INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS TERESINA ZONA SUL
CURSO LICENCIATURA EM COMPUTAÇÃO

JOÃO PEDRO MENDES DE OLIVEIRA

CIBERSEGURANÇA: UM RELATO DE EXPERIÊNCIA SOBRE O CURSO NO MODELO ADDIE APLICADO NO CEEP - JOSÉ PACIFICO

TERESINA
2024

JOÃO PEDRO MENDES DE OLIVEIRA

CIBERSEGURANÇA: UM RELATO DE EXPERIÊNCIA SOBRE O CURSO NO MODELO ADDIE APLICADO NO CEEP - JOSÉ PACIFICO

Projeto de Pesquisa apresentado como exigência parcial para aprovação na Disciplina TCC-I do Curso de Licenciatura em Computação do Instituto Federal de Educação, Ciência e Tecnologia do Piauí. Campus Teresina Zona Sul.
Professor(a) Orientador (a): Mestra Francisca Ocilma Mendes Monteiro

Professor(a) coorientador(a):Keoma de Sousa Coelho

TERESINA
2024

CIBERSEGURANÇA: UM RELATO DE EXPERIÊNCIA SOBRE O CURSO NO MODELO ADDIE APLICADO NO CEEP - JOSÉ PACIFICO

João Pedro Mendes de Oliveira[1]
Professor(a) Orientador (a):Francisca Ocilma Mendes Monteiro[2]
Professor(a) coorientador(a):Keoma de Sousa Coelho[3]

RESUMO

A evolução tecnológica constante trouxe inúmeras melhorias para a sociedade e suas diversas áreas do conhecimento. Contudo, também trouxe desafios, como a falta de conhecimento sobre métodos de proteção no mundo digital Este trabalho relata a experiência de desenvolvimento e aplicação do curso 'Aprendendo a se Proteger na Era Digital', fundamentado no modelo ADDIE, para estudantes do ensino médio integrado ao curso técnico em informática no CEEP José Pacífico. O objetivo foi capacitar os estudantes em práticas de cibersegurança, explicando conceitos alinhados à realidade dos alunos e conscientizando-os sobre os riscos digitais, abordando temas como privacidade online, ameaças cibernéticas e medidas preventivas. A pesquisa, de natureza qualitativa e metodologia de pesquisa-ação, envolveu observações em sala de aula, registros em diários de campo e aplicação de questionário. Os resultados indicaram um aumento significativo no engajamento dos alunos na adoção de boas práticas de segurança digital, bem como a formação de cidadãos mais conscientes e preparados para os desafios da era tecnológica, evidenciando a eficácia do curso.

Palavras-chave: Cibersegurança. Educação Digital; Modelo ADDIE; Segurança da Informação.

ABSTRACT

With the advent of constant technological evolution, numerous improvements have been brought to society and its various fields of knowledge. However, alongside this great progress came many challenges, one of which is the lack of knowledge about protection methods in the digital world. This paper presents an experience report on the development and implementation of the course "Learning to Protect Yourself in the Digital Age," based on the ADDIE model, for high school students enrolled in the integrated technical program in computer science at the State Center for Professional Education (CEEP) José Pacífico. The goal was to equip students with cybersecurity practices, explaining these concepts while aligning them with the students' realities and raising awareness about digital risks. The course addressed topics such as online privacy, cyber threats, and preventive measures.

[1] Graduando de Licenciatura em Computação. Instituto Federal de Educação, Ciência e Tecnologia do Piauí.Campus Teresina Zona Sul. E-mail: 20191LINF0310@aluno.ifpi.edu.br.
[2] Professora Ma. do eixo pedagógico do curso de Licenciatura em Computação. Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Zona Sul. E-mail: ocilma.monteiro@ifpi.edu.br
[3] Professor.Expecialista em segurança. E-mail: koabrasil@gmail.com

The research, qualitative in nature and employing an action research methodology, involved classroom observations, field journal entries, and the application of questionnaires. The results indicated a significant increase in student engagement and the adoption of good digital security practices, demonstrating the course's effectiveness. This study underscores the importance of digital education as a tool for fostering more conscious and prepared citizens to face the challenges of the technological era.

Keywords: Cybersecurity; Digital Education; ADDIE Model; Information Security; Technical Education.

Data de aprovação: 20/12/2024

1 INTRODUÇÃO

Em um mundo cada vez mais interconectado, onde informações sensíveis são transmitidas e armazenadas em redes e plataformas digitais constantemente, é bastante importante relembrar que, conforme Jhosaf Stenberg, dados sensíveis são informações pessoais que, se acessadas ou divulgadas sem autorização, podem gerar prejuízos ao indivíduo, como discriminação, invasão de privacidade ou perdas financeiras. Exemplos incluem dados de saúde, biométricos, financeiros, religiosos e de orientação política (STENBERG, 2021). Nesse contexto, garantir a segurança digital é uma prioridade não apenas para empresas e governos, mas também para instituições de ensino e indivíduos. O relatório anual de segurança da Internet da Cisco (2023), revela um aumento significativo nas ameaças cibernéticas direcionadas a instituições educacionais. Este relatório destaca que, em 2022, as tentativas de ataques de *ransomware*[4] cresceram 40%, com criminosos aprimorando suas táticas para contornar as defesas tradicionais, como conhecimento sobre os principais ataques cibernéticos e ate mesmo conhecimento previo de maneiras para buscar se manter mais seguro no ambiente digital, de escolas e universidades.

