Monumenta - Revista Científica Multidisciplinar

Artigos

Ensino de segurança da informação no fundamental 1: uso de ia e laboratórios virtuais como ferramentas

Teaching information security in elementary school: the use of ai and virtual labs as tools

Edson Wander Soares Viana Junior[1]

[1]Especialização em Engenharia de Software; Cientista da Computação; Licenciado em Informática; Licenciado em Matemática; Professor no Ensino Fundamental em Maricá.
✉ ed.wanderjr@gmail.com

Palavras-chave:
Segurança da informação;
Inteligência artificial;
Laboratórios virtuais;
Ensino fundamental;
Educação digital.

Resumo

Este artigo explora a relevância do ensino de segurança da informação no Ensino Fundamental 1, destacando a utilização de ferramentas como Inteligência Artificial (IA) e laboratórios virtuais para promover o aprendizado de práticas seguras e consciência digital desde cedo. São apresentados conceitos fundamentais, metodologias pedagógicas e exemplos práticos que ilustram como essas abordagens podem ser integradas ao currículo escolar, preparando as crianças para os desafios de um mundo cada vez mais conectado.

Keywords:
Information security;
Artificial intelligence;
Virtual labs;
Elementary education;
Digital literacy.

Abtract

This article explores the importance of teaching information security in elementary edu-cation, emphasizing tools such as Artificial Intelligence (AI) and virtual labs to promote safe practices and digital awareness from an early age. Fundamental concepts, pedago-gical methodologies, and practical examples are presented to demonstrate how these approaches can be integrated into the school curriculum, preparing children for the chal-lenges of an increasingly connected world.

1 INTRODUÇÃO

Com o avanço exponencial da tecnologia e sua incorporação no cotidiano das pessoas, tornou-se impossível ignorar a relevância de preparar crianças para um ambiente cada vez mais digital. Desde a primeira infância, as crianças começam a desenvolver habilidades por meio de estímulos familiares e vivências sociais. No Ensino Fundamental 1, a escola tem o papel de aprimorar essas habilidades, proporcionando um ambiente que favoreça seu aperfeiçoamento. Nesse contexto, a introdução da Segurança da Informação torna-se essencial para ampliar a consciência e a capacidade dos estudantes de interagir com a tecnologia de forma segura e responsável. O uso da internet por crianças não é apenas uma tendência, mas uma realidade que apresenta tanto benefícios quanto riscos (Silva, 2014).

A internet proporciona acesso a uma vasta gama de informações, plataformas educacionais, jogos interativos e redes sociais que podem enriquecer o aprendizado e a socialização. No entanto, a falta de orientação adequada expõe as crianças a uma série de ameaças, como *cyberbullying, phishing*, roubo de identidade, manipulação de informações e exposição a conteúdos inadequados. Nesse contexto, ensinar princípios básicos de Segurança da Informação desde cedo é essencial para ajudá-las a reconhecer e responder a esses desafios.

Embora o tema da Segurança da Informação geralmente seja associado a profissionais de tecnologia ou ambientes corporativos, ele deve ser visto como um elemento essencial na formação educacional básica. A alfabetização digital não se limita ao uso de ferramentas e dispositivos; ela inclui também a compreensão dos riscos associados a eles e a habilidade de tomar decisões informadas. A formação em Segurança da Informação no Ensino Fundamental 1 contribui para a construção de uma cidadania digital responsável, ampliando o senso crítico das crianças e preparando-as para um mundo onde a tecnologia desempenha um papel central.

A urgência em abordar essa temática também está relacionada à crescente independência tecnológica das crianças. Muitos jovens começam a usar dispositivos móveis e acessar redes sociais antes mesmo de completarem 10 anos. Sem a orientação necessária, eles podem se tornar vítimas de golpes online ou apresentar comportamentos de risco em ambientes digitais. A escola, como espaço de aprendizado e socialização, tem o potencial de ser um ambiente seguro e estruturado para iniciar essa educação (ANATEL, 2024).

Além disso, as crianças de hoje serão os adultos responsáveis pela manutenção da segurança digital no futuro. Investir na formação de habilidades críticas e éticas desde os primeiros anos escolares é uma estratégia preventiva que visa minimizar os impactos de ameaças digitais, não apenas na infância, mas ao longo de suas vidas. Assim, o ensino de Segurança da Informação no Ensino Fundamental 1 não é apenas uma necessidade imediata, mas também um investimento a longo prazo na segurança e bem-estar da sociedade.

O ambiente digital é um espaço onde crianças podem aprender, explorar e socializar, mas também um território que exige precauções específicas. A falta de conhecimento sobre práticas seguras pode levar as crianças a situações de vulnerabilidade. Por exemplo, muitas delas compartilham informações pessoais, como nome, endereço ou escola, em plataformas digitais sem compreender os possíveis riscos. Ensinar Segurança da Informação ajuda a prevenir esses comportamentos e a proteger a privacidade das crianças.

O *cyberbullying* é uma das ameaças mais frequentes enfrentadas por jovens no ambiente digital. Sem orientação, as crianças podem não reconhecer as formas de abuso *on-line* ou não saber como reagir a elas. A educação em Segurança da Informação não apenas ensina as crianças a evitar comportamentos que as exponham a situações de risco, mas também a identificar práticas nocivas e buscar ajuda. A compreensão das consequências de suas ações no ambiente digital também é essencial para promover um uso ético da tecnologia.

Outro risco significativo é o roubo de identidade. Crianças podem ser alvos fáceis para criminosos que buscam explorar informações sensíveis para atividades fraudulentas. Por meio de aulas e atividades práticas, é possível ensinar os alunos a reconhecer tentativas de *phishing* e a importância de senhas fortes e únicas. O aprendizado desses conceitos desde cedo ajuda a criar hábitos que serão úteis ao longo de toda a vida.

Além das ameaças diretas, há também desafios relacionados ao acesso a conteúdos impróprios ou prejudiciais. Sem supervisão adequada, as crianças podem ser expostas a materiais violentos, discriminatórios ou de cunho sexual. Educar sobre o uso consciente da internet inclui ensinar os alunos a discernir informações confiáveis e desenvolver senso crítico para avaliar esses conteúdos (Memória Forense, 2024).

A introdução à Segurança da Informação no Ensino Fundamental 1 também contribui para o desenvolvimento da cidadania digital. Isso inclui não apenas a proteção contra riscos, mas também a promoção de

comportamentos éticos, como o respeito à privacidade alheia e a não disseminação de informações falsas. Esses valores são fundamentais para a construção de um ambiente digital mais seguro e colaborativo.

Diante do cenário descrito, este estudo tem como foco explorar métodos inovadores para o ensino de Segurança da Informação no Ensino Fundamental 1. A abordagem central é o uso de Inteligência Artificial (IA) e laboratórios virtuais como ferramentas pedagógicas, com o objetivo de tornar o aprendizado mais eficiente e adequado ao perfil das crianças nessa faixa etária. A IA, com suas capacidades de personalização e interatividade, oferece uma oportunidade única para adaptar o ensino às necessidades individuais dos alunos (Amazon, 2024).

