais e a importância de mantê-las seguras ao utilizar tecnologias como celulares e tablets.

Diagnóstico inicial:

- **Você já usou um celular ou tablet para jogar ou assistir vídeos? Quem ajuda você a usar?** Objetivo: Verificar se as crianças já têm experiência com o uso de dispositivos digitais e se dependem de orientação de adultos, o que influencia na compreensão de segurança digital.
- **Você sabe o que são informações pessoais? Quais informações sobre você você acha que deve guardar em segredo?** Objetivo: Avaliar se os alunos têm algum entendimento inicial sobre o conceito de informações pessoais e o que deve ser mantido em sigilo.
- **Alguém já te pediu para dizer seu nome ou onde você mora enquanto jogava ou usava um aplicativo? O que você fez?** Objetivo: Entender como as crianças reagem em situações práticas de compartilhamento de informações e se já vivenciaram cenários que envolvem riscos online.

Material necessário:

- Cartões ou fichas.
- Imagens de dispositivos (celular, tablet, computador).
- Cartões com exemplos de informações pessoais (nome, endereço, idade, escola).
- Cartões com exemplos de cenários onde essas informações poderiam ser solicitadas (um jogo online, uma rede social, uma mensagem de texto).

Atividade:

1. **Introdução:** Explique às crianças que nem todas as pessoas na internet são confiáveis e que é importante manter certas informações em segredo para se proteger. Faça isso usando uma linguagem simples e exemplos do cotidiano das crianças.

2. **Apresentação dos cartões:** Mostre os cartões com informações pessoais e cenários. Discuta com as crianças quais informações são pessoais e por que é importante não compartilhá-las com estranhos.

3. **O jogo em si:**

   (a) Fase 1: Divida a turma em pequenos grupos. Cada grupo recebe um conjunto de cartões com informações pessoais e cenários. O objetivo é que, para cada cenário apresentado, as crianças decidam se "podem ou não podem"compartilhar as informações pessoais e por quê.

   (b) Fase 2: Depois que todos os grupos tiverem discutido, cada grupo apresenta suas decisões para a turma. O professor pode guiar a discussão, reforçando as boas práticas e corrigindo equívocos.

Reflexão em Grupo: Após o jogo, converse com as crianças sobre como se sentiram ao tomar decisões sobre o que compartilhar ou não. Reforce a importância de falar com um adulto de confiança se tiverem dúvidas sobre segurança online.

- O que você aprendeu sobre proteger suas informações pessoais?
- Por que é importante não compartilhar seu nome, endereço e outras informações pessoais com estranhos?
- Qual foi a parte mais divertida do jogo e por quê?
- Como você pode usar o que aprendeu na sua vida diária?

Material Didático Complementar:

- **Folheto de Dicas:** Crie um folheto simples com dicas de segurança online, como "Nunca diga seu nome completo a estranhos na internet"e "Peça ajuda a um adulto se alguém pedir informações pessoais". Este folheto pode ser enviado para casa para envolver também os pais no processo de aprendizado.
- **História em Quadrinhos:** Desenvolva uma história em quadrinhos simples onde um personagem enfrenta situações de risco online e toma decisões seguras. As crianças podem colorir e levar para casa.

5.3.2 Justificativa teórica

A atividade proposta se alinha diretamente aos princípios da aprendizagem significativa, conforme desenvolvida por David Ausubel [56]. Segundo essa teoria, a aprendizagem ocorre de maneira mais eficaz quando os novos conhecimentos se relacionam de maneira substancial e não arbitrária com o que o aluno já sabe. Na atividade, as crianças partem de conhecimentos prévios sobre o uso de dispositivos digitais no seu cotidiano, como o celular ou o tablet, e relacionam essas experiências com o novo aprendizado sobre segurança de dados. Isso gera uma ponte cognitiva que facilita a retenção e aplicação do conhecimento em contextos reais.

Além disso, o jogo e a reflexão posterior criam um ambiente de aprendizagem ativa, um princípio defendido por Jean Piaget e apoiado por John Dewey [59], onde o aluno é colocado no centro do processo de aprendizagem, não apenas recebendo informações, mas tomando decisões e refletindo sobre suas ações. Essa abordagem permite que as crianças experimentem situações nas quais devem tomar decisões sobre compartilhar ou não informações, promovendo uma aprendizagem por descoberta [60]. Ao tomar decisões durante o jogo, as crianças envolvem-se ativamente no processo, promovendo o engajamento cognitivo e fortalecendo o entendimento sobre os riscos relacionados ao compartilhamento de dados pessoais.

O conceito de aprendizagem colaborativa também é promovido na fase de discussão em grupo. Quando as crianças compartilham suas decisões e discutem com os colegas, elas têm a oportunidade de ouvir diferentes perspectivas e refletir criticamente sobre as suas próprias escolhas, o que favorece o desenvolvimento de habilidades sociais e de cooperação. A pedagogia de Paulo Freire [61], ao enfatizar a importância do diálogo na educação, corrobora essa prática. Para Freire, o processo educativo deve ser dialógico e democrático, o que nesta atividade é alcançado quando as crianças têm espaço para refletir coletivamente sobre suas ações e aprender com os erros e acertos dos colegas.

5.3.3 Conceitos Trabalhados

A atividade "Jogo Pode ou Não Pode?"explora diversos conceitos importantes para o desenvolvimento das competências digitais das crianças. Entre os principais conceitos estão:

Privacidade Digital: O jogo ajuda as crianças a entenderem que certas informações, como nome, idade e endereço, são privadas e devem ser protegidas, conforme recomendado em diversas políticas de segurança digital [28].

Segurança Online: As crianças são introduzidas a noções básicas de segurança digital, como a importância de não compartilhar informações pessoais com desconhecidos

online. A UNESCO [4] destaca a necessidade de conscientizar os jovens sobre a segurança online desde cedo, permitindo que eles naveguem de forma segura e responsável no ambiente digital.

Tomada de Decisão Crítica: Ao decidir em quais situações podem ou não compartilhar informações, as crianças desenvolvem a capacidade de refletir sobre os riscos, uma competência que será essencial à medida que envelhecem e se tornam usuários mais ativos da tecnologia.

5.4 2º Ano

Habilidade: Reconhecer os cuidados com a segurança no uso de dispositivos computacionais.

Explicação da habilidade: Nesta habilidade temos a perspectiva de trazer um panorama sobre os cuidados com a segurança ao usar dispositivos como celular, tablets, computadores dentre outros (roubo de dados em dispositivos físicos, rastro de dados online quando da utilização de jogos por exemplo etc.).

5.4.1 Atividade: Missão Agente Cibernético: Proteja seus Dispositivos!

Objetivo: Ensinar os alunos a reconhecerem os cuidados necessários para garantir a segurança ao usar dispositivos como celulares, tablets, e computadores, além de compreenderem os riscos associados, como roubo de dados e rastros online.

Diagnóstico inicial:

- **Quais dispositivos você costuma usar em casa ou na escola (celular, tablet, computador)? O que você mais gosta de fazer nesses dispositivos?** Objetivo: Entender quais dispositivos os alunos já utilizam e como eles interagem com esses dispositivos, o que ajudará a adaptar a atividade às experiências cotidianas deles.
- **Você já ouviu falar sobre proteger seu celular ou tablet? O que você faz para mantê-los seguros?** Objetivo: Verificar se os alunos têm algum entendimento prévio sobre a segurança dos dispositivos e práticas como usar senhas ou não clicar em links desconhecidos.
- **Você já recebeu alguma mensagem estranha ou de alguém que você não conhece enquanto jogava ou usava um aplicativo? O que você fez?** Objetivo: Avaliar como os alunos lidam com situações reais de risco, como o contato

com estranhos, para entender sua reação e ponto de partida no que diz respeito à segurança online.

Material necessário:

- Cartolina ou papel cartão para criar cartões de missão que descrevam diferentes cenários e tarefas.
- Papel colorido ou adesivos para criar recortes de informações pessoais como nome, endereço, senha, etc.
- Cadernetas pequenas ou blocos de notas onde os alunos podem registrar suas missões e aprendizados.
- Papel, lápis, canetas, cola, tesouras, e outros materiais de arte para criar desenhos e montagens.

Atividade: Os alunos assumem o papel de "Agentes Cibernéticos"e recebem diferentes "missões"para completar em sala de aula, cada uma focada em um aspecto da segurança no uso de dispositivos computacionais.