Diante dessa realidade, promover um curso de cibersegurança em uma instituição pública de ensino é essencial para contribuir com a formação de alunos, com ênfase na proteção de dados.

A Política Nacional de Cibersegurança (PNCiber), instituída pelo decreto nº

[4] ***Phishing***: Ataque cibernético que visa enganar usuários para obter informações confidenciais, como senhas ou dados financeiros, por meio de mensagens fraudulentas (STENBERG, 2021).

11.856, de 26 de dezembro de 2023, reforça a importância de promover a segurança cibernética no país, incentivando medidas de proteção e a educação sobre o tema (BRASIL, 2023).

Com o uso cada vez mais disseminado da tecnologia entre crianças e adolescentes, torna-se imprescindível garantir sua segurança no ambiente digital, tal como é feito no mundo físico. Isso exige o conhecimento de ferramentas e soluções que proporcionem maior proteção no meio virtual. Em resposta a essa necessidade, foi idealizado um curso de cibersegurança voltado aos alunos do segundo ano do Curso Técnico em Informática Integrado ao ensino médio do Centro Estadual de Educação Profissional - CEEP José Pacífico.

A escolha de uma instituição pública como foco da pesquisa busca capacitar os alunos por meio de práticas de segurança digital aplicadas ao uso cotidiano da internet, incluindo a web, situações offline envolvendo engenharia social e o uso seguro de smartphones. O objetivo foi apresentar métodos e práticas que ajudasse a garantir a segurança durante a navegação e a conscientização dos alunos sobre os riscos no ambiente digital.

A implementação desse curso visou reduzir os riscos associados ao uso da internet, uma necessidade cada vez mais urgente em virtude da crescente adoção de novas tecnologias. Uma vez que, a maioria dos alunos possui celulares e outros dispositivos conectado.

Este trabalho relata as experiências obtidas, enquanto residente, no âmbito do Programa Residência Pedagógica- RP. Programa este, que faz parte da Política de formação de professores da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES. A concepção do curso teve como base as aulas desenvolvidas no programa RP, evidenciando a necessidade de proteção digital." Programa este vinculado ao Curso de Licenciatura em Computação do Instituto Federal de Ciências e Tecnologia do Piauí (IFPI), campus Teresina zona sul.

As atividades foram realizadas durante a regência, em uma escola profissional da zona sudeste de Teresina (PI). O projeto destaca a relevância do tema para a formação dos alunos, abordando conhecimentos e conceitos fundamentais de cibersegurança.

Com o aumento das ameaças cibernéticas, a formação de profissionais capacitados em cibersegurança torna-se imperativa para a proteção de sistemas e a garantia da integridade, confidencialidade e disponibilidade dos dados. Nesse

contexto, a criação de um curso voltado à segurança digital em uma instituição pública é tanto relevante quanto oportuna. O site “TI Inside”[5], por exemplo, reportou um aumento de 35% nos ataques cibernéticos em janeiro de 2023 (TI Inside, 2023), evidenciando a urgência de intervenções que promovam bons hábitos e segurança na internet.

O objetivo geral deste trabalho foi apresentar um relato de experiência sobre o desenvolvimento e a aplicação do curso, no modelo ADDIE, “Aprendendo a se Proteger na Era Digital”, para os alunos do CETI José Pacífico. Os objetivos específicos incluem: planejar o curso seguindo o modelo ADDIE; desenvolver atividades teórico-práticas sobre crimes digitais; ensinar sobre *phishing* e o uso de senhas fortes e únicas; apresentar ferramentas online que auxiliem na compreensão de conceitos de segurança; conscientizar sobre as principais ameaças na internet e avaliar se os alunos adotam práticas mais seguras após o curso.

A cibersegurança é definida como a prática de proteger sistemas, redes e dados digitais de intrusões e acessos não autorizados, com medidas que previnam, mitiguem e respondam a ameaças. De acordo com a Cybersecurity and Infrastructure Security Agency -CISA, a proteção cibernética requer uma combinação de pessoas, processos e tecnologias, incluindo a educação sobre práticas seguras e o uso de defesas automatizadas (CISA, 2023).

Em um mundo onde a tecnologia permeia todos os aspectos da vida, dos negócios às relações pessoais, a consciência sobre os riscos digitais é fundamental. Joseph Steinberg, em ‘Cybersecurity for Dummies’ (Steinberg, 2019), ressalta a importância de entender e enfrentar essas ameaças, capacitando tanto especialistas quanto o público geral na proteção de dados.

2 CIBERSEGURANÇA NA EDUCAÇÃO

A cibersegurança refere-se à prática de salvaguardar sistemas, redes e dados digitais contra intrusões, danos ou acessos não autorizados, implementando medidas de segurança projetadas para prevenir, mitigar e responder a ameaças cibernéticas.

[5] O Site *TI INSIDE*. Portal de notícias especializado em tecnologia da informação, negócios digitais e inovação. Disponível em: https://tiinside.com.br/.

