

**UNIVERSIDADE DO ESTADO DO AMAZONAS  
NUCLEO DE ENSINO SUPERIORES DE COARI  
LICENCIATURA EM COMPUTAÇÃO**

**ISAIAS DE BRITO SANTOS**

**SEGURANÇA DIGITAL NA EDUCAÇÃO DE JOVENS E ADULTOS: APLICAÇÃO  
E MÉTODOS DE PREVENÇÃO**

**COARI**

**2024**

**ISAIAS DE BRITO SANTOS**

**SEGURANÇA DIGITAL NA EDUCAÇÃO DE JOVENS E ADULTOS: APLICAÇÃO  
E MÉTODOS DE PREVENÇÃO**

Projeto de pesquisa apresentado como requisito para aprovação na disciplina de Projeto Orientado em Informática na Educação II do curso de Licenciatura em Computação do Centro de Estudos Superiores de Coari da Universidade do Estado do Amazonas.

Orientador: Prof. Me. Genival Nunes de Souza

COARI

2024

## Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).  
**Sistema Integrado de Bibliotecas da Universidade do Estado do Amazonas.**

S237ss Santos, Isaias de Brito  
SEGURANÇA DIGITAL NA EDUCAÇÃO DE  
JOVENS E ADULTOS : Aplicação e Métodos de Prevenção  
/ Isaias de Brito Santos. Manaus : [s.n], 2024.  
59 f.: color.; 29 cm.

TCC - Graduação em Licenciatura em Computação -  
Licenciatura - Universidade do Estado do Amazonas,  
Manaus, 2024.

Inclui bibliografia

Orientador: Souza, Genival Nunes de

1. Phishing. 2. Engenharia social. 3. Segurança  
digital. I. Souza, Genival Nunes de (Orient.). II.  
Universidade do Estado do Amazonas. III. SEGURANÇA  
DIGITAL NA EDUCAÇÃO DE JOVENS E ADULTOS

ISAIAS DE BRITO SANTOS


## SEGURANÇA DIGITAL NA EDUCAÇÃO DE JOVENS E ADULTOS: APLICAÇÃO E MÉTODOS DE PREVENÇÃO

Trabalho de Conclusão de Curso,  
apresentado à Universidade do Estado do  
Amazonas, como parte das exigências  
para a obtenção do título de Licenciado  
em Computação.

Orientador: Me. Genival Nunes de Souza


Coari/AM, 02 de fevereiro de 2024.

### BANCA EXAMINADORA

Documento assinado digitalmente  
 **GENARDE MACEDO TRINDADE**  
Data: 02/02/2024 22:08:55-0300  
Verifique em <https://validar.iti.gov.br>


---

Genarde Macedo Trindade

Documento assinado digitalmente  
 **LANA SIQUEIRA DA SILVA**  
Data: 02/02/2024 22:46:47-0300  
Verifique em <https://validar.iti.gov.br>

---

Lana Siqueira da Silva

Documento assinado digitalmente  
 **JOAO DA MATA LIBORIO FILHO**  
Data: 02/02/2024 20:03:26-0300  
Verifique em <https://validar.iti.gov.br>

---

João da Mata Libório Filho

*“A educação, qualquer que seja ela, é sempre uma teoria do conhecimento posta em prática”.*

(Paulo Freire)

## **AGRADECIMENTOS**

Primeiramente, expresso minha profunda gratidão a Deus. Agradeço também ao meu dedicado orientador Genival Nunes de Souza pela paciência, orientação valiosa e constante estímulo nesta pesquisa. Não poderia deixar de mencionar a importância dos meus amigos, que compartilharam risos, desafios e conquistas ao longo dessa trajetória. Cada um de vocês contribuiu significativamente para o sucesso deste trabalho. Obrigado a todos que fizeram parte dessa jornada única.