Missões Detalhadas:

1. **Missão 1: Proteja o Tesouro Digital**
    - **Tarefa:** Os alunos devem identificar quais informações pessoais são "tesouros"que precisam ser protegidos (como senhas, nome, endereço, etc.).
    - **Exemplo:** Eles recebem um cartão com um desenho de um cofre e recortes de diferentes tipos de informações (nome, endereço, senha, idade, etc.). Eles devem colar no cofre apenas as informações que consideram valiosas e que não devem ser compartilhadas.
2. **Missão 2: Desconfie do Estranho**
    - **Tarefa:** Simular um jogo onde os alunos recebem mensagens (previamente preparadas pelo professor) em que personagens pedem informações pessoais ou oferecem algo tentador (como moedas em um jogo). Eles devem decidir se compartilham a informação ou ignoram a mensagem.
    - **Exemplo:** "Oi! Eu sou o Marco e estou jogando o mesmo jogo que você. Qual é o seu nome e onde você mora? Eu posso te ajudar a ganhar mais pontos!”
3. **Missão 3: Dispositivos à Prova de Perigos**

- **Tarefa:** Os alunos discutem em grupos como manter seus dispositivos seguros. Cada grupo deve listar ações como criar senhas fortes, não abrir links de fontes desconhecidas, e manter os dispositivos em locais seguros.
- **Exemplo:** Fazer um desenho do seu dispositivo (tablet, celular, computador) com um "escudo"ao redor dele, e escrever dentro do escudo as ações de segurança que eles aprenderam.

4. **Missão 4: Rastros Invisíveis**

    - **Tarefa:** Ensinar sobre os rastros digitais que deixamos ao navegar na internet. Os alunos observam exemplos de como atividades online podem ser rastreadas (como histórico de navegação).
    - **Exemplo:** Mostrar um "mapa"digital do caminho que um personagem faz ao usar diferentes sites e aplicativos, e destacar os rastros deixados (como buscas, cliques, etc.). Eles então discutem como poderiam "apagar"esses rastros ou minimizá-los.

Reflexão em Grupo: Após a realização da atividade, organize uma roda de conversa com os alunos para refletir sobre o que aprenderam. Perguntas orientadoras podem incluir:

- O que você aprendeu sobre como proteger seus dispositivos?
- Qual missão você achou mais interessante e por quê?
- Como você pode aplicar o que aprendeu na sua vida cotidiana?
- Quais são os cuidados mais importantes ao usar um dispositivo eletrônico?

Material Didático Complementar:

- **Caderneta do Agente Cibernético:** Uma pequena caderneta onde os alunos podem anotar as missões cumpridas, reflexões sobre segurança digital, e dicas importantes. Eles podem levar para casa e compartilhar com a família, incentivando a continuidade do aprendizado.
- **Pôster "Dicas de Segurança para Toda Família":** Um pôster ilustrado com as principais dicas de segurança aprendidas em sala, para ser levado para casa. Ele pode ser pendurado em algum local visível, como a cozinha ou a sala, para lembrar a todos da importância de proteger seus dados.
- **Cartão de Identificação do Agente Cibernético:** Um cartão personalizado para cada aluno, com o título de "Agente Cibernético", incentivando-os a se sentirem responsáveis pela sua segurança digital e a dos outros.

5.4.2 Justificativa Teórica

A atividade se fundamenta na teoria da aprendizagem significativa de David Ausubel [56], que afirma que o novo conhecimento é mais efetivamente assimilado quando pode ser relacionado aos conhecimentos prévios dos alunos. As crianças, no segundo ano, já possuem familiaridade com dispositivos como celulares e tablets, e o uso dessa experiência cotidiana como ponto de partida facilita a compreensão dos conceitos abstratos de segurança digital. As “missões” da atividade são projetadas para que as crianças façam associações diretas entre suas ações diárias e os riscos que podem enfrentar no ambiente digital, promovendo a construção de um aprendizado sólido e aplicável em suas vidas.

Além disso, a pedagogia do fazer, inspirada por John Dewey [59], enfatiza a importância da aprendizagem ativa e experiencial, onde as crianças participam ativamente da construção do conhecimento. No caso da atividade "Missão Agente Cibernético", as crianças assumem o papel de agentes que protegem seus dispositivos e dados. Ao engajarem-se ativamente na solução de problemas apresentados nas diferentes missões, os alunos internalizam conceitos de segurança digital de maneira prática e lúdica, consolidando o aprendizado por meio da ação. Cada missão oferece oportunidades para que os alunos se envolvam cognitivamente com o conteúdo, desenvolvendo tanto suas habilidades tecnológicas quanto seu pensamento crítico.

O uso de narrativas e jogos no processo educativo é amplamente defendido pela teoria do construtivismo, como formulado por Jean Piaget. Piaget [57] destacou que o aprendizado acontece quando os alunos estão ativamente envolvidos na descoberta de informações e na resolução de problemas. Ao participar de missões com desafios relacionados à segurança digital, os alunos experimentam situações semelhantes às que encontrarão em suas vidas digitais. Além disso, a metáfora de agentes cibernéticos os coloca em um contexto de aventura e responsabilidade, o que os motiva a aprender e os faz internalizar os conceitos de segurança digital de forma engajante e significativa.

A atividade também segue os princípios da educação para a cidadania digital, conforme discutido por autores como Ribble [17], que define cidadania digital como a prática de utilizar a tecnologia de maneira ética, crítica e responsável. Ao proteger suas informações e entender os riscos associados ao uso de dispositivos digitais, os alunos começam a desenvolver uma consciência crítica e ética em relação ao ambiente digital, algo crucial no contexto educacional contemporâneo.

5.4.3 Conceitos Trabalhados

Na atividade "Missão Agente Cibernético: Proteja seus Dispositivos!", diversos conceitos fundamentais para o desenvolvimento da competência digital e da segurança online são

trabalhados:

Proteção de Informações Pessoais: As crianças aprendem a identificar quais informações pessoais são valiosas e devem ser protegidas, como senhas, endereço e nome, conforme destacado por Greenleaf [28] em sua pesquisa sobre políticas de segurança digital.

Segurança de Dispositivos: A missão 3 ("Dispositivos à Prova de Perigos") ensina a importância de manter dispositivos seguros, com ênfase em práticas como o uso de senhas fortes e a não abertura de links desconhecidos, conforme as recomendações da UNESCO [4] para a promoção da segurança digital em ambientes escolares.

Rastros Digitais e Privacidade: A missão 4 ("Rastros Invisíveis") traz o conceito de rastros digitais, mostrando aos alunos como as atividades online podem ser monitoradas e como proteger a própria privacidade ao navegar na internet, uma questão central no debate sobre privacidade e cidadania digital.

Tomada de Decisão Consciente: Ao realizar escolhas sobre o que compartilhar ou como proteger seus dispositivos, as crianças começam a desenvolver a capacidade de tomada de decisão consciente e crítica, essencial para a segurança online, como discutido por Sampaio e Fernandes [29].

5.5 3º Ano

Habilidade: Reconhecer o potencial impacto do compartilhamento de informações pessoais ou de seus pares em meio digital.

Explicação da habilidade: A proposta nesta habilidade é que o aluno possa identificar alguns dos principais impactos de compartilhar informações pessoais com colegas ou pessoas em meio digital, como por exemplo endereço, nomes das pessoas da família, onde estuda, onde mora. Essas informações podem ser utilizadas por pessoas de forma mal-intencionadas, quando os alunos trocam informações online por celular, computador ou até mesmo quando estão jogando na internet.

5.5.1 Atividade: "O que acontece com as suas informações no mundo digital?"

Objetivo: Ensinar os alunos a reconhecerem os riscos e as consequências do compartilhamento de informações pessoais em meios digitais, como redes sociais, jogos online e aplicativos.

Diagnóstico inicial:

- **Você já compartilhou informações sobre você, como seu nome ou endereço, enquanto jogava ou usava aplicativos? Por que você fez isso?** Objetivo: Entender se os alunos já tiveram experiências de compartilhar informações pessoais online e qual é a compreensão deles sobre as implicações de tais ações.
- **Você acha que é perigoso compartilhar informações como seu endereço ou o nome da sua família na internet? Por que você pensa assim?** Objetivo: Avaliar se os alunos têm uma noção básica dos riscos associados ao compartilhamento de informações pessoais e entender como eles interpretam esses riscos.
- **Quando você vê um site ou aplicativo que pede informações pessoais, como nome ou idade, o que você faz? Você já pediu ajuda a um adulto?** Objetivo: Verificar como os alunos reagem a solicitações de informações online e se eles costumam pedir ajuda ou orientação antes de compartilhar.

Material Necessário:

- Cartolina ou papel grande.
- Marcadores, canetas coloridas, lápis de cor.
- Imagens de dispositivos computacionais (celular, tablet, computador) impressas ou desenhadas.
- Balões de fala recortados de papel para escrever as dicas de segurança.

Atividade:

1. **Introdução:** Comece a atividade explicando o que são informações pessoais (nome, endereço, fotos, etc.) e por que elas são valiosas. Discuta brevemente como essas informações podem ser usadas por outras pessoas na internet, destacando o conceito de rastros digitais.
2. **Estudo de Caso: "A História do Pedro":** Crie uma história fictícia sobre um personagem chamado Pedro, que compartilha suas informações pessoais em um jogo online. Por exemplo:
    - Pedro coloca seu nome completo no perfil do jogo.
    - Ele compartilha fotos de sua casa com amigos que conheceu no jogo.
    - Um estranho no jogo pede a Pedro informações sobre onde ele mora, e Pedro compartilha essa informação.