Segundo a Cybersecurity and Infrastructure Security Agency (CISA), a cibersegurança é essencial para proteger a integridade, confidencialidade e disponibilidade das informações. A proteção eficaz depende de uma combinação de pessoas, processos e tecnologia, incluindo a educação de funcionários sobre práticas de segurança e a utilização de tecnologias automatizadas de defesa cibernética (CISA, 2023).

O avanço tecnológico contínuo proporciona um terreno fértil para o surgimento regular de novas formas de ataques cibernéticos, exigindo uma resposta ágil e proativa por parte dos profissionais desta area.

No contexto contemporâneo, marcado pela interdependência tecnológica, desde transações financeiras até a partilha de momentos pessoais online, evidencia-se a relevância da cibersegurança frente aos riscos inerentes à dependência digital. Steinberg (2019), em *Cybersecurity for Dummies*, oferece uma análise pragmática das ameaças cibernéticas, capacitando tanto profissionais quanto leigos a protegerem sistemas e dados. A perspectiva de ter informações financeiras usurpadas ou identidades comprometidas por agentes maliciosos online torna-se inquietante, como destacado no estudo intitulado “O custo da negligência? Ou custo de um ataque?” (Horizontes, 2021). Este estudo sublinha a importância de investimentos em proteção digital, alertando para os custos financeiros e operacionais decorrentes de decisões negligentes e destacando o impacto de eventos como ataques de ransomware, intensificados durante a pandemia.

A cibersegurança, portanto, emerge como um elemento essencial para proteger dados pessoais e assegurar a continuidade das operações empresariais. Empresas em todo o mundo dependem de infraestrutura digital, sendo que ataques cibernéticos podem acarretar perdas financeiras significativas e danos à reputação.

No âmbito governamental, a segurança nacional está intrinsecamente ligada à proteção de sistemas críticos, como os de energia, saúde e defesa, frente a potenciais ataques que poderiam comprometer a segurança e o bem-estar dos cidadãos. Além disso, iniciativas como o Marco Civil da Internet (Lei nº 12.965/2014), criada para regulamentar o uso da internet no Brasil, reforçam a importância da cibersegurança. A legislação estabelece princípios fundamentais, como a neutralidade da rede e a proteção à privacidade dos usuários, promovendo um equilíbrio entre inovação tecnológica e direitos individuais.

No contexto educacional, destaca-se a aplicação do modelo Análise, Design, Desenvolvimento, Implementação e Avaliação- ADDIE no design instrucional de

cursos voltados à cibersegurança. Conforme Filatro (2008), o modelo ADDIE estrutura o desenvolvimento de experiências de ensino eficazes, guiando desde a análise das necessidades educacionais até a avaliação dos resultados. A aplicação desse modelo busca otimizar o processo de ensino, assegurando que os objetivos educacionais sejam alcançados e contribuindo para a formação de alunos conscientes e preparados para enfrentar os desafios da era digital.

2.1 DESIGN INSTRUCIONAL - MODELO ADDIE

É uma abordagem sistemática para desenvolver experiências de ensino mais eficazes. Envolve criação de materiais em ambientes de ensino que atendam às necessidades específicas dos alunos e aos objetivos educacionais. Nesta proposta, buscou-se usar as diretrizes do modelo para desenvolver o curso de Cibersegurança intitulado “Cibersegurança: protegendo-se na era digital para os alunos do Curso Técnico em Informática Integrado ao ensino médio do Centro Estadual de Educação Profissional (CEEP) José Pacífico de Moura Neto.

O design instrucional envolve uma variedade de processos, incluindo análise das necessidades de ensino, definição de metas educacionais, seleção e organização de conteúdo, desenvolvimento de estratégias de ensino, criação de materiais educacionais, implementação do ambiente de ensino e avaliação do desempenho dos alunos.

Conforme Filatro (2008), a metodologia ADDIE pode ser aplicada seguindo a dinâmica descrita a seguir:

Análise: é a fase inicial do processo de design instrucional. Durante essa etapa, os designers pedagógicos identificam as necessidades de ensino, os objetivos educacionais e os requisitos do público-alvo. Isso inclui avaliar o contexto educacional, analisar as características dos alunos, identificar recursos disponíveis e definir critérios de sucesso. Em suma, a análise no método ADDIE envolve compreender o problema educacional e encontrar uma solução.

Design: desenvolvimento de um plano de ensino detalhado, incluindo metas específicas de aprendizagem, estratégias de ensino, seleção de conteúdo, atividades de aprendizagem e métodos de avaliação.

Desenvolvimento: No método ADDIE, o estágio de desenvolvimento envolve a criação ou adaptação de materiais de ensino de acordo com o plano estabelecido na fase de design. Isso inclui a produção de recursos educacionais, como slides,

vídeos, textos, atividades interativas, jogos educacionais, entre outros. O objetivo é transformar o plano de ensino em materiais concretos que serão usados para ensinar e facilitar a aprendizagem dos alunos. Essa etapa é crucial para garantir que os materiais de ensino sejam de alta qualidade e atendam aos objetivos de aprendizagem definidos na fase de design.