Isaias de B. Santos

## RESUMO

A segurança digital na Educação de Jovens e Adultos (EJA) é um tema de crescente relevância na sociedade contemporânea, dada a ampla utilização das Tecnologias Digitais de Informação e Comunicação (TDICs) nesse contexto. No entanto, a falta de conscientização e as vulnerabilidades dos discentes da EJA em relação à segurança digital representam desafios significativos, com ameaças como *phishing* e engenharia social exigindo a implementação urgente de estratégias preventivas e educativas. O objetivo desta pesquisa é Contribuir para a compreensão de métodos e aplicações que permitam um aprimoramento no entendimento sobre segurança de dados, capacitando o estudante da EJA da 10ª etapa em uma escola estadual do município de Coari/AM, a lidar com situações relacionadas a crimes virtuais e computacionais que possam surgir em seu ambiente social ou profissional, enfatizando a importância da conscientização sobre segurança digital na EJA, identificando os riscos enfrentados pelos alunos e propondo medidas eficazes de prevenção.

Para atingir tais objetivos, foi adotada uma abordagem quali-quantitativa por meio de pesquisa-ação, utilizando questionários e debates com os discentes da EJA para coletar dados sobre suas percepções e experiências em relação à segurança digital. A análise dos dados, realizada com técnicas estatísticas descritivas e inferenciais, proporcionou uma compreensão abrangente do problema em questão.

Os resultados da pesquisa evidenciaram a vulnerabilidade dos discentes da EJA em relação à segurança digital, ressaltando a urgência de estratégias de prevenção e conscientização. Além disso, a eficácia das estratégias de conscientização na redução dos riscos de segurança digital para esses alunos foi identificada, Contribuindo assim para a reunião de informações valiosas que, além de oferecer estatísticas relevantes, também contribuirão para a criação de um cartaz. Este tem como objetivo conscientizar de forma lúdica sobre os perigos que os discentes podem enfrentar ao utilizar algum tipo de tecnologia capaz de armazenar informações pessoais. A imagem abaixo retrata o esboço do cartaz.

Diante desses resultados, conclui-se que a conscientização e a capacitação dos discentes da EJA são fundamentais para mitigar os riscos de segurança digital. A implementação de medidas preventivas, como materiais audiovisuais e informativos,

é essencial para criar um ambiente digital mais seguro e protegido para esses alunos, contribuindo assim para a promoção de uma educação digitalmente segura e consciente.

Palavras-chave: *Phishing*, Engenharia social, Segurança digital.



## **ABSTRACT**

Digital security in Youth and Adult Education (YAE) is a topic of increasing relevance in contemporary society, given the wide use of Digital Information and Communication Technologies (DICTs) in this context. However, the lack of awareness and vulnerabilities of YAE students in relation to digital security represent significant challenges, with threats such as phishing and social engineering requiring the urgent implementation of preventive and educational strategies. The objective of this research is to contribute to the understanding of methods and applications that allow an improvement in the understanding of data security, enabling the 10th stage YAE student in a state school in the city of Coari/AM, to deal with situations related to crimes virtual and computational environments that may arise in their social or professional environment, emphasizing the importance of raising awareness about digital security in YAE, identifying the risks faced by students and proposing effective prevention measures.

To achieve these objectives, a qualitative-quantitative approach was adopted through action research, using questionnaires and debates with YAE students to collect data on their perceptions and experiences in relation to digital security. Data analysis, carried out using descriptive and inferential statistical techniques, provided a comprehensive understanding of the problem in question.

The research results highlighted the vulnerability of YAE students in relation to digital security, highlighting the urgency of prevention and awareness strategies. Furthermore, the effectiveness of awareness strategies in reducing digital security risks for these students was identified, thus contributing to the gathering of valuable information that, in addition to offering relevant statistics, will also contribute to the creation of a poster. This aims to raise awareness in a playful way about the dangers that students may face when using some type of technology capable of storing personal information. The image below depicts the outline of the poster.

Given these results, it is concluded that the awareness and training of YAE students are fundamental to mitigating digital security risks. The implementation of preventive measures, such as audiovisual and informative materials, is essential to create a safer and more secure digital environment for these students, thus contributing to the promotion of digitally safe and aware education.

Keywords: Phishing, Social engineering, Digital security.