    A história deve mostrar as consequências dessas ações, como receber mensagens de pessoas desconhecidas ou ter suas informações usadas para fins indesejados.

3. **Discussão em Grupo:** Após a história, divida a turma em pequenos grupos e peça para eles discutirem o que Pedro poderia ter feito de diferente. Cada grupo pode apresentar uma solução para proteger melhor as informações de Pedro.

4. **Painel "Proteja Suas Informações!":** Peça aos alunos para criar um painel com imagens de dispositivos computacionais (celular, tablet, computador) e desenhar ou escrever em balões as informações pessoais que nunca devem ser compartilhadas. Este painel pode incluir mensagens como "Não compartilhe sua localização" ou "Use um apelido em jogos online".

5. **Tarefa para Casa: "Minha Política de Privacidade":** Os alunos devem criar, com a ajuda dos pais, uma "política de privacidade" para seu uso pessoal da internet. Isso incluiria regras sobre o que podem ou não compartilhar online. Eles podem trazer essa política para a próxima aula e compartilhar com a turma, incentivando a responsabilidade coletiva.

Reflexão em Grupo: Ao final, convide os alunos a refletir sobre as lições aprendidas durante a atividade e reforçar a importância da segurança no uso de tecnologias computacionais. As perguntas podem envolver:

- O que aprendemos hoje sobre o compartilhamento de informações online?
- Por que é importante pensar antes de compartilhar algo na internet?
- Como podemos ajudar nossos amigos e familiares a manterem suas informações seguras?

Material Didático Complementar:

- **Cartilha "Cuidando das Suas Informações Online":** Uma cartilha colorida que explique, de forma simples, as principais dicas de segurança online para crianças. Esta cartilha pode ser levada para casa, onde os alunos podem revisá-la com seus pais.
- **Jogo de Cartas "Segurança Online":** Um jogo de cartas onde cada carta tem uma situação online (ex.: "Alguém te pede para enviar uma foto", "Você quer postar onde está no momento") e as crianças precisam decidir se é seguro ou não. As cartas podem ser usadas em sala de aula para reforçar o aprendizado.
- **Certificado de "Guardião da Informação":** Ao final da atividade, cada aluno recebe um certificado de "Guardião da Informação", reconhecendo que agora eles entendem a importância de proteger suas informações pessoais online.

5.5.2 Justificativa Teórica

A teoria da aprendizagem significativa de David Ausubel [56] sustenta que novos conhecimentos são assimilados de forma mais eficaz quando podem ser conectados a conceitos já existentes na estrutura cognitiva dos alunos. Nesta atividade, as crianças, que já possuem alguma familiaridade com a utilização de dispositivos computacionais e com interações online, como jogos e redes sociais, são incentivadas a refletir sobre como suas ações digitais podem gerar consequências. Ao conectar as experiências reais dos alunos com novos conhecimentos sobre segurança digital, a atividade promove uma aprendizagem contextualizada, que permite que os alunos internalizem os riscos do ambiente digital de maneira mais profunda e duradoura.

Além disso, o uso de um estudo de caso — "A História do Pedro" — segue os princípios da aprendizagem por descoberta, de Bruner,[60] e do construtivismo, conforme desenvolvido por Jean Piaget [57]. Bruner e Piaget acreditavam que os alunos aprendem melhor quando participam ativamente da construção de seu conhecimento, ao invés de serem apenas receptores passivos. Ao analisar o comportamento de Pedro e discutir em grupo o que ele poderia ter feito de forma diferente, os alunos se tornam participantes ativos no processo de aprendizagem, aplicando habilidades críticas para resolver problemas de segurança online, ao invés de apenas memorizar regras.

Cidadania Digital e Ética

O conceito de cidadania digital proposto por Ribble [17] está no cerne desta atividade. Ribble define cidadania digital como o uso responsável, ético e seguro da tecnologia. A atividade aborda esse conceito ao ensinar os alunos sobre os riscos de compartilhar informações pessoais online e a importância de adotar práticas de proteção de dados. Segundo Ribble, o desenvolvimento dessas habilidades é fundamental para que os alunos naveguem no mundo digital de forma segura e ética, entendendo que suas ações online têm consequências.

O painel "Proteja Suas Informações" e a tarefa para casa "Minha Política de Privacidade" proporcionam uma oportunidade para que os alunos se apropriem dessas práticas de cidadania digital, desenvolvendo a consciência de que são responsáveis por proteger suas informações e as de seus familiares. O envolvimento dos pais na tarefa para casa também promove a educação colaborativa, conforme defendida por Paulo Freire [61], que destaca a importância do diálogo e da participação ativa de todos os envolvidos no processo de aprendizagem.

Reflexão Crítica e Ética Digital

A atividade incentiva os alunos a desenvolverem pensamento crítico em relação ao uso de dispositivos digitais, ao discutir o que Pedro poderia ter feito de forma diferente e ao criar suas próprias "políticas de privacidade". Isso está alinhado com as recomendações da UNESCO [4], que afirma que a educação para a cidadania digital deve ir além de ensinar habilidades técnicas, incorporando reflexões éticas sobre as responsabilidades e os direitos dos usuários de tecnologias digitais. A atividade promove essa reflexão ao destacar que as informações compartilhadas online podem ser usadas de maneiras prejudiciais, e ao pedir que os alunos pensem nas consequências de suas próprias ações digitais.

5.5.3 Conceitos Trabalhados

A atividade "O que acontece com as suas informações no mundo digital?"trabalha diversos conceitos fundamentais para a formação de uma cidadania digital consciente e responsável:

Rastros Digitais: Os alunos aprendem sobre os rastros que deixam ao compartilhar informações online e os riscos associados a essas ações, um conceito essencial para a privacidade digital [28].

Tomada de Decisão Crítica: A atividade incentiva os alunos a refletirem criticamente antes de compartilhar informações, desenvolvendo a habilidade de tomar decisões responsáveis no ambiente digital.

Consequências do Compartilhamento Online: A história de Pedro ilustra os perigos do compartilhamento de informações pessoais, reforçando a ideia de que a internet não é um espaço totalmente seguro e que é necessário agir com cautela.

Responsabilidade Coletiva: A atividade de criar uma "política de privacidade" com a ajuda dos pais promove a responsabilidade compartilhada entre alunos, professores e pais, conforme proposto por autores como Sampaio e Fernandes [29].

5.6 4o ano - I

Habilidade: Demonstrar postura ética nas atividades de coleta, transferência, guarda e uso de dados.

Explicação da habilidade: Propõe-se que o aluno reflita sobre aspectos éticos relacionados a manipulação de dados, como por exemplo quando assiste e faz download, compartilha uma imagem, dentre outros.

5.6.1 Atividade: “Os Guardiões da Ética Digital”

Objetivo: Ensinar os alunos a reconhecer e praticar uma postura ética ao manipular dados digitais, como assistir, fazer download e compartilhar conteúdos, refletindo sobre as responsabilidades envolvidas em cada ação.

Diagnóstico inicial:

- **Você já compartilhou informações sobre você, como seu nome ou endereço, enquanto jogava ou usava aplicativos? Por que você fez isso?** Objetivo: Avaliar a compreensão dos alunos sobre o conceito básico de ética digital e ver se eles conseguem relacionar o comportamento ético no mundo real com o comportamento no mundo digital.
- **Você já parou para pensar se é certo compartilhar uma foto ou vídeo que encontrou na internet com seus amigos? O que faz você decidir se vai compartilhar ou não?** Objetivo: Identificar se os alunos já refletem sobre as consequências éticas de compartilhar conteúdo digital, explorando se eles têm noção sobre direitos autorais e privacidade.
- **Se você visse um vídeo ou foto embaraçosa de alguém, você acha que seria certo compartilhar com seus colegas? Por quê?** Objetivo: Entender a sensibilidade dos alunos em relação a questões de consentimento e o impacto emocional e ético de suas ações no ambiente digital.

Material Necessário:

- Cartolina ou papel cartão para criar cartões com diferentes cenários éticos.
- Marcadores, canetas coloridas, lápis de cor.
- Papel grande, cartolina ou papelão.

Atividade:

1. **Introdução:** Comece explicando o conceito de ética, destacando como ele se aplica ao mundo digital. Use exemplos simples, como o que significa ser honesto e respeitar os outros online. Apresente a ideia de que, como "Guardiões da Ética Digital", os alunos têm a responsabilidade de cuidar bem das informações e imagens que encontram na internet.
2. **Explorando Cenários Éticos:** Divida a turma em pequenos grupos e distribua cartões de cenários éticos relacionados ao uso de dados digitais. Cada grupo discutirá como agiria em cada situação e qual seria a decisão mais ética. Exemplos de cenários:

- "Você encontra uma imagem engraçada online e quer compartilhar com seus amigos, mas a imagem pertence a alguém que você não conhece."
- "Alguém envia para você um vídeo que mostra outra pessoa em uma situação embaraçosa. Você deve compartilhar?"
- "Você fez o download de um filme ou música, mas não tem certeza se é legal ou não."