Implementação: a implementação é a etapa em que o plano de ensino é colocado em prática e os materiais de ensino são entregues aos alunos. Isso pode incluir dar aulas, oferecer cursos online, distribuir materiais impressos, entre outras formas de fornecer o ensino planejado. Durante essa fase, os instrutores ou facilitadores trabalham para garantir que os alunos tenham acesso aos recursos e suporte necessários para alcançar os objetivos de aprendizagem estabelecidos no design pedagógico. Além disso, é comum fazer monitoramento e ajustes conforme necessário para garantir que a implementação seja eficaz e atenda às necessidades dos alunos.

Avaliação: aa etapa de avaliação do método, é feita uma análise do desempenho do curso ou material de ensino. Isso inclui verificar/perceber se as metas de aprendizagem foram alcançadas e se os conhecimentos foram aplicados de maneira prática. Com base nessa avaliação, ajustes podem ser feitos para melhorar futuras implementações do design instrucional.

O objetivo final do design instrucional é criar experiências de ensino envolventes e capazes de promover o sucesso do aluno. Isso pode incluir a seleção e organização de conteúdo, o desenvolvimento de estratégias de ensino e aprendizagem, o uso de tecnologia educacional e a avaliação do impacto do ensino.

Em resumo, o design instrucional busca otimizar o processo de ensino e aprendizagem para alcançar os melhores resultados possíveis.

Diante do exposto, optou-se pela aplicabilidade do curso utilizando a metodologia ADDIE.

A Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto nº 10.222/2020, estabelece diretrizes para proteger a infraestrutura cibernética do Brasil, promover a defesa cibernética e criar um ambiente seguro para o desenvolvimento econômico e social. Entre suas principais orientações estão a promoção da cultura de segurança cibernética, o fortalecimento da capacitação e formação de profissionais, o incentivo à inovação tecnológica nacional, a proteção de infraestruturas críticas e a articulação entre governo, setor privado e academia.

Essas diretrizes destacam a importância de incluir a cibersegurança na educação, desde a conscientização nas escolas até a formação técnica e superior, alinhando os cursos às necessidades do mercado e às políticas nacionais. Além disso, fomentam a pesquisa e o desenvolvimento de soluções inovadoras, essenciais para a soberania digital do país. Alinhar os cursos à PNCiber é fundamental para formar uma sociedade ciberconsciente, fortalecer a segurança nacional e atender à crescente demanda por especialistas na área.

3 METODOLOGIA

3.1 MODALIDADE DE PESQUISA

Esta pesquisa busca planejar e aplicar um curso sobre cibersegurança destinado a alunos do Curso Técnico em Informática Integrado ao ensino médio de uma instituição de educação profissional situada na região sudeste da cidade de Teresina (PI). Trata-se de uma pesquisa qualitativa, que se distingue pela ênfase na compreensão profunda e contextual dos fenômenos sociais, priorizando significados, experiências e contextos sociais. De acordo com Anselm Strauss (1987), a pesquisa qualitativa difere da quantitativa ao privilegiar a interpretação e a contextualização em detrimento da quantificação e generalização. Para isso, utiliza métodos como observação participante para capturar as nuances e os significados dos eventos sociais.

A pesquisa adota uma abordagem qualitativa para explorar, em profundidade, as experiências de aprendizagem dos alunos durante a aplicação do curso proposto e a prática pedagógica do professor responsável. Quanto ao método de procedimento, optou-se pela metodologia de pesquisa-ação, conforme proposta por Michel Thiollent (2011), que integra pesquisa e prática de forma colaborativa, envolvendo os participantes no processo investigativo. A pesquisa-ação tem uma rotina que apresenta três ações principais: observar para ter informações e construir um cenário que possa pensar, explorar, analisar e interpretar os fatos; e agir, implementando e avaliando as ações.

Os resultados foram discutidos quanto à sua relevância para a prática profissional, melhorias no curso e futuras iniciativas educacionais em cibersegurança. Com essa abordagem metodológica, foi possível obter uma compreensão significativa sobre a eficácia do curso e sua contribuição na formação dos alunos para os desafios do mundo digital.

3.2 INSTRUMENTOS DE COLETA DE DADOS

Os dados foram coletados por meio de observações participante realizadas em sala de aula, registradas em diários de campo. Segundo Falkembach (1987), o diário de campo é um recurso essencial para pesquisadores e educadores, pois incentiva o hábito de observar atentamente, descrever com precisão e refletir sobre os acontecimentos do cotidiano profissional. Nesse registro, anotam-se fatos concretos, fenômenos sociais, experiências do investigador, reflexões e comentários sobre o que foi observado.

A coleta de dados incluiu o registro de observações e reflexões após cada aula, visando compreender o nível de conhecimento dos alunos em relação ao conteúdo ministrado e documentar o desenvolvimento da turma.

Outro instrumento utilizado foi um questionário composto por 10 perguntas que abordava os principais temas apresentados e discutidos durante o curso de cibersegurança. O questionário, segundo (LAKATOS; MARCONI, 2003, p.201) “é um instrumento, constituído por uma série ordenada de perguntas, que devem ser respondidas por escrito”.