## LISTA DE TABELAS

<b>Tabela 1-</b> Agrupamento das perguntas com base nos tipos de vulnerabilidade na segurança digital.....	39
<b>Tabela 2</b> – Demonstração das respostas que indicam possíveis ataques decorrentes de interação telefônica.....	40
<b>Tabela 3</b> – Demonstração das respostas que indicam possíveis ataques decorrentes de internet e redes sociais.....	42
<b>Tabela 4</b> – Demonstração das respostas que indicam possíveis ataques decorrentes de phishing.....	44
<b>Tabela 5</b> – Demonstração das respostas que indicam possíveis ataques decorrentes de engenharia social.....	46

## LISTA DE ILUSTRAÇÕES

<b>Figura 1</b> – Matéria sobre estatísticas de golpes online.....	20
<b>Figura 2</b> – Matéria sobre proteção de golpes Virtuais.....	20
<b>Figura 3</b> – Matéria sobre como identificar riscos na internet.....	20
<b>Figura 4</b> – Matéria sobre os principais riscos na internet em 2024.....	20
<b>Figura 5</b> – gráfico exemplificando as respostas obtidas.....	41
<b>Figura 6</b> – Resumo das respostas que indicam possíveis ataques decorrentes de interação telefônica.....	41
<b>Figura 7</b> – Gráfico exemplificando as respostas obtidas com Internet e Redes Sociais.....	43
<b>Figura 8</b> – Resumo das respostas que indicam possíveis ataques decorrentes de Internet e Redes sociais.....	43
<b>Figura 9</b> – gráfico exemplificando as respostas obtidas sobre a pratica de <i>Phishing</i> .....	44
<b>Figura 10</b> – Resumo das respostas que indicam possíveis ataques decorrentes de <i>phishing</i> .....	45
<b>Figura 11</b> – gráfico exemplificando as respostas obtidas relacionadas a Engenharia Socia.....	46
<b>Figura 12</b> – Resumo das respostas que indicam possíveis ataques decorrentes de engenharia sócia. ....	47
<b>Figura 13</b> – discente preenchendo o questionário.....	47
<b>Figura 14</b> – discente relatado as experiências sobre a segurança digita .....	49
<b>Figura 15</b> – discente relatando as suas experiências sobre segurança.....	50
<b>Figura 16</b> – esboço do cartaz produzido a partir das contribuições dos discentes.....	52
<b>Figura 17</b> – Cartaz exposto em sala de aula.....	52

## LISTA DE QUADROS

<b>Quadro 1-</b> Trabalhos Correlatos.....	31
<b>Quadro 2-</b> Resultado da reunião e entrevista dos discentes.....	49

## **LISTA DE SIGLAS E ABREVIATURAS**

**TDIC:** Tecnologias Digitais da Informação e Comunicação.

**EJA:** Educação de Jovens e Adultos

## GLOSSÁRIO

**Cyberbullying:** Refere-se ao assédio, intimidação ou agressão verbal e psicológica que ocorre online, geralmente nas redes sociais, mensagens instantâneas ou outras plataformas digitais.

**Dados:** São informações coletadas, registradas ou analisadas durante a pesquisa.

**E-mails:** São mensagens eletrônicas enviadas e recebidas por meio de serviços de correio eletrônico.

**Fishing:** Refere ao ato de pescar.

**Insights:** São descobertas, conclusões ou observações perspicazes que surgem a partir da análise de dados ou da investigação.

**MSN:** Serviços de mensagens instantâneas são mais populares, como o WhatsApp e o Facebook Messenger.

**Phishing:** É uma forma de ataque cibernético em que os criminosos tentam enganar as pessoas para que revelem informações confidenciais, como senhas e números de cartão de crédito, fingindo ser uma entidade confiável.

**Insights:** Insight ou insights é um substantivo com origem no idioma inglês e que significa compreensão súbita de alguma coisa ou determinada situação.

**WhatsApp:** WhatsApp é um aplicativo multiplataforma de mensagens instantâneas e chamadas de voz para smartphones.

**Internet:** é uma rede global de computadores que permite a comunicação e o compartilhamento de informações em todo o mundo.