O objetivo principal deste estudo é identificar estratégias que unam tecnologia e pedagogia para ensinar conceitos básicos de Segurança da Informação de forma lúdica e interativa. A pesquisa busca responder às seguintes perguntas: Como a IA pode ser usada para personalizar o aprendizado em Segurança da Informação? De que maneira laboratórios virtuais podem simular situações reais para ensinar práticas seguras? Quais são as metodologias mais eficazes para engajar crianças nessa temática?

Além disso, o estudo pretende avaliar os impactos dessas abordagens na aprendizagem e no comportamento digital das crianças. Serão analisados aspectos como a retenção de conhecimento, a mudança de atitudes em relação ao uso da tecnologia e a capacidade de identificar riscos e adotar práticas seguras. A combinação de IA e laboratórios virtuais é investigada como uma solução integrada para superar os desafios tradicionais do ensino desse tema, como a abstração de conceitos técnicos e a dificuldade de engajar alunos mais jovens (Jornal O Candeeiro, 2024).

Por meio deste estudo, espera-se não apenas oferecer uma base teórica sólida para o ensino de Segurança da Informação, mas também propor práticas concretas que possam ser implementadas por educadores. Ao longo do trabalho, serão apresentados exemplos de atividades, estudos de caso e diretrizes para a criação de programas educacionais que abordem a segurança digital de maneira acessível e eficaz. Com isso, almeja-se contribuir para a formação de uma geração mais preparada para os desafios do mundo digital e comprometida com a construção de um ambiente virtual seguro e responsável.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Fundamentos de Segurança da Informação

A Segurança da Informação é um campo essencial para garantir a proteção de dados em uma sociedade cada vez mais dependente de tecnologias digitais. Com o aumento do uso de dispositivos conectados, a relevância desse tema transcende o ambiente corporativo e se torna fundamental no cotidiano de qualquer pessoa, incluindo crianças em idade escolar. No Ensino Fundamental 1, a introdução de conceitos básicos de segurança cibernética oferece uma oportunidade para preparar crianças para lidar com os desafios de um mundo digital em rápida evolução, proporcionando um ambiente que favoreça o aprimoramento de competências essenciais ao longo de suas vidas.

A compreensão dos fundamentos de Segurança da Informação é vital para identificar os principais riscos associados ao uso da internet e adotar medidas de proteção. Esses fundamentos abrangem desde definições conceituais até práticas que promovem a conscientização e o comportamento seguro. O ensino dessas práticas para crianças exige uma abordagem simplificada, mas consistente, para assegurar que conceitos técnicos possam ser compreendidos e aplicados de forma prática em seu cotidiano (Profissionais TI, 2024).

2.1.1 Definição de Segurança da Informação

Segurança da Informação é definida como o conjunto de práticas, políticas e tecnologias destinadas a proteger dados e sistemas contra acessos não autorizados, alterações não permitidas, usos indevidos e destruição, seja ela acidental ou intencional. O foco principal é garantir a confidencialidade, integridade e disponibilidade dos dados, ao mesmo tempo que se promove a autenticidade e a irretratabilidade das interações digitais. Esses elementos formam o núcleo do que é necessário para manter um ambiente digital seguro (Schelenz *et al.*, 2023).

No contexto educacional, a definição de Segurança da Informação deve ser adaptada para facilitar o entendimento pelas crianças. Isso pode ser feito por meio de analogias, como comparar senhas a chaves de casa ou explicar que "informações importantes precisam ser protegidas como se fossem segredos valiosos". Essa simplificação permite que os alunos compreendam a importância de proteger seus dados e os dados dos outros (Santos, 2024).

Mais do que uma simples aplicação de tecnologia, a Segurança da Informação envolve uma mudança cultural e comportamental. Encorajar boas práticas, como o uso de senhas fortes e a desconfiança de *link*s desconhecidos, é tão importante quanto implementar medidas tecnológicas. Isso reflete a natureza abrangente do conceito, que vai além do técnico e inclui aspectos éticos e sociais.

A necessidade de ensinar Segurança da Informação no Ensino Fundamental 1 também está relacionada à crescente independência das crianças no uso de dispositivos conectados. Elas estão cada vez mais expostas a situações que exigem discernimento, como interagir em redes sociais ou utilizar aplicativos educacionais. Assim, entender o que é a Segurança da Informação é o primeiro passo para capacitá-las a enfrentar esses desafios (Biblioteca de Segurança, 2024).

2.1.2. Princípios Básicos de Segurança

Os princípios fundamentais da Segurança da Informação são essenciais para a proteção de dados e sistemas. Eles fornecem uma estrutura que orienta tanto a criação de tecnologias seguras quanto o desenvolvimento de hábitos comportamentais responsáveis. Esses princípios incluem confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade.

Confidencialidade: A confidencialidade busca assegurar que informações sejam acessíveis apenas para pessoas ou sistemas autorizados. Esse princípio protege dados sensíveis contra acessos não autorizados. No Ensino Fundamental 1, a confidencialidade pode ser ensinada por meio de práticas simples, como não compartilhar senhas e manter informações pessoais privadas, ajudando as crianças a compreenderem a importância de proteger seus próprios dados e respeitar a privacidade dos outros (ANATEL, 2024).

Integridade: A integridade garante que os dados permaneçam precisos e consistentes, ou seja, que não sejam alterados de forma indevida ou não autorizada. Para as crianças, isso pode ser exemplificado com situações cotidianas, como a necessidade de manter o conteúdo original de um trabalho escolar ou evitar a exclusão acidental de arquivos. Ensinar esse conceito ajuda a construir um senso de responsabilidade em relação ao uso de informações digitais.

Disponibilidade: A disponibilidade assegura que informações e sistemas estejam acessíveis sempre que necessários. Para instituições educacionais, isso significa que plataformas digitais, redes de computadores e materiais online devem ser operacionais para atender às demandas dos alunos e professores.

Esse princípio destaca a importância de infraestrutura confiável, algo que também pode ser discutido em atividades práticas em sala de aula.

Autenticidade: A autenticidade refere-se à garantia de que informações e comunicações são genuínas e provenientes de fontes confiáveis. No contexto educacional, a autenticidade pode ser abordada ao ensinar crianças a verificarem a origem de mensagens, reconhecerem e-mails suspeitos e confirmarem a validade de informações obtidas na internet.

Irretratabilidade: Também chamada de não-repúdio, a irretratabilidade assegura que uma pessoa ou entidade não possa negar a autoria de uma ação ou transação realizada. Na educação das crianças, esse conceito pode ser introduzido com exemplos práticos, como lembrar que ações digitais, como o envio de mensagens ou a postagem de conteúdos, deixam rastros. Essa noção ajuda a reforçar o senso de responsabilidade e ética no ambiente online.

Esses cinco princípios não apenas fundamentam a proteção técnica de sistemas, mas também fornecem uma base pedagógica para ensinar Segurança da Informação de forma eficaz. Incorporar esses conceitos no Ensino Fundamental 1 ajuda a criar uma cultura de segurança desde cedo, preparando as crianças para interagir de maneira responsável com o ambiente digital.

2.1.3 Tipos de Ameaças e Vulnerabilidades

As ameaças e vulnerabilidades no ambiente digital representam desafios significativos para a Segurança da Informação. Ensinar esses conceitos às crianças requer abordagens que transformem cenários complexos em exemplos práticos e compreensíveis. É essencial que elas saibam identificar situações de risco e aprender como evitá-las, promovendo um comportamento seguro online.