Esse questionário foi aplicado aos alunos participantes com o objetivo de analisar o desenvolvimento e identificar avanços nos conhecimentos adquiridos. A análise dos resultados permitiu avaliar o impacto do curso e o grau de melhoria ou não nos conhecimentos dos estudantes, correlacionando-os ao objetivo da pesquisa.

3.3 PARTICIPANTES DA PESQUISA

Os participantes desta pesquisa foram os alunos do segundo ano do Curso Técnico em Informática Integrado ao ensino médio do Centro Estadual de Educação Profissional (CEEP) José Pacífico. A escolha desse público se deve ao fato da turma esta participando das atividades do projeto Residência Pedagógica (RP).

4 RESULTADOS E DISCURSSÕES

A coleta de dados utilizada nesta pesquisa foi realizada por meio de diários de campo, observações em sala de aula como também a aplicação de um questionário ao final do curso. Tornando assim possível desenvolver uma análise qualitativa e detalhada da experiência dos alunos ao longo do curso. A seguir, os resultados

encontrados em cada um dos instrumentos de coleta utilizados.

O curso teve uma carga horária total de 40 horas. As aulas foram realizadas em encontros 20, com duração de 2 horas cada, permitindo uma abordagem mais detalhada dos conteúdos.

4.1.1 Diário de Campo e Observações do tipo participante

O tema principal das aulas sobre cibersegurança, estava sempre alinhado com atividades páticas. Aproveitava o momento para apresentar algumas ferramentas práticas, como um mapa em tempo real mostrando os ataques virtuais em curso e uma ferramenta, como o site "*have i been pwned?*[6]", que serve para verificar se um e-mail já foi comprometido por vazamentos de dados. A apresentação dessas ferramentas despertou grande interesse entre os alunos, que passaram a demonstrar maior atenção ao assunto. Isso resultou em um diálogo produtivo sobre como as empresas identificam e lidam com os ataques virtuais, no qual pude explicar detalhadamente o processo. Refletindo em um aprendizado mais colaborativo e uma construção de conhecimento sobre cibersegurança.

Durante as observações em sala de aula, foi possível perceber um aumento significativo no engajamento por parte dos alunos nas atividades propostas. Os alunos demonstraram um interesse maior nas aulas de simulações de ataques cibernéticos, uma vez que estas atividades eram voltadas para a realidade dos alunos, facilitando uma maior identificação por parte deles.

Foi gratificante perceber o crescente interesse dos alunos por assuntos práticos e demonstrações concretas. Esse entusiasmo foi aproveitado nos demais encontros, buscando sempre proporcionar experiências enriquecedoras e relevantes para o aprendizado.

O ensino para os alunos do segundo ano do ensino médio demonstrou a necessidade do uso de demonstrações práticas para causar mais interesse por parte deles. Outro ponto a ser mencionado é a pré organização do laboratório. Organizar todos os computadores para que eles estejam aptos a utilização no momento da aula mostrou-se de grande necessidade para uma interação mais prática do conteúdo.

O interesse e entusiasmo dos alunos pelo tema foi notável, uma vez que o uso

[6] O site ***HAVE I BEEN PWNED***. Serviço online que permite aos usuários verificar se seus dados pessoais foram comprometidos em violações de segurança. Disponível em: https://haveibeenpwned.com/.

de tecnologia é algo que está presente em todo o momento na vida dos alunos, e a necessidade de compreender, utilizar e proteger o seus dados é de extrema importância. Todos mostravam interesse pelo próximo encontro.

4.1.2 Questionários Aplicados

Os questionários foram aplicados ao final do curso para avaliar o nível de compreensão dos alunos sobre os temas abordados durante o curso. Os resultados indicaram que 85% dos alunos demonstraram uma melhoria significativa no conhecimento sobre boas práticas de segurança digital, como o uso de senhas fortes, autenticação de dois fatores, e os riscos de navegação em sites não seguros. Aproximadamente 75% dos alunos relataram ter adotado novas práticas de segurança após o curso, como o uso de antivírus, atualizações constantes nos aparelhos móveis e a escolha mais criteriosa na composição de suas senhas.