3. **Discussão e Decisão:** Cada grupo apresenta suas discussões e decisões para a turma. O professor guia a discussão, destacando as decisões éticas e os riscos associados a cada cenário. Durante essa parte, o professor pode introduzir termos como "direitos autorais", "consentimento", e "pirataria digital"de forma acessível para as crianças, explicando por que é importante respeitar essas regras.
4. **Códigos de Ética Digital:** Cada grupo cria um "Código de Ética Digital"com regras e dicas sobre como agir de maneira ética online. Eles podem incluir orientações sobre o uso correto de imagens, vídeos, e como proteger as informações dos outros. Os alunos decoram e ilustram seus códigos, que podem ser exibidos na sala de aula como lembrete das boas práticas online.

Reflexão em Grupo: Finalize a atividade reforçando que a ética digital é uma parte importante de ser um bom cidadão online, faça pergunta como:

- O que significa agir de forma ética na internet?
- Por que é importante pedir permissão antes de compartilhar algo que não é seu?
- Como podemos ser "Guardiões da Ética Digital"no dia a dia?

Material Didático Complementar:

- **História em Quadrinhos:** "A Aventura dos Guardiões da Ética Digital": Uma história em quadrinhos curta que conta a história de personagens que enfrentam dilemas éticos online e tomam decisões corretas. A história pode ser divertida e educativa, reforçando os conceitos de ética digital de uma maneira que ressoe com os alunos. Eles podem ler em casa e até compartilhar com irmãos ou amigos.
- **Pôster "Regras de Ouro da Ética Digital":** Um pôster para colorir com as "Regras de Ouro"da ética digital. O pôster pode ser ilustrado com personagens ou símbolos relacionados à segurança online e ética. Os alunos podem colorir o pôster em casa e pendurá-lo em seu quarto ou em um espaço comum, como um lembrete constante das boas práticas online.

5.7 4o ano - II

Habilidade: Reconhecer a importância de verificar a confiabilidade das fontes de informações obtidas na Internet.

Explicação da habilidade: Nesta habilidade espera-se que os alunos possam reconhecer que, ao se obter informações na Internet, é preciso identificar as suas fontes e se elas são seguras e a informação é confiável.

5.7.1 Atividade: "Detetives da Informação"

Objetivo: Capacitar os alunos a identificar e avaliar a confiabilidade das fontes de informações online, desenvolvendo habilidades críticas para discernir entre fontes seguras e não seguras.

Diagnóstico inicial:

- **Quando você busca algo na internet, como você decide se uma informação ou site é confiável? Você acha que todas as informações online são verdadeiras? Por quê?** Objetivo: Avaliar se os alunos já possuem uma noção inicial sobre a verificação da veracidade e confiabilidade das fontes de informação na internet.
- **Você já se deparou com notícias ou informações que pareciam falsas ou duvidosas? O que te fez pensar que elas não eram verdadeiras?** Objetivo: Investigar se os alunos têm experiência ou reflexão sobre fake news e informações não confiáveis e se eles já utilizam algum critério de análise para desconfiar das fontes.
- **Como você acha que podemos saber se uma notícia ou um site na internet está nos dando uma informação verdadeira? Que pistas podemos procurar?** Objetivo: Explorar o conhecimento pré-existente dos alunos sobre os critérios de confiabilidade, como verificar autoria, data de publicação, fontes citadas, etc.

Material Necessário:

- Cartões de Informação: Exemplos de diferentes tipos de fontes online (sites de notícias, blogs, redes sociais, vídeos, etc.).
- Cartões de Características de Fontes Confiáveis e Não Confiáveis: Características como autoria clara, data de publicação, domínio do site, entre outros.
- Quadro branco ou cartolina: Para criar um mural interativo.
- Marcadores coloridos: Para destacar as categorias no mural.

- Computadores ou tablets: Para pesquisa online (opcional, se disponível).
- Lupa de Detetive (opcional): Uma lupa de brinquedo ou símbolo que os alunos possam usar para “investigar” as fontes.

Atividade:

1. **Introdução:** Explique o conceito de confiabilidade das fontes, enfatizando por que é importante verificar a veracidade das informações na internet. Use um exemplo simples, como a diferença entre uma notícia em um site reconhecido e um boato em redes sociais.
2. **Divisão em Grupos:** Forme pequenos grupos de 3 a 4 alunos. Entregue a cada grupo um conjunto de cartões de informação e cartões de características.
3. **Exploração dos Cartões:** Os grupos devem associar cada cartão de informação a características de fontes confiáveis ou não confiáveis. Por exemplo, se o cartão de informação descreve um blog desconhecido sem data de publicação, o grupo deve associá-lo a características como “sem autoria clara” e “não atualizado”. Incentive os alunos a justificar suas escolhas, promovendo o pensamento crítico.
4. **Discussão e Mural:** Cada grupo apresenta suas associações à turma, explicando as razões por trás de suas escolhas. Crie um mural com duas colunas: "Fontes Confiáveis"e "Fontes Não Confiáveis". Organize os cartões de acordo com as discussões. Os alunos podem adicionar comentários ou observações ao lado dos cartões para enriquecer o mural.
5. **Atividade de Pesquisa:** Se possível, permita que os alunos usem computadores ou tablets para pesquisar informações online. Eles devem procurar um tópico específico em diferentes fontes e identificar quais são confiáveis e quais não são, justificando suas escolhas. Incentive-os a usar o checklist de verificação de fontes para guiar sua pesquisa.
6. **Criação do “Guia de Detetives da Informação":** Em grupos, os alunos criam um pequeno guia visual, onde resumem as características das fontes confiáveis e dão exemplos. Esse guia pode ser feito em formato de mini-livro ou folheto para ser compartilhado com a turma e levado para casa.

Reflexão em Grupo: Perguntas para direcionar a reflexão em grupo no final da atividade:

- Quais foram as dicas mais úteis que vocês aprenderam para verificar se uma fonte é confiável?

- Como vocês podem usar essas dicas no dia a dia ao pesquisar na internet?

Material Didático Complementar:

- **Guia de Fontes Confiáveis e Não Confiáveis:** Um guia ilustrado que resume as principais características das fontes confiáveis e não confiáveis, com exemplos práticos. Os alunos podem levá-lo para casa e usá-lo como referência.
- **Jogo de Cartas "Desvendando Fontes":** Um jogo de cartas em que os alunos devem combinar fontes com características confiáveis e não confiáveis, reforçando o aprendizado de forma divertida.
- **Checklist de Verificação de Fontes:** Um checklist simples que os alunos podem usar sempre que fizerem uma pesquisa online. Inclui perguntas como "Quem é o autor?", "Qual é a data de publicação?", "O site é conhecido e respeitado?".
- **Certificado de "Detetive da Informação":** Ao final da atividade, cada aluno recebe um certificado de "Detetive da Informação", reconhecendo que agora eles entendem a importância de ser um bom detetive da informação.

5.8 Justificativa Teórica para as atividades do 4º Ano

No contexto educacional do 4º ano do ensino fundamental, as atividades "Os Guardiões da Ética Digital" e "Detetives da Informação" são essenciais para promover habilidades relacionadas à cidadania digital e ao pensamento crítico. Ambas as atividades são fundamentadas em teorias de aprendizagem significativa [56] e no desenvolvimento moral [62], além de abordarem a ética digital e a alfabetização midiática como pilares para a formação de cidadãos conscientes e responsáveis no ambiente digital [17], [53].

5.8.1 Ética Digital e Alfabetização Midiática

A ética digital é um componente central da cidadania no século XXI, englobando o comportamento responsável no uso de tecnologias e a manipulação de dados e informações. Ao propor a atividade "Os Guardiões da Ética Digital", os alunos são convidados a refletir sobre questões éticas como o respeito aos direitos autorais, a proteção da privacidade e a responsabilidade de compartilhar conteúdo de forma consciente. Essa atividade é estruturada para desenvolver a consciência ética dos alunos, com base na teoria do desenvolvimento moral de Kohlberg [62], que aponta que as crianças dessa faixa etária (9-10 anos) começam a compreender as regras morais e suas implicações sociais.

A atividade também está alinhada com a perspectiva de Freire [61], que argumenta que a educação deve capacitar os indivíduos para a reflexão crítica sobre suas ações no

mundo. Nesse sentido, a criação de um Código de Ética Digital pelos alunos, ao final da atividade, promove a autonomia e a participação ativa no processo de construção de normas de comportamento digital, refletindo um princípio central da pedagogia crítica de Freire.