Principais Ameaças:

- *Malware*: Programas maliciosos, como vírus e *ransomware*, podem prejudicar dispositivos ao roubar ou destruir informações. Para crianças, isso pode ser explicado como "programas ruins que podem bagunçar o computador".
  Phishing: Ataques que enganam os usuários para que forneçam informações pessoais. Isso pode ser ensinado com alertas sobre mensagens ou *links* suspeitos.
- Roubo de Identidade: Uso não autorizado de informações pessoais, como nome ou fotos, para fins fraudulentos.
- *Cyberbullying*: Comportamentos prejudiciais praticados por meio de plataformas digitais, que podem afetar a saúde emocional das crianças.
  Invasões de Privacidade: Acesso indevido a dados pessoais, algo que pode ser mitigado com a aplicação de configurações de privacidade adequadas.

Vulnerabilidades Comuns:

- Senhas Fracas: Utilizar combinações simples ou reutilizar senhas em várias contas aumenta o risco de invasões.
- Sistemas Desatualizados: A falta de atualizações de segurança deixa dispositivos mais suscetíveis a ataques.
- Comportamentos Impulsivos: Clicar em *links* desconhecidos ou baixar aplicativos de fontes não confiáveis pode comprometer a segurança.
- Conexões Inseguras: Redes *Wi-Fi* públicas ou mal configuradas são alvos fáceis para *hackers*.

- Falta de Conscientização: A ausência de conhecimento sobre práticas seguras é um fator agravante em ambientes digitais.

Incorporar esses conceitos ao currículo do Ensino Fundamental 1 é essencial para capacitar as crianças a identificarem riscos e adotarem práticas preventivas. Além disso, atividades práticas e jogos podem ajudar a reforçar esses conceitos de maneira lúdica, preparando os alunos para um uso mais seguro e responsável da tecnologia.

2.2. Introdução à Inteligência Artificial (IA)

A Inteligência Artificial (IA) é uma das áreas mais inovadoras da ciência da computação, transformando significativamente a forma como vivemos, trabalhamos e interagimos com a tecnologia. Desde sistemas de recomendação em plataformas de *streaming* até veículos autônomos, a IA desempenha um papel central em inúmeras aplicações modernas. Sua capacidade de aprender, raciocinar e se adaptar a diferentes cenários a torna uma ferramenta poderosa, especialmente em áreas críticas como a Segurança da Informação.

Com o avanço exponencial das tecnologias de IA, sua aplicação está se tornando cada vez mais acessível e diversificada, permitindo que seja integrada em contextos educacionais. No Ensino Fundamental 1, a introdução de conceitos básicos de IA pode despertar a curiosidade das crianças e ajudá-las a entender como essa tecnologia funciona, ao mesmo tempo que promove uma compreensão prática de sua importância para a segurança no ambiente digital.

2.2.1 Definição e Conceitos Básicos de IA

A Inteligência Artificial é definida como a ciência que projeta sistemas computacionais capazes de executar tarefas que tradicionalmente exigem inteligência humana. Isso inclui atividades como reconhecimento de padrões, aprendizado a partir de dados, resolução de problemas, planejamento e até mesmo tomada de decisões. Em termos simples, a IA pode ser vista como a habilidade de uma máquina em "pensar" e "aprender" para realizar tarefas de forma autônoma.

Os sistemas de IA geralmente são divididos em dois tipos principais: IA estreita e IA geral. A IA estreita refere-se a sistemas projetados para executar uma tarefa específica, como tradução de idiomas ou reconhecimento facial. Já a IA geral, ainda em desenvolvimento, seria capaz de realizar qualquer tarefa intelectual que um ser humano possa executar.

No contexto educacional, é essencial introduzir esses conceitos de maneira simples e acessível, utilizando exemplos do cotidiano das crianças, como assistentes virtuais (ex.: Alexa ou Google Assistente) e aplicativos de tradução. Essas abordagens ajudam a desmistificar a IA e tornam seu aprendizado mais relevante e interessante para os alunos.

2.2.2. Aplicações de IA na Segurança da Informação

Na área de Segurança da Informação, a IA emergiu como uma aliada indispensável para combater as ameaças digitais em constante evolução. Ferramentas baseadas em IA oferecem capacidades avançadas de monitoramento, análise e resposta a incidentes, permitindo uma abordagem mais proativa e eficiente para a proteção de sistemas e dados.

Monitoramento em Tempo Real: A IA é amplamente utilizada para monitorar redes e sistemas em tempo real. Por meio de algoritmos avançados, é possível detectar atividades suspeitas, como acessos não

autorizados, comportamento anômalo de usuários e tentativas de invasão. Esses sistemas analisam um volume massivo de dados que seria impossível para humanos processarem em tempo hábil.

Identificação de Padrões Suspeitos: Ferramentas de IA empregam técnicas de aprendizado de máquina para identificar padrões de comportamento que indicam potenciais ameaças. Por exemplo, um sistema pode reconhecer quando um usuário está tentando acessar repetidamente áreas restritas de um sistema, algo que poderia indicar uma tentativa de força bruta.

Detecção e Resposta a Ataques: Sistemas de IA são capazes de detectar ataques em andamento, como ataques de negação de serviço (DDoS) ou tentativas de *phishing*, e responder automaticamente para minimizar os danos. Essa capacidade de resposta rápida é crucial em um ambiente digital onde cada segundo conta para proteger informações sensíveis.

Prevenção Proativa: A IA não apenas responde a ameaças existentes, mas também prevê ataques futuros com base em dados históricos e padrões emergentes. Essa capacidade de prever cenários potenciais permite que administradores de sistemas implementem medidas preventivas antes que ocorram incidentes de segurança.

Autenticação Inteligente: Outra aplicação importante da IA na Segurança da Informação é a autenticação baseada em comportamentos. Por exemplo, sistemas podem usar dados biométricos, como impressões digitais ou reconhecimento facial, combinados com o comportamento típico do usuário (como horários de acesso e locais) para determinar se uma tentativa de login é legítima.

Educação e Conscientização: A IA também pode ser usada para criar ambientes educacionais adaptativos que ensinam boas práticas de segurança cibernética. Plataformas interativas podem personalizar o aprendizado com base nas necessidades do usuário, tornando o processo de conscientização mais eficaz.

No contexto do Ensino Fundamental 1, essas aplicações podem ser integradas a ferramentas educacionais que simulem ameaças e ensinem crianças a identificar comportamentos suspeitos. Por exemplo, jogos baseados em IA podem ensinar os alunos a reconhecer tentativas de *phishing* ou proteger informações pessoais de forma lúdica e envolvente.

Desafios da Implementação de IA na Segurança da Informação: Embora as aplicações de IA ofereçam inúmeros benefícios, sua implementação também apresenta desafios. A complexidade dos sistemas de IA pode dificultar a compreensão de como eles chegam a determinadas conclusões, algo conhecido como o problema da "caixa preta". Além disso, é necessário garantir que os dados utilizados para treinar os algoritmos sejam confiáveis e éticos, especialmente em um ambiente educacional.