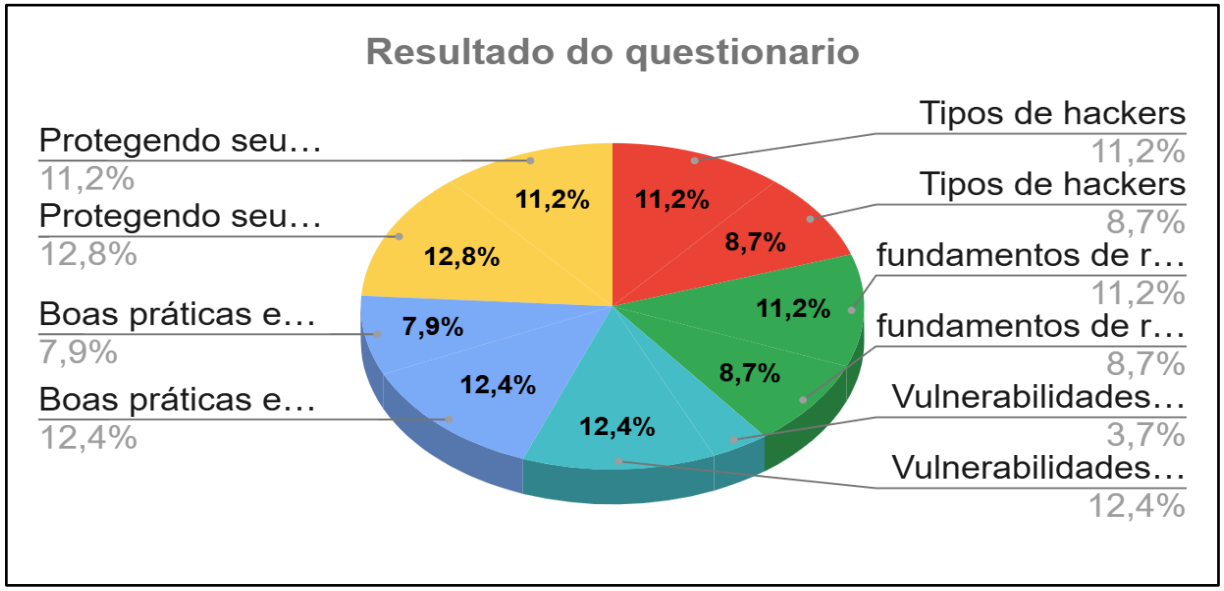
Ademais, o questionário revelou que 70% dos alunos estavam conscientes da importância da cibersegurança no ambiente digital e sua relação direta com a proteção de dados pessoais e financeiros. Essas respostas refletem a eficácia do curso na transmissão de conceitos essenciais sobre segurança no mundo digital.

Quadro 1: Tabulação das respostas questionário aplicado sobre a aprendizagem do curso de Cibersegurança

Questão	Eixo Temático	Acertos	Erros	Total
1	Tipos de hackers	27	5	32
2	Tipos de hackers	21	11	32
3	fundamentos de rede	27	5	32
4	fundamentos de rede	21	11	32
5	Vulnerabilidades e suas características	9	23	32
6	Vulnerabilidades e suas características	30	2	32
7	Boas práticas e mitigação	30	2	32
8	Boas práticas e mitigação	19	13	32
9	Protegendo seu dispositivo móvel	31	1	32
10	Protegendo seu dispositivo móvel	27	5	32

Fonte: Construído pelo autor. 2024

Gráfico 1. Percentual da tabulação das respostas do questionário aplicado sobre a aprendizagem do curso de Cibersegurança.



Fonte: contruído pelo autor 2024.

4.2 Discussão dos Resultados

Os resultados obtidos são consistentes com as evidências encontradas na literatura sobre a importância da cibersegurança na formação educacional. Conforme destacado por Steinberg (2019), e pela *Cybersecurity and Infrastructure Security Agency* (CISA, 2023), a proteção digital se torna uma competência essencial no contexto atual, dada a crescente interdependência tecnológica. A melhoria no conhecimento dos alunos e a adoção de novas práticas de segurança digital indicam que o curso foi eficaz em atender aos objetivos educacionais propostos, alinhando-se com as melhores práticas de ensino descritas no modelo ADDIE.

A abordagem prática adotada, com simulações de cenários reais de ataques cibernéticos, foi identificada como um ponto-chave para o sucesso do curso. Isso está em consonância com a literatura sobre aprendizagem ativa, que enfatiza a importância de experiências práticas para consolidar o conhecimento (Filatro, 2008). As atividades práticas permitiram que os alunos não apenas compreendessem os conceitos teóricos de cibersegurança, mas também os aplicassem de forma concreta, preparando-os para situações reais.

No entanto, o curso também revelou algumas limitações. Embora a maioria dos

alunos tenha demonstrado uma compreensão sólida dos conceitos, 25% dos participantes relataram dificuldades em adotar todas as práticas recomendadas, como o uso de autenticação de dois fatores. Essa resistência pode ser explicada, em parte, pela falta de familiaridade com as ferramentas digitais necessárias ou pela percepção de que essas medidas são excessivas ou difíceis de implementar. Segundo Falkembach (1987), a mudança de comportamento, especialmente no que diz respeito à segurança digital, é um processo gradual que depende tanto da educação quanto da prática constante.

Ademais, os resultados indicam que o curso teve um impacto positivo na conscientização dos alunos sobre os riscos cibernéticos, mas a aplicação de ferramentas mais específicas e avançadas de segurança (como gerenciadores de senhas) poderia ser melhor explorada para fortalecer ainda mais a formação dos alunos.

Ao final, a análise sugere que a metodologia de pesquisa-ação adotada foi eficaz para promover um ambiente de aprendizagem colaborativa, permitindo que tanto os alunos quanto o professor participassem ativamente do processo educativo e do processo de melhoria contínua do curso. Isso reforça a ideia de que a prática pedagógica deve ser dinâmica e adaptativa, sempre em busca de melhorias baseadas na reflexão e no feedback constante, conforme preconizado por Michel Thiollent (2011).