Por outro lado, a atividade "Detetives da Informação"aborda a alfabetização midiática, que, segundo Buckingham [53], é essencial para o desenvolvimento de uma cidadania ativa e crítica no contexto digital. A habilidade de distinguir entre fontes confiáveis e não confiáveis é crucial para que os alunos naveguem com segurança na internet e desenvolvam uma compreensão mais ampla sobre as informações que consomem. Conforme Ribble [17], essa competência é parte integrante da cidadania digital, que envolve o uso crítico e ético das tecnologias digitais.

5.8.2 Aprendizagem Significativa e Desenvolvimento Cognitivo

Ambas as atividades são embasadas na teoria da aprendizagem significativa de Ausubel [56], que enfatiza que o aprendizado é mais eficaz quando os novos conhecimentos são ancorados em conceitos já existentes. No caso de "Os Guardiões da Ética Digital", os alunos já possuem noções básicas de certo e errado, e a atividade amplia esses conceitos para o ambiente digital. A interação social durante as discussões em grupo também é um elemento chave no desenvolvimento das habilidades cognitivas e morais, conforme descrito por Vygotsky [58], que destaca a importância do aprendizado colaborativo.

Na atividade "Detetives da Informação", os alunos constroem conhecimento ao analisar diferentes fontes de informação, associando características de confiabilidade a exemplos práticos. A utilização de cenários concretos e o uso de recursos visuais, como cartões e murais, facilitam o entendimento de conceitos abstratos, como a veracidade das informações online. A criação do Guia de Detetives da Informação ao final da atividade reforça a importância da reflexão crítica e do compartilhamento de conhecimento, transformando os alunos em agentes ativos de sua própria aprendizagem.

5.8.3 Conceitos Trabalhados nas Atividades

Ética Digital: Envolve a prática de comportamentos responsáveis e respeitosos no uso de dados e informações digitais, como o respeito aos direitos autorais, a proteção da privacidade e a não disseminação de conteúdos não autorizados.

Cidadania Digital: Refere-se ao uso consciente e ético das tecnologias digitais, promovendo a segurança online e o respeito aos direitos dos outros. A atividade "Detetives da Informação"aborda esse conceito ao ensinar os alunos a verificar a confiabilidade das informações que encontram online.

Responsabilidade Social: Ambos os exercícios destacam a importância de agir de forma responsável no ambiente digital, considerando o impacto das ações individuais sobre a comunidade. A criação de um código de ética e a discussão sobre a disseminação de informações são exemplos claros dessa abordagem.

Alfabetização Midiática: A capacidade de avaliar e analisar criticamente diferentes fontes de informação, distinguindo entre conteúdos confiáveis e não confiáveis. Esse conceito é trabalhado na atividade "Detetives da Informação", que ensina os alunos a identificarem características de fontes seguras e não seguras.

Pensamento Crítico: As atividades incentivam a reflexão crítica dos alunos sobre as informações que consomem e compartilham online, desenvolvendo habilidades para questionar a veracidade e a confiabilidade dessas informações.

Direitos Autorais: O conceito de respeitar a propriedade intelectual e os direitos de criação de conteúdo digital é central para a atividade "Os Guardiões da Ética Digital", que ensina aos alunos que compartilhar conteúdos de terceiros sem permissão pode ser prejudicial e ilegal.

5.9 5º ano - I

Habilidade: Acessar as informações na Internet de forma crítica para distinguir os conteúdos confiáveis de não confiáveis.

Explicação da habilidade: Nesta habilidade é importante que os alunos possam refletir e acessar informações em buscas na Internet criticamente, identificando características de conteúdos prejudiciais, informações confiáveis, notícias falsas.

5.9.1 Atividade: "Caça às Fakes: Desmascarando Notícias Falsas"

Objetivo: Capacitar os alunos a identificar e desmascarar notícias falsas, desenvolvendo habilidades críticas para avaliar a veracidade das informações que encontram na internet.

Diagnóstico inicial:

- **Quando você vê uma notícia na internet ou nas redes sociais, como você decide se ela é verdadeira ou não? Quais coisas você olha para saber se pode confiar na informação?** Objetivo: Identificar se os alunos já possuem noção de como avaliar a veracidade de uma notícia ou se confiam cegamente em qualquer fonte de informação.
- **Você já ouviu falar de notícias falsas ou "fake news"? Como você acha que essas notícias se espalham?** Objetivo: Explorar o conhecimento prévio dos

alunos sobre o conceito de "fake news"e verificar se eles têm alguma familiaridade com o impacto negativo de compartilhar informações falsas.

- **Quais sinais ou características você acha que podem indicar se uma notícia é falsa ou verdadeira?** Objetivo: Avaliar o conhecimento dos alunos sobre as características que podem ajudar a distinguir notícias verdadeiras de falsas, como a presença de fontes confiáveis, autoria, data de publicação, entre outros.

Material Necessário:

- Cartões de Notícias: Cartões que contêm exemplos de notícias falsas e verdadeiras, incluindo manchetes, trechos de artigos e imagens.
- Cartões de Evidências: Cartões com diferentes tipos de evidências, como links para fontes confiáveis, citações de especialistas, ou indicadores de sensacionalismo.
- Folha de Investigação: Um formulário para que os alunos registrem suas descobertas sobre cada notícia, incluindo perguntas guiadas como “Essa notícia tem fontes confiáveis?”, “Há evidências claras?”, “A linguagem parece sensacionalista?”.
- Computadores ou Tablets: Para pesquisa online e verificação de fatos (opcional).
- Marcadores e cartolinas: Para a apresentação final.

Atividade:

1. **Introdução:** Explicação: Introduza o conceito de fake new e explique como essas notícias podem se espalhar na internet. Discuta as consequências de acreditar e compartilhar informações falsas. Exemplos: Mostre exemplos recentes de notícias falsas que tiveram grande repercussão e explique como foram desmascaradas.
2. **Distribuição e investigação:** Distribuição: Divida os alunos em grupos de 4 a 5 pessoas. Cada grupo recebe um conjunto de "Cartões de Notícias"e "Cartões de Evidências". Investigação: Os grupos devem analisar cada notícia usando os cartões de evidências para decidir se a notícia é verdadeira ou falsa. Eles podem utilizar as “Folhas de Investigação” para registrar suas conclusões. Pesquisa Online (opcional): Se disponível, os alunos podem usar computadores ou tablets para pesquisar mais informações sobre as notícias, verificando fontes e comparando com outras informações disponíveis online.
3. **Apresentação e debate:** Apresentação: Cada grupo apresenta suas descobertas para a turma, explicando por que acreditam que uma notícia é verdadeira ou falsa. Eles devem usar as evidências que encontraram para apoiar suas conclusões. Debate:

Promova um debate saudável, onde os grupos podem questionar as conclusões dos outros, incentivando a troca de ideias e a análise crítica.

4. **Criação do mural “Fakes Desmascaradas":** Mural: Usando cartolinas e marcadores, os alunos criam um mural com as notícias falsas que desmascararam. O mural pode incluir os cartões de evidências que ajudaram a desmascarar cada notícia, criando um guia visual para a sala de aula.

Reflexão em Grupo: Perguntas para direcionar a reflexão em grupo no final da atividade:

- Por que é importante verificar se uma notícia é verdadeira antes de compartilhá-la com outras pessoas?
- Quais sinais você notou que ajudaram a identificar uma notícia como falsa ou verdadeira?
- Como você pode usar o que aprendeu hoje para ajudar seus amigos e familiares a evitar fake news?

Material Didático Complementar:

- **Guia “Como Desmascarar Fake news”:** Um guia ilustrado que resume as principais características das fontes confiáveis e não confiáveis, com exemplos práticos. Os alunos podem levá-lo para casa e usá-lo como referência.
- **Jogo “Fakes & Fatos”:** Um jogo de cartas em que os alunos devem combinar fontes com características confiáveis e não confiáveis, reforçando o aprendizado de forma divertida.
- **Pôster “Dicas para Detectar Fake news”:** Um checklist simples que os alunos podem usar sempre que fizerem uma pesquisa online. Inclui perguntas como “Quem é o autor?”, “Qual é a data de publicação?”, “O site é conhecido e respeitado?”.
- **Certificado de “Caçador de Fakes”:** Ao final da atividade, cada aluno recebe um certificado de “Caçador de fakes”, reconhecendo que agora eles estão aptos a desmascarar notícias falsas.

5.10 5º Ano - II

Habilidade: Usar informações considerando aplicações e limites dos direitos autorais em diferentes mídias digitais.

Explicação da habilidade: O objetivo desta habilidade é que o aluno possa utilizar informações e dados na Internet reconhecendo os direitos autorais, como por exemplo de uma música, um filme, um livro, e os cuidados em seu compartilhamento e uso pessoal.