Outro desafio é a acessibilidade: Ferramentas avançadas de IA podem ser caras e exigir infraestrutura robusta, o que pode ser um obstáculo em escolas com recursos limitados. Apesar disso, o uso de IA em plataformas educacionais mais simples, como jogos interativos ou aplicativos de aprendizado, já oferece uma introdução prática para os alunos.

A Inteligência Artificial, quando aplicada à Segurança da Informação, tem o potencial de transformar a forma como protegemos dados e sistemas. No Ensino Fundamental 1, essas tecnologias podem ser incorporadas em atividades práticas e lúdicas que ensinem às crianças os conceitos básicos de segurança digital, ajudando-as a desenvolver uma compreensão sólida e aplicável para um futuro mais seguro no mundo digital.

2.3. Laboratórios Virtuais como Ferramenta de Ensino

O uso de laboratórios virtuais no ensino de Segurança da Informação tem se consolidado como uma abordagem eficiente e inovadora para proporcionar experiências práticas e interativas. Essas plataformas permitem que os alunos explorem conceitos complexos em um ambiente controlado, simulando cenários do mundo real sem os riscos associados a experimentos diretos em sistemas reais. No Ensino Fundamental 1, laboratórios virtuais oferecem uma maneira lúdica e segura de introduzir conceitos de segurança digital, tornando o aprendizado mais envolvente e significativo.
A integração de laboratórios virtuais no currículo permite superar barreiras tradicionais de ensino, como a falta de equipamentos físicos e a dificuldade em replicar situações reais de ameaças e defesas cibernéticas. Além disso, esses ambientes possibilitam personalizar o aprendizado de acordo com o nível de conhecimento dos alunos, ajudando-os a desenvolver habilidades críticas e práticas desde cedo (UFMT, 2024).

2.3.1 Importância dos Laboratórios Virtuais no Ensino de Segurança da Informação

Laboratórios virtuais desempenham um papel essencial no ensino de Segurança da Informação, especialmente para crianças do Ensino Fundamental 1. Por meio desses ambientes, conceitos que poderiam parecer abstratos ou complexos são traduzidos em atividades práticas e acessíveis. Essa abordagem não apenas melhora a retenção de conhecimento, mas também desenvolve habilidades práticas que são fundamentais no mundo digital.

Aprendizado Prático e Interativo: Diferentemente de abordagens exclusivamente teóricas, os laboratórios virtuais oferecem oportunidades para "aprender fazendo". As crianças podem participar de atividades que simulem situações reais, como identificar e mitigar ameaças online ou configurar medidas básicas de proteção, como senhas seguras. Esse aprendizado prático é mais eficaz para fixar conceitos e preparar os alunos para aplicar o que aprendem.

Ambiente Seguro para Experimentação: Um dos maiores benefícios dos laboratórios virtuais é a segurança. Alunos podem explorar cenários de ataques cibernéticos e práticas de defesa sem o risco de comprometer dados reais ou sistemas operacionais. Isso é particularmente importante no Ensino Fundamental 1, onde o objetivo principal é ensinar boas práticas de segurança sem expor os alunos a riscos.
Engajamento e Motivação: Laboratórios virtuais frequentemente utilizam elementos de gamificação, como desafios, recompensas e rankings, para manter os alunos motivados. Essa abordagem é especialmente eficaz para crianças, que tendem a se engajar mais em atividades lúdicas e competitivas.

Inclusão Digital e Democratização do Ensino: Muitas escolas enfrentam limitações financeiras e tecnológicas que dificultam o acesso a equipamentos físicos para práticas de segurança digital. Laboratórios virtuais eliminam essas barreiras, permitindo que alunos em qualquer lugar, com acesso a um computador ou tablet, participem de atividades práticas de alta qualidade.

Desenvolvimento de Habilidades para o Futuro: O uso de laboratórios virtuais prepara as crianças para um futuro digital, ajudando-as a entender conceitos como privacidade, proteção de dados e a importância da ética no uso da tecnologia. Essas habilidades serão essenciais à medida que crescem e se tornam cada vez mais expostas ao mundo conectado.

2.3.2 Tipos de Laboratórios Virtuais Disponíveis

Os laboratórios virtuais para o ensino de Segurança da Informação são diversificados, oferecendo soluções adaptadas para diferentes necessidades e faixas etárias. No Ensino Fundamental 1, é essencial

selecionar plataformas que combinem simplicidade, interatividade e relevância para a faixa etária, garantindo que os alunos se envolvam e aprendam de forma eficaz.

Ambientes Gamificados: Os laboratórios gamificados são projetados para ensinar segurança digital por meio de jogos e desafios interativos. Esses ambientes simulam cenários do mundo real, como identificar e evitar tentativas de *phishing* ou proteger uma rede contra ataques virtuais.

Exemplos incluem jogos como *CyberStart Game*, que apresenta desafios crescentes, permitindo que os alunos aprendam enquanto se divertem. Esses ambientes estimulam o pensamento crítico e a resolução de problemas, habilidades valiosas no contexto da segurança digital.

Plataformas de Simulação de Ameaças: Essas plataformas recriam cenários reais de ameaças cibernéticas, permitindo que os alunos pratiquem estratégias de defesa em um ambiente seguro. Simulações podem incluir ataques de *malware*, roubo de dados e invasões de privacidade.

Por exemplo, ferramentas como o *SafeKids* simulam o envio de e-mails maliciosos e ajudam os alunos a reconhecer sinais de *phishing*. Essa abordagem é útil para desenvolver a capacidade de identificar ameaças no mundo real.

Laboratórios Baseados em IA: Os laboratórios que utilizam inteligência artificial personalizam os desafios de aprendizado com base no progresso e nas necessidades de cada aluno. Esses ambientes ajustam a dificuldade das tarefas automaticamente, garantindo que todos aprendam no seu próprio ritmo.

Um exemplo é o AI *Cyber Lab*, que utiliza IA para criar cenários de segurança adaptativos, como a configuração de *firewalls* ou o reconhecimento de padrões de ataque. Além de ensinar habilidades técnicas, esses laboratórios promovem uma compreensão mais profunda de como a IA é usada na segurança digital.

Plataformas Online Interativas: Plataformas como o *Code.org* oferecem módulos específicos sobre segurança digital, incluindo atividades práticas e tutoriais interativos. Embora sejam amplamente usadas para ensinar programação, também possuem módulos que introduzem conceitos de segurança digital de maneira simplificada e acessível.

Sistemas de Simulação Multiusuário: Algumas plataformas permitem que alunos colaborem em equipes para resolver problemas de segurança. Esse tipo de laboratório incentiva o trabalho em equipe e o desenvolvimento de habilidades interpessoais, além de ensinar a importância da colaboração em cenários de segurança cibernética.

Os laboratórios virtuais são uma ferramenta poderosa para ensinar Segurança da Informação de forma prática e interativa. Sua capacidade de simular cenários reais em um ambiente seguro, combinada com elementos de gamificação e personalização, os torna uma escolha ideal para o Ensino Fundamental 1. À medida que a tecnologia avança, espera-se que esses laboratórios se tornem ainda mais acessíveis e diversificados, desempenhando um papel central na formação de jovens cidadãos digitais conscientes e preparados.