Os seguintes resultados da pesquisa mostrado no **Quadro 2** evidenciam o cumprimento dos objetivos propostos no planejamento e desenvolvimento do curso seguindo o modelo *ADDIE*. O curso foi planejado e estruturado de forma a proporcionar aprendizado prático, com atividades organizadas em cada etapa do modelo. O desenvolvimento das atividades teórico-práticas, especialmente no contexto de crimes digitais, permitiu que os alunos compreendessem conceitos teóricos de forma prática, por meio de oficinas colaborativas e resolução de problemas reais.

Além disso, o curso abordou conteúdos relacionados a ***phishing*** e outros métodos para garantir uma segurança a mais no mundo digital. Como resultado, observou-se uma melhoria significativa no conhecimento dos alunos sobre esses temas e a adoção de práticas de segurança digital mais robustas. Também foram apresentadas ferramentas online, como mapas que mostram ataques virtuais em tempo real e o site "***Have I Been Pwned***", que permite verificar se um e-mail foi

comprometido por vazamentos de dados. Essas ferramentas auxiliaram os alunos a compreenderem melhor a importância da cibersegurança e sua relação com a proteção de dados pessoais e financeiros.

Outro objetivo importante foi a conscientização sobre as principais ameaças na internet e a avaliação de mudanças nos hábitos de segurança dos alunos após o curso. Os resultados demonstraram um aumento na motivação e no engajamento dos participantes, refletido em práticas como o uso de antivírus, atualizações constantes em dispositivos móveis e uma escolha mais criteriosa na criação de senhas. Assim, os dados coletados confirmam o impacto positivo do curso no desenvolvimento de uma cultura de segurança digital.

Quadro 2: objetivos alcançados na pesquisa

Objetivo	Resposta Alcançada	Como foi alcançado
Planejar o curso seguindo o modelo ADDIE	O curso planejado no modelo ADDIE	Desenvolvimento do Curso planejado no modelo proposto proporcionando aprendizado prático.
Desenvolver atividades teórico-práticas sobre crimes digitais;	O curso proporciou uma compreensão prática dos conceitos teóricos abordados.	Participação ativa dos alunos nas oficinas, colaborando e resolvendo problemas práticos.
Ensinar sobre *phishing* e o uso de senhas fortes e únicas;	Conteúdo sobre *phishing* e o uso de senhas fortes e únicas.	A melhoria no conhecimento dos alunos e a adoção de novas práticas de segurança digital.
Apresentar ferramentas online que auxiliem na compreensão de conceitos de segurança;	Ferramentas como um mapa em tempo real mostrando os ataques virtuais em curso e ferramentas, como o have i been pwned para verificar se um e-mail já foi comprometido por vazamentos de dados.	conscientes da importância da cibersegurança no ambiente digital e sua relação direta com a proteção de dados pessoais e financeiros
conscientizar sobre as principais ameaças na internet e avaliar se os alunos adotam práticas	Aumento da motivação e o engajamento dos alunos durante o curso.	A coleta demostrouque os alunos adotaram novas práticas de segurança após o curso, como o uso de antivírus, atualizações constantes

mais seguras após o curso.		nos aparelhos móveis e a escolha mais criteriosa na composição de suas senhas.

Construído pelo autor 2024

Análise: Foi a fase inicial do processo. Durante essa etapa, foi identificada a necessidade da temática, as necessidades de ensino, os objetivos educacionais e os requisitos do público-alvo. O contexto educacional, dispunha dos recursos disponíveis como laboratório com a infra estrutura necessaria para o curso.

Design: Foi realizado o planejamento do curso com um plano detalhado, incluindo metas específicas de aprendizagem, estratégias de ensino, seleção de conteúdo, atividades de aprendizagem e métodos de avaliação.

Desenvolvimento: No método ADDIE, o desenvolvimento envolve a criação ou adaptação de materiais de ensino de acordo com o plano estabelecido na fase de design. Isso incluiu a produção de recursos educacionais, como slides, textos, atividades interativas, aulas práticas aplicacção de atividades escritas em forma de questionários, entre outros.

Implementação: Na etapa da implementação o plano de ensino foi colocado em prática. Isso incluii dar aulas, distribuir materiais impressos, entre outras formas de fornecer o ensino planejado. Durante essa fase, foi garantido que os alunos tivessem acesso aos recursos e suporte necessários para alcançar os objetivos de aprendizagem estabelecidos no design pedagógico. Por isso a pré organização do laboratório foi fundamental para que eles estivessem aptos a utilização no momento da aula.

Avaliação: Observações, anotações e aplicação de questionários foram realizados durante e ao final do curso para avaliar o nível de compreensão dos alunos sobre os temas abordados durante o curso. Com isso pode-se perceber se as metas de aprendizagem foram alcançadas e se os conhecimentos foram aplicados de maneira prática. Com base nessas avaliações, ajustes poderam ser feitos para melhorar ações durante o curso e futuras implementações.

5 CONSIDERAÇÕES FINAIS

O projeto de implementação do curso de cibersegurança no Centro Estadual de Educação Profissional (CEEP) José Pacífico, voltado aos alunos do segundo ano

do Curso Técnico em Informática Integrado ao ensino médio, demonstrou ser uma iniciativa essencial para enfrentar os desafios de um mundo cada vez mais digital e exposto a ameaças cibernéticas constantes. A proposta alcançou os objetivos propostos e metas traçadas, confirmando a hipótese de que a aplicação do curso contribuiria significativamente para o entendimento e adoção de práticas seguras no ambiente digital pelos alunos.