5.10.1 Atividade: “Exploradores dos Direitos Autorais”

Diagnóstico inicial:

- **Você já ouviu falar sobre direitos autorais? O que você acha que significa "respeitar os direitos autorais"quando usamos músicas, filmes ou livros na internet?** Objetivo: Avaliar o conhecimento básico dos alunos sobre o conceito de direitos autorais e seu entendimento sobre como essas regras se aplicam ao uso de mídias digitais.
- **Você acha que é permitido copiar e compartilhar músicas ou vídeos da internet com seus amigos? Por que sim ou por que não?** Objetivo: Identificar a percepção dos alunos sobre as práticas comuns de compartilhamento online e o quanto estão cientes das implicações legais e éticas desse tipo de ação.
- **Quando você faz um trabalho escolar ou usa uma imagem da internet, o que você faz para mostrar de onde tirou essas informações?** Objetivo: Entender se os alunos têm noção sobre a importância de citar fontes e reconhecer a autoria de conteúdo, mesmo em atividades escolares.

Material Necessário:

- Cartões de Mídia: Cartões com imagens e informações sobre diferentes tipos de mídias digitais, como capas de livros, pôsteres de filmes, álbuns de música e vídeos. Cada cartão deve incluir detalhes sobre os direitos autorais associados ao conteúdo.
- Mapa do Tesouro de Direitos Autorais: Um mapa temático que guia os alunos através de diferentes “ilhas” (etapas) onde precisam resolver desafios relacionados aos direitos autorais.
- Folhas de Registro de Descobertas: Formulários para os alunos registrarem suas respostas e reflexões ao longo da atividade.
- Computadores ou Tablets (opcional): Para pesquisa online adicional sobre exemplos reais de aplicação de direitos autorais.
- Prêmios Simbólicos: Pequenos prêmios (como adesivos ou certificados) para motivar os alunos a completarem as etapas do mapa.

Atividade:

1. **Introdução:**

   Explanação: Explique o conceito de direitos autorais, sua importância e as consequências de ignorá-los. Fale sobre como músicas, filmes, livros e outros conteúdos digitais estão protegidos por direitos autorais, e o que isso significa para o uso e compartilhamento desses conteúdos. Exemplos Práticos: Mostre exemplos de como o respeito aos direitos autorais é importante, como quando alguém usa uma música em um vídeo sem permissão.

2. **Exploração pelo mapa de direitos autorais:**

   Distribuição: Divida os alunos em pequenos grupos e entregue a cada grupo um "Mapa do Tesouro de Direitos Autorais". Cada "ilha" no mapa representa uma etapa com um desafio relacionado aos direitos autorais. Desafios: Os grupos resolvem os desafios em cada "ilha". Por exemplo:

   - Ilha da Música: Identificar quem detém os direitos autorais de uma canção e como ela pode ser utilizada legalmente.
   - Ilha dos Filmes: Discutir o que é permitido e o que não é ao compartilhar um filme online.
   - Ilha dos Livros: Explorar como citar um livro corretamente em um trabalho escolar respeitando os direitos autorais.

   Pesquisa (opcional): Use computadores ou tablets para que os alunos pesquisem exemplos reais de aplicação de direitos autorais, ajudando a resolver os desafios.

3. **Apresentação e debate:**

   Apresentação: Cada grupo apresenta suas descobertas e soluções para os desafios enfrentados em cada "ilha". Eles explicam como identificaram os direitos autorais e o que aprenderam sobre o uso legal dos conteúdos. Debate: Conduza um debate sobre a importância de respeitar os direitos autorais, perguntando aos alunos como suas ações online podem afetar os criadores de conteúdo.

Reflexão em Grupo: Perguntas para direcionar a reflexão em grupo no final da atividade:

- Por que é importante respeitar os direitos autorais ao usar músicas, filmes ou livros online?
- O que você faria se quisesse usar uma música ou imagem em seu próprio projeto?
- Como você pode aplicar o que aprendeu sobre direitos autorais em suas atividades diárias na internet?

Material Didático Complementar:

- **Guia "Conheça Seus Direitos (Autorais)":** Um guia que os alunos podem levar para casa, explicando os conceitos básicos de direitos autorais, como reconhecer conteúdo protegido e como utilizá-lo corretamente.
- **Pôster "Respeite os Direitos Autorais":** Um jogo de cartas em que os alunos devem combinar fontes com características confiáveis e não confiáveis, reforçando o aprendizado de forma divertida.
- **Certificado de "Explorador dos Direitos Autorais":** Um certificado para cada aluno que completou a atividade, reconhecendo seu conhecimento sobre o respeito aos direitos autorais.

5.11 Justificativa Teórica para as Atividades do 5º Ano

As atividades "Caça às Fakes: Desmascarando Notícias Falsas" e "Exploradores dos Direitos Autorais" para o 5º ano do ensino fundamental são elaboradas com base em teorias de aprendizagem significativa [56] e construtivismo [57], aliadas à crescente importância da cidadania digital e da alfabetização midiática no contexto educacional contemporâneo. Essas atividades visam desenvolver o pensamento crítico e a reflexão ética entre os alunos, ao mesmo tempo que os preparam para atuar de forma responsável e consciente no ambiente digital.

5.11.1 Alfabetização Midiática e Pensamento Crítico

A atividade "Caça às Fakes: Desmascarando Notícias Falsas" trabalha diretamente a alfabetização midiática e o desenvolvimento do pensamento crítico. Conforme Buckingham [53], a alfabetização midiática é crucial no processo de empoderamento dos cidadãos no século XXI, capacitando-os a analisar criticamente o conteúdo que consomem, especialmente em um contexto digital marcado por informações falsas e sensacionalistas. O desenvolvimento da capacidade de distinguir entre notícias verdadeiras e falsas é uma habilidade essencial para evitar a disseminação de desinformação e fomentar uma cultura de cidadania digital responsável, como enfatizado por Ribble [17].

A atividade se baseia na ideia de que a aprendizagem é mais significativa quando os alunos estão ativamente envolvidos no processo de investigação e descoberta, como proposto por Piaget [57]. Os alunos, ao assumirem o papel de "detetives", não apenas identificam as notícias falsas, mas também são incentivados a refletir criticamente sobre as

fontes de informação e a importância da verificação dos fatos, promovendo a metacognição – a capacidade de pensar sobre o próprio processo de pensamento.

Além disso, a atividade promove o uso de habilidades de investigação colaborativa, onde os alunos trabalham em grupos para analisar as notícias e discutir suas descobertas. De acordo com Vygotsky [58], o aprendizado colaborativo é fundamental para a construção do conhecimento, uma vez que as interações sociais contribuem significativamente para o desenvolvimento cognitivo. Ao final da atividade, a criação do mural "Fakes Desmascaradas" reforça a aprendizagem visual e construtiva, permitindo que os alunos consolidem o que aprenderam de forma prática e interativa.

5.11.2 Direitos Autorais e Ética Digital

A atividade "Exploradores dos Direitos Autorais" aborda conceitos centrais da ética digital, capacitando os alunos a compreenderem e respeitarem os direitos autorais no ambiente online. Conforme Ribble [17], a ética digital é um dos nove elementos da cidadania digital e envolve a responsabilidade no uso de recursos digitais, incluindo o respeito pela propriedade intelectual e o entendimento das regras de direitos autorais. Para alunos do 5º ano, que já estão mais familiarizados com o uso de tecnologias, essa atividade é essencial para introduzir conceitos sobre como utilizar conteúdos digitais de maneira ética e legal.

Baseada na teoria da aprendizagem significativa de Ausubel [56], a atividade ajuda os alunos a conectar novos conhecimentos sobre direitos autorais com suas experiências prévias de uso de mídias digitais. A exploração do "Mapa do Tesouro de Direitos Autorais", que guia os alunos por diferentes "ilhas"temáticas, proporciona uma experiência de aprendizagem ativa, onde os alunos resolvem desafios e constroem o entendimento sobre como os direitos autorais se aplicam a conteúdos como músicas, filmes e livros.

Ao trabalhar em grupos para resolver esses desafios, os alunos não apenas aprendem a identificar quem detém os direitos sobre determinados conteúdos, mas também desenvolvem um senso ético e crítico em relação ao uso desses materiais. Piaget [57] argumenta que essa capacidade de reflexão e tomada de decisão moral começa a se desenvolver nessa fase da infância, o que torna essa atividade relevante para preparar os alunos para tomarem decisões conscientes sobre o uso de informações digitais no futuro.

5.11.3 Conceitos Trabalhados nas Atividades

Alfabetização Midiática: A capacidade de analisar e avaliar criticamente as informações que circulam nas mídias digitais, identificando notícias falsas e fontes não confiáveis.

Cidadania Digital: Promove o uso responsável e ético das tecnologias digitais, capacitando os alunos a respeitar direitos autorais e a verificar a veracidade das informações que consomem e compartilham.