**Software:** programas de computador que possibilitam a execução de tarefas específicas.

## SUMÁRIO

<b>1 INTRODUÇÃO</b> .....	<b>17</b>
<b>1.1 CONTEXTUALIZAÇÃO E CARACTERIZAÇÃO DO PROBLEMA</b> .....	<b>18</b>
<b>1.2 JUSTIFICATIVA</b> .....	<b>21</b>
<b>1.3 OBJETIVOS</b> .....	<b>21</b>
1.3.1 Objetivo geral .....	21
1.3.2 Objetivos específicos .....	22
<b>1.4 ORGANIZAÇÃO DO TRABALHO</b> .....	<b>22</b>
<b>2 FUNDAMENTAÇÃO TEÓRICA</b> .....	<b>24</b>
<b>2.1 ASPECTOS SOCIAIS DA SEGURANÇA DIGITAL</b> .....	<b>24</b>
<b>2.2 O ENSINO DE JOVENS E ADULTOS (EJA)</b> .....	<b>25</b>
<b>2.3 IMPACTO PSICOLÓGICO DOS CRIMES DIGITAIS</b> .....	<b>26</b>
<b>2.4 MÉTODOS DE PROTEÇÃO DE DADOS</b> .....	<b>27</b>
<b>2.5 TRABALHOS RELACIONADOS</b> .....	<b>27</b>
2.5.1 Geraldo e Takeda (2019) .....	28
2.5.2 Souza (2020) .....	28
2.5.3 Alves e Freitas (2021) .....	29
2.5.4 Amaral e Palomar (2021) .....	29
2.5.5 Salviano, Santos e Silva (2022) .....	30
2.5.6 Neves (2022) .....	30
<b>3 METODOLOGIA</b> .....	<b>33</b>
<b>3.1 PLANO DE PESQUISA NA INSTITUIÇÃO SELECIONADA</b> .....	<b>33</b>
<b>3.2 MÉTODOS, FERRAMENTAS E TÉCNICAS UTILIZADAS</b> .....	<b>34</b>
3.2.1 Coleta de Dados .....	35
3.2.2 Análise de Dados .....	35
3.2.3 Pesquisa-ação .....	36
<b>3.3 ETAPAS DO PROJETO</b> .....	<b>36</b>
<b>4 RESULTADOS E DISCURSÕES</b> .....	<b>38</b>
<b>4.1 QUESTIONÁRIO</b> .....	<b>38</b>
4.1.1 Resultados de possíveis ataques decorrentes de interação telefônica .....	40
4.1.2 Resultados de possíveis ataques decorrentes internet e redes sociais .....	42



4.1.3 Resultados de possíveis ataques decorrentes de <i>phishing</i> .....	44
4.1.4 Resultados de possíveis ataques decorrentes de abordagem através de engenharia social .....	45
<b>4.2 REUNIÕES .....</b>	<b>48</b>
4.2.1 Resultado da reunião do primeiro dia .....	48
4.2.2 Reunião para planeja o um cartaz .....	50
<b>5 CONCLUSÃO E TRABALHOS FUTUROS .....</b>	<b>53</b>
<b>REFERÊNCIAS.....</b>	<b>55</b>
<b>ANEXOS .....</b>	<b>58</b>

## 1 INTRODUÇÃO

Este projeto de pesquisa é fruto de um esforço que visa auxiliar os discentes e prepará-los para um mundo no qual a segurança pessoal e virtual está passando por mudanças velozes. A pesquisa tem como público-alvo uma turma do ensino médio da Educação de Jovens e Adultos (EJA). Conforme destacado por Amaral e Palomar (2023, p.15), em que relata “ao longo da história, muitas pessoas não tiveram a oportunidade de ingressarem em uma instituição escolar ao longo de suas vidas, por motivos diversos e quase sempre ligados à exclusão social”. Nesse contexto, a questão da segurança digital pode causar um impacto significativo, uma vez que a engenharia social tem como alvo pessoas com pouca instrução.