2.4. Integração de IA e Laboratórios Virtuais no Ensino de Segurança da Informação

A integração da Inteligência Artificial (IA) com laboratórios virtuais no ensino de Segurança da Informação oferece uma oportunidade única para transformar a maneira como os alunos aprendem conceitos fundamentais de proteção digital. Essa união combina as capacidades analíticas e adaptativas da IA com

os ambientes práticos e simulados dos laboratórios virtuais, criando uma experiência de aprendizado mais rica, personalizada e eficaz. Essa abordagem não apenas torna o aprendizado mais atrativo para os alunos do Ensino Fundamental 1, mas também os prepara para os desafios de um mundo cada vez mais conectado.

2.4.1. Benefícios da Integração de IA e Laboratórios Virtuais

A aplicação conjunta de IA e laboratórios virtuais no ensino de Segurança da Informação proporciona diversos benefícios significativos, tanto para alunos quanto para educadores. Esses benefícios vão além do ensino convencional, explorando novas formas de transmitir conhecimentos e desenvolver habilidades.

Personalização do Aprendizado: Uma das maiores vantagens da IA é sua capacidade de personalizar a experiência de aprendizado. Com base no desempenho e nas interações de cada aluno, os sistemas de IA podem ajustar o nível de dificuldade dos desafios, sugerir atividades específicas para corrigir falhas de entendimento e até mesmo recomendar materiais de estudo complementares. No contexto da segurança da informação, isso significa que alunos podem receber tarefas adaptadas às suas habilidades, como identificar um *phishing* simples ou configurar um sistema de autenticação mais avançado.

Melhora na Retenção de Conhecimentos por Meio de Interatividade: A integração de IA permite que os laboratórios virtuais se tornem mais interativos e dinâmicos, criando experiências de aprendizado imersivas. Por exemplo, um laboratório pode simular um ataque cibernético em tempo real, onde a IA avalia as ações do aluno e fornece *feedback* imediato. Essa interação direta com cenários realistas melhora significativamente a retenção de conhecimentos.

Identificação e Correção de Lacunas no Aprendizado em Tempo Real: Ferramentas de IA podem monitorar continuamente o desempenho do aluno e identificar áreas onde ele apresenta dificuldades. Se um aluno, por exemplo, tem dificuldades em reconhecer sinais de um ataque de *malware*, o sistema pode propor atividades específicas para reforçar esse conhecimento, garantindo que lacunas de aprendizado sejam preenchidas rapidamente.

Aprimoramento da Experiência do Educador: Para os professores, a integração de IA e laboratórios virtuais fornece relatórios detalhados sobre o progresso de cada aluno, permitindo uma abordagem mais direcionada e eficiente. Em vez de ensinar conceitos de forma genérica, os educadores podem concentrar esforços em áreas específicas onde os alunos apresentam maior dificuldade.

Engajamento e Motivação: A gamificação, potencializada pela IA, incentiva os alunos a se engajarem mais ativamente no aprendizado. Elementos como *ranking*s, conquistas e desafios personalizados tornam o processo educacional mais atrativo, especialmente para crianças do Ensino Fundamental 1, que respondem positivamente a estímulos lúdicos.

Preparação para o Futuro: A integração dessas tecnologias prepara os alunos para lidar com tecnologias emergentes e práticas avançadas de segurança digital desde cedo. Isso os posiciona como cidadãos mais conscientes e preparados para enfrentar os desafios do mundo digital.

2.4.2. Desafios e Limitações

Apesar dos benefícios significativos, a integração de IA e laboratórios virtuais no ensino de Segurança da Informação apresenta desafios que precisam ser abordados para garantir sua eficácia e acessibilidade.

Alto Custo de Implementação: A implementação de sistemas de IA e laboratórios virtuais requer investimentos substanciais em tecnologia, infraestrutura e manutenção. Muitos *softwares* de IA e plataformas de laboratório virtual possuem licenças caras, o que pode limitar seu uso em escolas públicas e instituições com orçamentos reduzidos.

Necessidade de Formação dos Professores: Para que a integração seja bem sucedida, os educadores precisam ser capacitados para utilizar essas tecnologias de maneira eficaz. Isso inclui entender como funcionam os sistemas de IA, como configurar e gerenciar laboratórios virtuais, e como interpretar os dados gerados pelas ferramentas. Sem a formação adequada, há o risco de as tecnologias serem subutilizadas ou aplicadas de forma incorreta.

Acessibilidade em Escolas com Recursos Limitados: Muitas escolas, especialmente em regiões menos favorecidas, enfrentam desafios relacionados à falta de equipamentos adequados, como computadores e conexões de internet de alta qualidade. Isso limita o acesso aos laboratórios virtuais e às ferramentas de IA, criando um fosso digital entre alunos de diferentes contextos socioeconômicos.

Complexidade de Uso: Embora as ferramentas de IA sejam projetadas para facilitar o aprendizado, sua interface e funcionamento podem ser complicados para crianças muito novas ou professores menos familiarizados com tecnologia. Isso exige que as plataformas sejam intuitivas e adaptadas à faixa etária e ao nível de experiência dos usuários.

Riscos de Dependência Tecnológica: Uma preocupação associada ao uso intensivo de IA e laboratórios virtuais é a possível dependência excessiva dessas ferramentas. Embora sejam excelentes auxiliares no ensino, é importante garantir que os alunos também desenvolvam habilidades analíticas e práticas que não dependam exclusivamente da tecnologia.

Privacidade e Segurança dos Dados: Ferramentas de IA e laboratórios virtuais muitas vezes coletam dados dos alunos para personalizar a experiência de aprendizado. É fundamental garantir que esses dados sejam protegidos e usados de forma ética, especialmente quando se trata de crianças, que são mais vulneráveis a violações de privacidade.

Desafios na Avaliação de Resultados: Mensurar o impacto real da integração de IA e laboratórios virtuais no aprendizado pode ser complicado. Embora existam métricas para avaliar o desempenho técnico, os efeitos no desenvolvimento de habilidades interpessoais e na conscientização digital podem ser mais difíceis de quantificar.

A integração de IA e laboratórios virtuais no ensino de Segurança da Informação apresenta um enorme potencial para transformar a educação digital desde os primeiros anos escolares. No entanto, é essencial abordar os desafios associados a essa implementação para garantir que os benefícios sejam amplamente acessíveis. Com investimentos adequados, formação docente e a criação de plataformas inclusivas, essa abordagem pode preparar uma nova geração de cidadãos digitais para navegar e proteger-se em um mundo cada vez mais conectado.

3 METODOLOGIA

Ensinar Segurança da Informação para crianças exige uma abordagem que considere tanto o estágio de desenvolvimento cognitivo quanto o contexto sociocultural dos alunos. No Ensino Fundamental 1, é essencial utilizar estratégias pedagógicas que combinem ludicidade, interatividade e práticas concretas para garantir a assimilação de conceitos e a aplicação no cotidiano. Essa seção apresenta metodologias

e atividades que se destacam pela eficiência em envolver e capacitar crianças no tema da segurança digital (We Live Security, 2024).

3.1. Abordagens Pedagógicas Eficientes

Uma abordagem pedagógica eficiente para o ensino de Segurança da Informação deve partir do princípio de que as crianças aprendem melhor por meio de experiências práticas e contextuais. Nessa perspectiva, estratégias como gamificação, aprendizado baseado em projetos e metodologias ativas têm se mostrado especialmente eficazes.