Pensamento Crítico: Envolve a análise reflexiva e a avaliação cuidadosa das informações, desenvolvendo habilidades para distinguir entre notícias verdadeiras e falsas e reconhecer conteúdos confiáveis.

Direitos Autorais: A compreensão dos princípios de propriedade intelectual e a importância de respeitar os direitos de autores de conteúdos digitais, como músicas, filmes e livros.

Ética Digital: Incentiva os alunos a agir de maneira responsável no ambiente digital, considerando as implicações éticas de compartilhar conteúdos sem autorização e de violar os direitos autorais.

Investigação Colaborativa: O trabalho em grupo é utilizado para promover a troca de ideias e a resolução conjunta de problemas, fortalecendo as habilidades sociais e cognitivas dos alunos.

Capítulo 6

Considerações Finais

Neste trabalho, explorou-se a crescente demanda por uma educação que inclua segurança digital como parte fundamental da formação cidadã no contexto escolar. Em uma sociedade onde o uso de tecnologias permeia diversas atividades cotidianas, torna-se imperativo que educadores, estudantes e a sociedade em geral estejam preparados para lidar com os desafios e riscos do ambiente digital. Questões como privacidade, segurança de dispositivos, proteção de informações pessoais e rastros digitais são exemplos de temas críticos que todos os usuários de tecnologia enfrentam, consciente ou inconscientemente, ao interagir em ambientes online. Esses elementos não apenas envolvem o conhecimento técnico, mas também exigem uma compreensão ética e social das implicações de nossas escolhas e interações na esfera digital. [55]

A capacitação dos educadores para ensinar esses conceitos é um ponto-chave, pois a simples inclusão de conteúdos tecnológicos nas escolas não assegura a sua efetiva integração ao processo pedagógico [63]. O professor precisa não apenas ser letrado digitalmente, mas também capaz de transmitir esse letramento de forma que os alunos compreendam as implicações éticas e práticas da segurança digital. O papel dos professores é transformar esses conhecimentos em práticas pedagógicas que se alinhem com a realidade digital vivenciada pelos estudantes [28]. Ao alinhar-se às diretrizes da Base Nacional Comum Curricular (BNCC), as atividades voltadas para o letramento digital podem contribuir para a formação de cidadãos críticos e responsáveis [1].

A legislação brasileira é clara sobre o dever de promover uma educação que inclua habilidades digitais e que promova a responsabilidade no uso das tecnologias. Nesse sentido, a BNCC apresenta diretrizes valiosas para nortear essa educação digital desde os anos iniciais, proporcionando um suporte estruturado para que professores possam desenvolver competências digitais nos alunos [55]. Contudo, essa formação não deve ser encarada de maneira superficial: é necessário incorporar princípios pedagógicos, como a Aprendizagem Significativa, que proporcionem uma compreensão profunda das implicações do uso

da tecnologia. O uso de metodologias ativas, lúdicas e inclusivas, que permitam o engajamento dos estudantes sem a necessidade constante de acesso à internet, torna-se uma alternativa viável para integrar esses conceitos de maneira prática e eficaz [64].

A importância de uma abordagem lúdica na educação de segurança digital tem raízes em teorias pedagógicas consolidadas, como as de Piaget e Vygotsky, que defendem o aprendizado ativo e colaborativo. A criação de jogos e atividades interativas, que simulem situações cotidianas relacionadas ao uso seguro das tecnologias, proporciona um ambiente de aprendizado que estimula a participação e o senso crítico das crianças. Tais atividades também permitem que os alunos desenvolvam habilidades práticas e aprendam, por exemplo, a reconhecer os riscos e a importância de proteger suas informações pessoais [63].

Ao buscar uma sociedade mais consciente e preparada para as ameaças digitais, é crucial que a educação para segurança digital seja tratada como um compromisso coletivo. Envolver a família, a escola e a comunidade nesse processo amplia o impacto das ações educativas e reforça o entendimento de que a responsabilidade pela segurança digital é de todos. A implementação de atividades em sala de aula que podem ser estendidas para o ambiente doméstico, como folhetos educativos e guias para os pais, é uma estratégia que promove a continuidade do aprendizado e fortalece a conscientização coletiva [55].

Espera-se que a segurança digital nas escolas vá além de um conjunto de práticas isoladas e se torne parte integral da formação cidadã. Com a rápida evolução das tecnologias, educadores e legisladores precisam trabalhar em conjunto para manter o currículo escolar atualizado e em sintonia com as novas demandas digitais. Dessa forma, ao seguir as diretrizes estabelecidas pela BNCC e integrá-las com metodologias pedagógicas eficazes, será possível formar uma geração de cidadãos preparados para utilizar a tecnologia de maneira responsável e ética, contribuindo para uma sociedade digital mais segura e inclusiva.

Em estudos futuros, seria interessante desenvolver e aplicar instrumentos de avaliação tanto para professores quanto para alunos, com o objetivo de promover reflexões sobre as atividades propostas, permitindo a identificação de pontos a serem aprimorados. Esses instrumentos podem ajudar os educadores a ajustar as práticas pedagógicas e a melhorar o processo de ensino-aprendizagem relacionado à segurança digital. Além disso, a criação de novos materiais didáticos e ferramentas pedagógicas, como jogos educativos e guias interativos, pode enriquecer ainda mais o repertório de ensino e contribuir para uma maior conscientização dos alunos. Recomenda-se também que as atividades práticas, sugeridas neste trabalho, sejam aplicadas nas escolas, e que seus impactos sejam avaliados em termos de engajamento e eficácia na formação de competências digitais. Dessa maneira, o ciclo de aprendizado torna-se dinâmico e constantemente ajustado às necessidades tanto dos estudantes quanto dos educadores.

Isso reforça a importância da contínua capacitação docente e da criação de recursos pedagógicos que estimulem o aprendizado significativo e a reflexão constante sobre as práticas adotadas.

Referências

[1] MEC - Ministério da Educação: *Base Nacional Comum Curricular: Computação: Complemento à BNCC.* MEC, Brasília - DF - Brasil, 2023. http://portal.mec.gov.br/docman/fevereiro-2022-pdf/236791-anexo-ao-parecer-cneceb-n-2-2022-bncc-computacao/file, acesso em 2023-05-05. 4, 24, 60

[2] Nunes, D. H., Lehfeld L. S.: *Cidadania digital: Direitos, deveres, lides cibernéticas e responsabilidade civil no ordenamento jurídico brasileiro.* Revista de Estudos Jurídicos UNESP, 22(35):437–453, 2018. 6, 7

[3] Ribble, Mike: *Digital Citizenship in Schools.* International Society for Technology in Education, 2nd ed. edição, dezembro 2010. 6, 7, 9

[4] 2017, UNESCO: *Guidelines on the inclusion of digital literacy in education.* https://www.gcedclearinghouse.org/sites/default/files/resources/180161eng.pdf, [Accessed 15-09-2024]. 7, 23, 37, 41, 45

[5] Teixeira, M. M., Lima J. A.: *Cidadania digital: Uma proposta de dispositivo móvel para o monitoramento das cidades.* Temática, 1-22., 2013. 8

[6] Dias-Trindade, Sara, Santo Eniel do Espírito: *CompetÊncias digitais de docentes universitÁrios em tempos de pandemia: AnÁlise da autoavaliaÇÃo digcompedu.* Práx. Educ. [online]., vol.17, n.45:pp.100–116, 2021. http://educa.fcc.org.br/scielo.php?script=sci_arttext&pid=S2178-26792021000200100&lng=pt&nrm=iso. 9

[7] Lima, J. P.: *Formação docente para a era digital: Desafios e perspectivas*, 2019. 9

[8] Tardif, Maurice: *Saberes docentes e formação profissional.* Vozes, novembro 2011, ISBN 9788532644282. 9

[9] Pesce, L.: *Cidadania digital e educação: Novos desafios para os professores na era da informação*, 2014. 9

[10] Serres, M.: *A polegarzinha: A revolução digital na escola e na sociedade*, 2015. 10

[11] Moreira, Carla: *Letramento digital: Do conceito à prática.* Anais do SIELP, 2(1):1–12, 2012. 11

[12] Freitas, Maria Teresa: *Letramento digital e formação de professores.* Educação em Revista, 26(03):335–352, 2010. 11, 13

[13] Serim, Francis: *The importance of contemporary literacy in the digital age.* The Big 6: Information Skills for Student Achievement, 2002. http://www.big6.com/showarticle.php?id=157. 12

[14] Selfe, Cynthia L.: *Technology and literacy in the twenty-first century: The importance of paying attention.* Southern Illinois University Press, 1999. 12

[15] Gilster, Paul: *Digital literacy.* John Wiley & Sons, 1997. 12

[16] Tavani, Herman T.: *Ethics and technology: Controversies, questions, and strategies for ethical computing.* Wiley, 2013. 13