A abordagem adotada, que combinou atividades teóricas e práticas, proporcionou um aprendizado dinâmico e contextualizado, permitindo aos alunos aplicar os conceitos de cibersegurança em situações mais ligadas à realidade dos estudantes. A aplicação de alguns métodos específicos foram de suma importância para o êxito deste projeto, tais como, como observações em sala de aula, registros em diários de campo e questionários, que de maneira nítida evidenciou um aumento no engajamento dos alunos e melhorias no entendimento sobre segurança digital. Os dados indicaram que a estratégia de utilizar simulações de ataques cibernéticos, pegando pontos importantes da realidade dos alunos foi um diferencial para despertar o interesse dos estudantes e facilitar a assimilação dos conteúdos.

Ademais, a análise dos resultados confirmou a relevância da educação digital como ferramenta indispensável para a formação de cidadãos conscientes e preparados para os riscos da era tecnológica, uma vez que com o passar do tempo em uma sociedade cada vez mais conectada, a tendência é que os processos civis, pessoais e profissionais estejam cada vez mais conectados à rede. O curso não apenas forneceu conhecimentos técnicos, mas também promoveu a conscientização sobre responsabilidade digital e a importância da proteção de dados pessoais.

Como contribuição para futuras pesquisas e práticas educacionais, sugere-se a expansão do projeto para outras instituições de ensino, bem como o aprofundamento de conteúdos mais avançados, como o uso de gerenciadores de senhas e estratégias de autenticação. Essas ações podem potencializar o impacto do curso e preparar os alunos para desafios mais complexos no âmbito da segurança digital.

Finalmente, a experiência adquirida reforça a importância de iniciativas educacionais alinhadas às necessidades do mundo contemporâneo, onde a cibersegurança deve ser tratada como uma prioridade. A continuidade e aprimoramento desse tipo de projeto são fundamentais para a construção de uma cultura de segurança digital e para garantir que os jovens se tornem um multiplicador

de conhecimentos em sua realidade, como agentes ativos na promoção de um ambiente digital mais seguro e confiável

REFERÊNCIAS

CISA. What is Cybersecurity? Disponível em: https://www.cisa.gov/news-events/news/what-cybersecurity. Acesso em: 01 mai. 2024.

Custo da Negligência? Ou Custo de um Ataque? - Horizontes. Disponível em: https://horizontes.sbc.org.br/index.php/2021/08/custo-negligencia-ou-do-ataque/. Acesso em: 10 mai. 2024.

Cybersecurity Report Series - Download PDFs. Disponível em: https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html. Acesso em: 30 abr. 2024.

FILATRO, A. Design instrucional na prática. São Paulo (SP): Pearson Education do Brasil, 2008.

FALKEMBACH, Elza Maria Fonseca. Diário de campo: um instrumento de reflexão. In: Contexto e Educação, nº 7, Juí: Inijuí, 1987. Disponível em: https://www.unirio.br/cchs/ess/Members/silvana.marinho/disciplina-instrumentos-e-tecnicas-de-intervencao/unid-2-instrumentos-de-conhecimento-intervencao-e-registro/texto-7-falkembach-elza-maria-fonseca-diario-de-campo-um-instrumento-de-reflexao-in-contexto-e-educacao-no-7-jui-inijui-1987/view. Acesso em: 29 abr. 2024.

GLASER, B. G.; STRAUSS, A. L. A descoberta da teoria fundamentada: estratégias para pesquisa qualitativa. Londres: Routledge, 1967.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de Metodologia Científica. 5. ed. São Paulo: Atlas S.A., 2003.

REDAÇÃO. Golpes digitais crescem 35% em 2023. Disponível em: https://tiinside.com.br/29/12/2023/golpes-digitais-crescem-35-em-2023/. Acesso em: 01 mai. 2024.

SBC. Referenciais de Formação em Computação: Educação Básica. 2017. Disponível em: https://www.sbc.org.br/documentos-da-sbc/send/131-curriculos-de-referencia/1166-referenciais-de-formacao-em-computacao-educacao-basica-julho-2017. Acesso em: 04 mar. 2024.

Segurança da INFORMAÇÃO: Saiba como proteger seus dados – Guia prático de segurança de dados. [s.l: s.n.]. Disponível em: https://vilavelha.ifes.edu.br/images/stories/files/guia-pratico-seguranca-da-informacao.pdf. Acesso em: 04 mar. 2024.

STEINBERG, J. Cibersegurança para leigos. [Ano, edição, cidade, s.l.: s.n.].

THIOLLENT, M. Metodologia da pesquisa-ação. São Paulo: Cortez Editora e Livraria Ltda., 2022.

BRASIL. Lei nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 01 jul. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 jul. 2024.

BRASIL. Ministério da Educação. Base Nacional Comum Curricular. Brasília, DF, 2017. Disponível em: EDUCAÇÃO É A BASE. [s.l.: s.n.]. Disponível em: http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf. Acesso em: 04 mar. 2024.