Gamificação no Ensino: A gamificação transforma o aprendizado em uma experiência lúdica, utilizando elementos de jogos como pontuação, níveis e recompensas para engajar os alunos. Por exemplo, ao ensinar a importância de criar senhas seguras, as crianças podem participar de um jogo onde acumulam pontos ao identificar vulnerabilidades em senhas fictícias e sugerir melhorias. Essa abordagem torna o aprendizado mais divertido e memorável, incentivando a participação ativa (Mizuno, 2024).

Histórias Interativas: Histórias interativas são outra ferramenta poderosa para ensinar conceitos abstratos. Narrativas que apresentam personagens enfrentando ameaças cibernéticas, como *phishing* ou *malwares*, ajudam as crianças a contextualizar o problema e entender a importância das práticas de segurança. Ao decidir como os personagens devem agir, os alunos exercitam o pensamento crítico e a tomada de decisão (ESET, 2024).

Aprendizado Baseado em Projetos: No aprendizado baseado em projetos, os alunos trabalham em equipes para resolver problemas reais ou simulados. Por exemplo, eles podem criar um guia digital para outros estudantes sobre como navegar na internet de maneira segura. Esse método incentiva a colaboração, a pesquisa e o desenvolvimento de habilidades práticas, além de reforçar os conceitos de segurança.

Uso de Tecnologia como Meio de Ensino: Tecnologias como aplicativos educativos, ferramentas de simulação e laboratórios virtuais permitem que as crianças experimentem os conceitos de segurança em ambientes controlados. Esses recursos são fundamentais para aproximar o conteúdo da realidade digital dos alunos, especialmente em um contexto onde o uso de dispositivos eletrônicos é cada vez mais comum (UFRN, 2024).

Aprendizagem Baseada em Problemas (PBL): No PBL, os alunos são expostos a situações-problema relacionadas à Segurança da Informação e são incentivados a encontrar soluções. Por exemplo, podem ser apresentados a um caso fictício de roubo de identidade e desafiados a identificar como isso ocorreu e como prevenir situações semelhantes.

Integração Multidisciplinar: Uma abordagem interdisciplinar também pode enriquecer o ensino. A Segurança da Informação pode ser vinculada a outras disciplinas, como matemática (para ensinar conceitos de criptografia) ou ciências (para explorar o impacto da tecnologia na sociedade). Essa integração amplia a visão dos alunos sobre o tema e reforça sua relevância.

Abordagem por Tarefas: A abordagem por tarefas enfatiza o aprendizado por meio de atividades autênticas e contextualizadas, conectando teoria e prática de forma significativa. No ensino de Segurança da Informação, isso pode ser feito por meio de desafios práticos, como a criação de um conjunto de boas práticas para o uso seguro da internet em casa e na escola. Dessa forma, as crianças não apenas aprendem os conceitos, mas também os aplicam em seu cotidiano, tornando o aprendizado mais relevante e eficaz.

3.2. Atividades Práticas e Lúdicas

Para crianças do Ensino Fundamental 1, atividades práticas e lúdicas são essenciais para reforçar o aprendizado. Elas permitem que os alunos experimentem os conceitos de forma concreta, tornando o aprendizado mais tangível e relevante.

Criação de Senhas Seguras com Dinâmicas de Palavras: Uma atividade comum é ensinar as crianças a criar senhas seguras usando combinações de palavras, números e símbolos. Pode-se propor que cada aluno crie uma senha baseada em algo que eles gostem, como "Cachorro123@", e depois discutir por que essa senha é mais segura do que outras mais simples. Essa dinâmica mostra a importância de escolher senhas fortes e fáceis de lembrar.

Simulações de Ataques Cibernéticos Controlados: Em um ambiente controlado, os alunos podem simular ataques cibernéticos básicos e aprender a defender-se deles. Por exemplo, podem experimentar como um vírus afeta arquivos digitais em uma simulação e, em seguida, descobrir maneiras de prevenir esse tipo de ataque. Isso ajuda a entender o impacto das ameaças cibernéticas e a importância de práticas preventivas.

Resolução de Desafios em Jogos Educativos: Jogos educativos, como desafios de "capturar a bandeira" no ciberespaço, são atividades lúdicas que envolvem os alunos em um processo de resolução de problemas. Eles podem ser desafiados a proteger um sistema fictício contra invasores ou identificar falhas em um ambiente digital. Essas atividades estimulam o pensamento estratégico e ensinam conceitos técnicos de maneira acessível.

Atividades Artísticas e Criativas: Incorporar atividades artísticas, como a criação de cartazes ou histórias em quadrinhos sobre segurança na internet, permite que os alunos expressem o que aprenderam de forma criativa. Além disso, essas atividades podem ser usadas para conscientizar outras crianças e até mesmo a comunidade escolar.

Simulações de Cenários Cotidianos: Apresentar cenários do dia a dia, como receber um e-mail suspeito ou encontrar um USB desconhecido, ajuda os alunos a relacionar o conteúdo com suas experiências pessoais. Após a simulação, é possível discutir as melhores práticas de segurança para cada situação.
Exploração de Ferramentas Tecnológicas: Introduzir as crianças a ferramentas simples de segurança, como gerenciadores de senhas ou verificadores de autenticidade de e-mails, mostra que existem recursos tecnológicos disponíveis para protegê-las. Isso também incentiva o uso consciente e responsável da tecnologia.

Colaboração com a Família: Envolver os pais ou responsáveis nas atividades ajuda a reforçar os aprendizados em casa. Uma tarefa pode incluir ensinar os familiares a identificar sites seguros ou criar senhas fortes, promovendo a conscientização além do ambiente escolar.

Competição de Segurança: Organizar competições saudáveis, onde os alunos demonstram habilidades adquiridas, pode ser um grande motivador. Por exemplo, eles podem competir para ver quem resolve mais rapidamente um desafio de segurança digital.

Essas abordagens pedagógicas e atividades práticas são fundamentais para tornar o ensino de Segurança da Informação acessível e relevante para crianças do Ensino Fundamental 1. Ao combinar ludicidade, tecnologia e experiências práticas, é possível capacitar os alunos a adotarem comportamentos seguros no ambiente digital e desenvolverem uma base sólida de conhecimentos para o futuro.

4 RESULTADOS E DISCUSSÃO

A aplicação de atividades práticas com o uso de Inteligência Artificial (IA) e laboratórios virtuais no ensino de Segurança da Informação para crianças do Ensino Fundamental 1 tem demonstrado resultados promissores. Essas iniciativas aproximam os alunos do mundo real, proporcionando uma experiência de aprendizado ativa e envolvente. Nesta seção, serão apresentados estudos de caso e exemplos que ilustram como a combinação de IA e laboratórios virtuais pode transformar o ensino de segurança digital.

4.1 Exemplos de Atividades com IA e Laboratórios Virtuais Simulação de Phishing em Ambientes Virtuais

Uma das atividades mais eficazes no ensino de Segurança da Informação é a simulação de ataques de *phishing*. Em um ambiente virtual controlado, os alunos recebem e-mails fictícios com características típicas de *phishing*, como *links* suspeitos, erros de ortografia ou ofertas tentadoras. A tarefa deles é identificar os elementos que tornam o e-mail suspeito. Após a atividade, uma análise coletiva dos resultados permite discutir as boas práticas para evitar cair nesse tipo de armadilha. Essa abordagem combina aprendizado prático com o desenvolvimento do pensamento crítico, fundamental para a segurança digital.