[17] Ribble, Mike: *Digital Citizenship in Schools: Nine Elements All Students Should Know.* International Society for Technology in Education, 2015. 13, 23, 40, 44, 50, 51, 57, 58

[18] Melhoramentos (editor): *Michaelis Moderno Dicionário da Língua Portuguesa.* UOL, São Paulo, 5th edição, 2023. Disponível online: https://michaelis.uol.com.br/, acessado em 2 de outubro de 2024. 13

[19] von, Solms Basie e Solms Rossouw von: *Cybersecurity and information security – what goes where?* Information & Computer Security, 26(1):2–9, janeiro 2018, ISSN 2056-4961. https://doi.org/10.1108/ICS-04-2017-0025, acesso em 2024-04-24. 14

[20] Stallings, William e Lawrie Brown: *Computer Security: Principles and Practice.* Pearson Education, 2018. 14

[21] Whitman, Michael E. e Herbert J. Mattord: *Principles of Information Security.* Cengage Learning, 2017. 14

[22] Shoniregun, Charles A.: *Information Security Management: Global Challenges in the New Millennium.* Springer, 2005. 15

[23] International Telecommunication Union: *Global Cybersecurity Index 2020*, 2024. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E, acesso em 2024-04-25. 15, 22

[24] Singer, PW e Allan Friedman: *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press, 2014. 15

[25] European Union Agency for Cybersecurity (ENISA): *Enisa threat landscape 2021*, 2021. Retrieved from https://www.enisa.europa.eu. 15

[26] Buchanan, Robert, Charles Bradley e Liz Seymour: *Cybersecurity education for citizens.* Journal of Digital Citizenship, 3:33–45, 2017. 15

[27] Almeida, Joana e Marcos Silva: *Privacidade digital no ambiente educacional: uma questão de direito.* Revista de Tecnologia Educacional, 15(2):45–62, 2020. 16

[28] Greenleaf, Graham: *Global data privacy laws: 89 countries, and accelerating.* Privacy Laws Business International Report, (121):1–6, 2014. 16, 17, 23, 36, 41, 45, 60

[29] Sampaio, J. C., Fernandes R. S.: *Formação continuada e o uso de tecnologias digitais: Reflexões sobre a cidadania digital no ensino fundamental.* Cadernos de Educação, 22(3):62–81, 2019. 16, 24, 41, 45

[30] Costa, Felipe e Ana Souza: *Controle de dados e privacidade digital: desafios na era da informação.* Revista de Direito Digital, 18(2):78–93, 2021. 16

[31] Doneda, Danilo: *Da privacidade à proteção de dados pessoais.* Revista da Faculdade de Direito - UFPR, 53:29–64, 2011. 17

[32] Ruaro, Regina Linden e Daniel Piñeiro Rodriguez: *O direito à proteção de dados pessoais e a privacidade.* Revista da Faculdade de Direito - UFPR, 47:29–64, 2008. 17

[33] Schaar, René Ariel: *Tutela jurídica da privacidade.* Saraiva, 2007. 17

[34] Karabatak, Müjgan e Recep Şahin: *Security of mobile devices: A systematic review of issues, challenges, and solutions.* Future Internet, 13(5):1–22, 2021. 18

[35] Amrozi, Elly, Rina Hasan e Dwi Priatna: *The importance of mobile device security and its impact on digital privacy.* Em *International Conference on Cyber Security and Protection of Digital Services*, páginas 45–50. IEEE, 2019. 18

[36] Montes, João Carlos: *Rastros digitais: privacidade e vigilância no ambiente digital.* Revista de Estudos Digitais, 7(3):56–78, 2020. 18

[37] Silva, Andréia e Gustavo Oliveira: *O impacto dos rastros digitais na privacidade online.* Revista Brasileira de Segurança Digital, 5(2):123–145, 2018. 18

[38] Pereira, Clara e Júlia Almeida: *Riscos e benefícios dos rastros digitais no contexto da cidadania digital.* Educação e Tecnologia, 12(1):89–112, 2021. 19

[39] Gomes, Rafael: *Rastros digitais e a segurança de jovens na internet: desafios e práticas educacionais.* Tecnologia na Educação, 10(4):101–125, 2019. 19

[40] Buckingham, David: *The Media Education Manifesto.* Polity Press, Cambridge, 2019. 19

[41] Hobbs, Renée: *Create to Learn: Introduction to Digital Literacy.* Wiley, New Jersey, 2017. 19

[42] Jenkins, Henry: *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century.* MIT Press, Cambridge, MA, 2009. 19

[43] Organization, World Intellectual Property: *Understanding Copyright and Related Rights.* WIPO, 2020. `https://www.wipo.int/publications/en/details.jsp?id=500`. 20

[44] Silva, Maria de Fátima: *Os direitos autorais e o ambiente digital: desafios e perspectivas.* Revista de Direito e Tecnologia, 12(3):45–60, 2020. 20

[45] Pontes, Carlos Henrique: *Direitos morais e patrimoniais: uma abordagem contemporânea*. Revista Jurídica de Propriedade Intelectual, 8(2):120–138, 2019. 20

[46] Pereira, João Augusto: *A gestão de direitos autorais no ambiente digital: novas tecnologias e desafios*. Cadernos de Direito Digital, 10(1):100–115, 2021. 20

[47] Varela, Carlos: *Teaching copyright in the digital age: Legal and ethical aspects*. Journal of Digital Literacy, 10(2):45–58, 2018. 20

[48] Sherman, Brad e Lionel Bently: *The Making of Modern Intellectual Property Law*. Cambridge University Press, Cambridge, 2014. 21

[49] Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação: *TIC Domicílios 2023*. https://cetic.br/pt/pesquisa/domicilios/indicadores/, acesso em 2024-04-25. 22, 33

[50] Novais, Alessandra Ferreira Salgado, Elineide Cavalcanti De Oliveira, Francisco Benilson Soares Da Silva, Hermócrates Gomes Melo Júnior, Jocelino Antonio Demuner, Karina Freitas Teofilo Da Silva, Mara Lívia Linhares Da Silva, Maria Gneglauda Holanda e Murilo Monteiro De Souza: *Promovendo Segurança Online no Ambiente Educacional Moderno*. REVISTA FOCO, 17(1):e4113, janeiro 2024, ISSN 1981-223X. https://ojs.focopublicacoes.com.br/foco/article/view/4113, acesso em 2024-04-25. 22

[51] Livingstone, Sonia e Ellen J. Helsper: *Parental Mediation of Children's Internet Use*. Journal of Broadcasting & Electronic Media, 52(4):581–599, novembro 2008, ISSN 0883-8151, 1550-6878. http://www.tandfonline.com/doi/abs/10.1080/08838150802437396, acesso em 2024-04-25. 23

[52] Boyd, Danah: *It's Complicated: The Social Lives of Networked Teens*. Yale University Press, dezembro 2020, ISBN 9780300166439. https://www.degruyter.com/document/doi/10.12987/9780300166439/html, acesso em 2024-04-25. 23

[53] Buckingham, David: *Youth, Identity, and Digital Media*. novembro 2007, ISBN 9780262524834. https://mitpress.mit.edu/9780262524834/youth-identity-and-digital-media/, acesso em 2024-04-25. 23, 50, 51, 57

[54] Wing, Jeannette M.: *Computational thinking*. Communications of the ACM, 49(3):33–35, 2006. 26

[55] Desiderá, Lucimara e Miriam von Zuben: *Crianças e adolescentes: usando a internet com segurança*. Comitê Gestor da Internet no Brasil, 2012. Disponível em: http://cartilha.cert.br/. 33, 60, 61

[56] Ausubel, David P.: *Educational Psychology: A Cognitive View*. New York: Holt, Rinehart Winston, 1968. 33, 36, 40, 44, 50, 51, 57, 58

[57] Piaget, Jean: *Development and learning*. Journal of Research in Science Teaching, 2:176–186, 1964. 33, 40, 44, 57, 58

[58] Vygotsky, Lev S: *Mind in Society: The Development of Higher Psychological Processes*. Harvard University Press, Cambridge, MA, 1978. 33, 51, 58

[59] Dewey, J.: *Democracy and education: An introduction to the philosophy of education.*, 1916. 36, 40

[60] Bruner, Jerome S.: *The act of discovery*. Harvard Educational Review, 31:21–32, 1961. 36, 44

[61] Freire, Paulo: *Pedagogia do Oprimido*. Rio de Janeiro: Paz e Terra, 1970. 36, 44, 50

[62] Kohlberg, Lawrence: *Essays on Moral Development: The Philosophy of Moral Development*. Harper & Row, San Francisco, 1981. 50

[63] Lankshear, Colin e Michele Knobel: *New Literacies: Everyday Practices and Classroom Learning*. McGraw-Hill International, 2008. 60, 61

[64] Papert, Seymour: *Mindstorms: Children, Computers, and Powerful Ideas*. Basic Books, 1980. 61