Uso de Assistentes de IA para Explicação Interativa: Assistentes virtuais baseados em IA, como *chatbots* educacionais, têm sido usados para responder perguntas sobre Segurança da Informação de maneira interativa e personalizada. Os alunos podem fazer perguntas como "O que é uma senha forte?" ou "Como posso saber se um site é seguro?", e o assistente fornece explicações detalhadas em uma linguagem acessível. Essa ferramenta permite que os alunos aprendam no próprio ritmo, reforçando o conteúdo sempre que necessário. Além disso, os assistentes de IA podem gerar cenários de prática com base nas dificuldades individuais dos alunos, criando um ambiente de aprendizado adaptativo.

Jogos Gamificados Baseados em IA: Plataformas educacionais que utilizam IA para ajustar o nível de dificuldade dos desafios de acordo com o progresso dos alunos têm se destacado no ensino de Segurança da Informação. Um exemplo é um jogo onde os alunos precisam proteger um sistema virtual de ataques simulados. À medida que demonstram maior domínio do conteúdo, os desafios se tornam mais complexos, incentivando o aprendizado contínuo. Esse tipo de abordagem não apenas engaja os alunos, mas também permite uma avaliação constante do desempenho e das áreas que precisam ser reforçadas (Bitfindeis, 2024).

Laboratórios Virtuais de Detecção de Ameaças: Em laboratórios virtuais, os alunos podem explorar cenários em que sistemas fictícios apresentam vulnerabilidades. Por exemplo, eles podem ser encarregados de identificar senhas fracas, proteger informações confidenciais ou configurar um *firewall* básico. Com o suporte de ferramentas de IA, o laboratório fornece *feedback* imediato sobre as ações tomadas, explicando os impactos das escolhas feitas. Essa experiência prática ajuda os alunos a internalizar os conceitos de segurança e entender sua aplicação prática (Viana Júnior, 2017).

Atividades de Criptografia com IA: Uma atividade prática interessante é a exploração de conceitos de criptografia. Usando um laboratório virtual, os alunos podem experimentar a criação e a quebra de mensagens codificadas. A IA pode ser usada para gerar desafios personalizados, como decifrar mensagens criptografadas com diferentes níveis de complexidade. Isso não só ensina os fundamentos da criptografia, mas também mostra sua importância na proteção da informação.

Treinamento de Resposta a Incidentes: Outra aplicação prática é o treinamento em resposta a incidentes de segurança. Em um ambiente virtual, os alunos são expostos a um ataque simulado, como um *ransomware* fictício, e precisam tomar medidas para mitigar os danos. Com o suporte da IA, eles recebem dicas e orientações durante o processo, permitindo que aprendam com seus erros. Essa atividade prepara os alunos para agir de forma rápida e eficiente diante de ameaças reais.

Exploração de Redes Seguras em Simulações: Atividades que envolvem a configuração de redes seguras em laboratórios virtuais também são relevantes. As crianças podem aprender sobre a importância de redes Wi-Fi protegidas e como configurar senhas adequadas para roteadores. A IA pode avaliar as configurações feitas pelos alunos e sugerir melhorias, tornando a atividade mais interativa e educativa.

Campanhas Educativas Simuladas: Outra abordagem é pedir que os alunos criem campanhas educativas para conscientizar outros colegas sobre práticas seguras na internet. Usando laboratórios virtuais, eles podem desenvolver materiais interativos, como pôsteres digitais ou vídeos explicativos. A IA pode ajudar fornecendo modelos prontos ou avaliando a clareza e eficácia do conteúdo produzido.

Exploração de Identidade Digital e Privacidade: Em um ambiente simulado, os alunos podem aprender sobre o conceito de identidade digital. Por exemplo, podem analisar perfis fictícios de redes sociais e identificar quais informações não devem ser compartilhadas publicamente. A IA pode destacar boas práticas e corrigir possíveis equívocos durante a atividade.

Integração com o Mundo Real: Após a conclusão das atividades em laboratórios virtuais, os alunos são incentivados a aplicar o que aprenderam em situações do dia a dia, como ensinar um parente a configurar autenticação em duas etapas ou revisar as configurações de privacidade em redes sociais. Essa transferência de aprendizado para o mundo real consolida os conceitos e amplia o impacto do ensino.

Esses exemplos de atividades demonstram como a integração de IA e laboratórios virtuais no ensino de Segurança da Informação pode promover um aprendizado ativo, adaptativo e relevante para as crianças do Ensino Fundamental 1. Além de fortalecer as habilidades digitais, essas experiências preparam os alunos para enfrentar os desafios de um mundo cada vez mais conectado (5Rights Foundation, 2024).

5 CONSIDERAÇÕES FINAIS

O ensino de Segurança da Informação no Ensino Fundamental 1 tem ganhado relevância em um mundo cada vez mais digitalizado. Crianças, como usuárias ativas de dispositivos conectados, enfrentam uma série de riscos que tornam indispensável o desenvolvimento de competências críticas para a navegação segura. Este estudo destacou como a combinação de Inteligência Artificial (IA) e laboratórios virtuais pode transformar esse ensino, fornecendo ferramentas que promovem a aprendizagem interativa e adaptativa (Lunetas, 2024).

Uma das principais conclusões deste trabalho é que a IA e os laboratórios virtuais oferecem um potencial significativo para tornar o ensino de Segurança da Informação mais acessível e eficaz. A IA desempenha um papel crucial ao personalizar o aprendizado, ajustando os desafios e o conteúdo às necessidades individuais dos alunos. Isso é especialmente importante para crianças do Fundamental 1, cuja compreensão varia amplamente em função de fatores como idade, maturidade e experiências prévias com tecnologia.

Os laboratórios virtuais, por sua vez, proporcionam um ambiente seguro para que os alunos experimentem conceitos complexos sem o risco de consequências negativas. A prática em cenários simulados,

como a identificação de ameaças e a criação de senhas seguras, mostrou-se eficaz no fortalecimento da retenção de conhecimento e na construção de habilidades práticas.

Outro ponto de destaque foi a relevância de atividades lúdicas e interativas no engajamento das crianças. Jogos educativos, simulações de *phishing* e a exploração de redes seguras são exemplos de como as ferramentas tecnológicas podem ser usadas para transformar conceitos abstratos em experiências concretas e significativas. Apesar de suas vantagens, a implementação dessas tecnologias também apresenta desafios, como custos elevados, a necessidade de formação específica para professores e limitações de infraestrutura em algumas escolas. Esses fatores devem ser considerados para garantir a viabilidade e a equidade na aplicação dessa abordagem em larga escala.

Embora este estudo tenha fornecido *insights* importantes sobre o potencial da IA e dos laboratórios virtuais no ensino de Segurança da Informação, ainda há muito a ser explorado. Futuros estudos podem se concentrar em áreas específicas para maximizar o impacto dessas tecnologias na educação básica.
Um dos principais desafios apontados é o custo elevado associado à implementação de laboratórios virtuais e sistemas de IA. Pesquisas futuras poderiam investigar métodos mais acessíveis, como o uso de plataformas de código aberto, parcerias com empresas de tecnologia ou o desenvolvimento de ferramentas simplificadas que mantenham a eficácia sem comprometer o orçamento.

A formação dos professores é outro aspecto essencial para o sucesso dessa abordagem. Pesquisas futuras devem explorar estratégias para desenvolver programas de treinamento que sejam acessíveis e eficazes, permitindo que os professores se sintam confiantes em usar ferramentas tecnológicas no ensino de Segurança da Informação.

Embora as vantagens imediatas da integração de IA e laboratórios virtuais sejam claras, é importante entender como essas tecnologias influenciam a aprendizagem e o comportamento das crianças a longo prazo. Estudos longitudinais podem avaliar, por exemplo, se os alunos continuam aplicando práticas seguras na internet ao longo de suas vidas.

Pesquisas futuras também podem focar em garantir que essas tecnologias sejam acessíveis a todas as crianças, independentemente de sua localização geográfica ou condição socioeconômica. Isso inclui explorar como adaptar a abordagem para escolas com infraestrutura limitada ou acesso restrito à internet.

Outra área promissora para pesquisa é a evolução de jogos educativos e simulações baseados em IA. Estudos podem investigar como melhorar a interatividade e o engajamento, bem como integrar sistemas que monitoram o progresso do aluno em tempo real, oferecendo suporte direcionado para lacunas específicas no aprendizado.

Um aspecto ainda pouco explorado é como integrar o ensino de Segurança da Informação de forma mais orgânica no currículo escolar. Pesquisas futuras podem investigar maneiras de combinar essas lições com disciplinas como matemática, ciências e habilidades digitais, criando um aprendizado interdisciplinar mais coeso. Por fim, um campo de pesquisa relevante é a colaboração entre escolas, famílias e comunidades para fortalecer a educação em Segurança da Informação. Estudos podem explorar como envolver os pais no processo educativo e promover uma cultura de segurança digital que vá além da sala de aula.

A integração de IA e laboratórios virtuais no ensino de Segurança da Informação é uma abordagem promissora que pode preparar as crianças para navegar com segurança em um mundo digital cada vez mais complexo. No entanto, seu sucesso depende de esforços contínuos para superar desafios e garantir que

essas tecnologias sejam implementadas de forma inclusiva e sustentável. As recomendações apresentadas servem como ponto de partida para explorar o vasto potencial desse campo, destacando a importância de unir inovação tecnológica e práticas pedagógicas eficazes para transformar a educação básica.

REFERÊNCIAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). **Proteção On-line Infantil**. Disponível em: https://www.gov.br/anatel/pt-br/consumidor/habilidades-digitais/protecao-on-line-infantil. Acesso em: 5 dez. 2024.

AMAZON. **Segurança Digital para Crianças e Adolescentes:** Guia Completo. Disponível em: https://www.amazon.com.br/Segurança-Digital-para-Crianças-Adolescentes/dp/B0D77Q4HVC. Acesso em: 13 dez. 2024.

BIBLIOTECA DE SEGURANÇA. **Proteção de Crianças e Adolescentes na Internet**. Disponível em: https://www.bibliotecadeseguranca.com.br/livros/protecao-de-criancas-e-adolescentes-na-internet/. Acesso em: 8 dez. 2024.

BITFINDEIS. **Segurança para crianças**. Disponível em: https://www.bitfindeis.com/p/seguranca-para-criancas.html. Acesso em: 5 dez. 2024.

ESET. **Livros infantis educam sobre cibersegurança**. Disponível em: https://www.welivesecurity.com/pt/safe-kids/livros-infantis-educam-sobre-ciberseguranca/. Acesso em: 4 dez. 2024.

JORNAL O CANDEEIRO. **Autora infantil lança livro que ensina crianças a navegar com segurança na era digital**. Disponível em: https://www.jornalocandeeiro.com.br/noticia-35982-autorainfantillancalivroqueensinacriancasanavegarcomsegurancanaeradigital. Acesso em: 12 dez. 2024.

LUNETAS. **6 livros para conversar com as crianças sobre o uso de tecnologia**. Disponível em: https://lunetas.com.br/livros-para-conversar-com-as-criancas-sobre-o-uso-de-tecnologia/. Acesso em: 9 dez. 2024.

MEMÓRIA FORENSE. **Crianças no Ambiente Digital:** Riscos, Oportunidades e Proteção. Disponível em: https://www.memoriaforense.com/produtos/livro-criancas-no-ambiente-digital/. Acesso em: 15 dez. 2024.

MIZUNO, E. **Crianças no Ambiente Digital:** Riscos, Oportunidades e Proteção. Editora Mizuno, 2024. Disponível em: https://www.editoramizuno.com.br/products/livro-criancas-no-ambiente-digital-2024. Acesso em: 4 dez. 2024.

PROFISSIONAIS TI. **A importância da conscientização sobre Segurança da Informação na Educação Infantil**. Disponível em: https://s.profissionaisti.com.br/wp-content/uploads/2013/06/Artigo-Tecnologia-Educacao-Infantil.pdf. Acesso em: 13 dez. 2024.

SANTOS, A. L. **Segurança da Informação no Contexto Escolar**. Disponível em: https://editorarealize.com.br/artigo/visualizar/80791. Acesso em: 8 dez. 2024.

SCHELENZ, L.; STAPF, I.; HEESEN, J. **Security for Children in the Digital Society – A Rights-based and Research Ethics Approach**. arXiv preprint arXiv:2309.12340, 2023. Disponível em: https://arxiv.org/abs/2309.12340. Acesso em: 8 dez. 2024.

SILVA, C. A. **Análise sobre o uso da Segurança da Informação na Internet pelos jovens**. Disponível em: https://www.ensinosuperior.sed.sc.gov.br/wp-content/uploads/2015/01/Artigo-Carlos-Alberto-Conceição.pdf. Acesso em: 4 dez. 2025.

UFMT. **Plataformas Digitais, Crianças e Adolescentes**. Disponível em: https://periodicoscientificos.ufmt.br/ojs/index.php/educacaopublica/article/view/13381. Acesso em: 12 dez. 2024.

UFRN. **Segurança da Informação no Âmbito Escolar**. Disponível em: https://repositorio.ufrn.br/handle/123456789/39691. Acesso em: 12 dez. 2024.

UFSC. **Segurança da Informação no Contexto Escolar**. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/168731/TCC%20Santos.pdf?isAllowed=y&sequence=1. Acesso em: 10 dez. 2024.

VIANA JUNIOR, E. W. S. **Ensino de Noções Básicas de Segurança da Informação nas Escolas Brasileiras**. ResearchGate, 2017. Disponível em: https://www.researchgate.net/publication/320969758_Ensino_de_Nocoes_Basicas_de_Seguranca_da_Informacao_nas_Escolas_Brasileiras. Acesso em: 9 dez. 2024.

WE LIVE SECURITY. **Livros infantis educam sobre cibersegurança**. Disponível em: https://www.welivesecurity.com/pt/safe-kids/livros-infantis-educam-sobre-ciberseguranca/. Acesso em: 15 dez. 2024.

5Rights Foundation. **Como tornar realidade a segurança online para crianças**. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2022/05/como-tornar-realidade-seguranca-on-line-para-criancas-1.pdf. Acesso em: 2 dez. 2024.