O avanço tecnológico e o crescimento do uso de dispositivos digitais têm desempenhado um papel fundamental na evolução do processo educacional, especialmente na EJA. Onde é oferecido uma nova oportunidade de escolaridade para quem deixou os estudos por trabalho, ligando-se à vulnerabilidade socioeconômica em áreas com pouca estrutura educacional, como comunidades rurais e ribeirinhas, devido a limitações geográficas (Quaresma, 2019).

Quaresma destaca a amplitude dos objetivos da EJA, sublinhando a diversidade de processos formativos abrangidos por essa modalidade, desde a qualificação profissional até questões culturais, facilitando assim a inclusão desses participantes na sociedade.

Na elaboração deste Trabalho de Conclusão de Curso (TCC), foi usado uma abordagem metodológica que engloba a aplicação de questionários e a realização de reuniões. Esses métodos foram escolhidos para coletar dados relevantes sobre a percepção dos discentes em relação à segurança digital na EJA, com enfoque nas Tecnologias Digitais de Informação e Comunicação (TDICs).

A aplicação de questionários proporcionará uma análise quantitativa, permitindo a obtenção de dados estatísticos sobre as experiências e conhecimentos dos alunos em relação aos riscos cibernéticos, como *phishing* e engenharia social. Além disso, as reuniões serão um meio eficaz para a coleta de informações qualitativas, possibilitando uma compreensão mais aprofundada das percepções e preocupações dos participantes.

Os dados coletados ao longo desta pesquisa são de suma importância para a compreensão e a produção de materiais que possam aprimorar a compreensão da relação entre os discentes e a segurança digital. Isso, por sua vez, será valioso para instruir e prevenir possíveis ataques cibernéticos, contribuindo assim para a conscientização e capacitação dos envolvidos no ambiente educacional da EJA.

### **1.1 Contextualização e caracterização do problema**

Na atualidade, em que a tecnologia exerce influência sobre o avanço da civilização, é indispensável que o indivíduo evolua em paralelo. Desde as grandes revoluções ocorridas em épocas passadas, os progressos tecnológicos têm impulsionado a sociedade a desenvolver-se de maneira natural, visando corrigir deficiências que surgem tanto devido ao desenvolvimento social quanto ao próprio avanço das TDICs:

A história da Computação está marcada por interrupções repentinas, por mudanças inesperadas e imprevistas, tornando-se difícil a visão da evolução dos computadores mediante uma mera enumeração linear de invenções-nomes-datas (Fonseca, 2007, p.13).

A evolução imprevisível da Computação, conforme destacado por Fonseca, ressalta a importância de compreender os desafios inerentes à segurança digital. Em um contexto educacional, especialmente para alunos da EJA, essa compreensão torna-se crucial. A implementação de tecnologias de segurança visa preparar esses alunos para um ambiente digital em constante transformação, oferecendo ferramentas e conhecimentos necessários para enfrentar as adversidades online.

Em relação as novas tecnologias Freire (1996, p. 36) afirma “Não tenho dúvida nenhuma do enorme potencial de estímulos e desafios à curiosidade que a tecnologia põe a serviço das crianças e dos adolescentes das classes sociais chamadas favorecidas”.

A complexa evolução da Computação, destacada por Fonseca (2007), contrasta com o potencial estimulante e desafiador que a tecnologia oferece, especialmente para crianças e adolescentes de classes sociais mais privilegiadas,

conforme ressalta Freire. Essas perspectivas ressaltam a imprevisibilidade e as oportunidades intrínsecas ao avanço tecnológico. Dessa forma, para assegurar a integridade física, mental e patrimonial dos utilizadores, que tendem a fazer uso cada vez mais indiscriminado destas tecnologias, foi imprescindível a evolução dos meios de segurança.

Há duas décadas, a única preocupação em relação à segurança que um indivíduo comum tinha era apenas guardar a chave da sua residência ou uma senha bancária. No entanto, a rápida disseminação da comunicação e a introdução das mídias sociais aceleraram os riscos à integridade moral e física das pessoas, sobretudo daquelas que demonstram inaptidão face a estas ameaças. Para Trindade e Carvalho (2019, p.11), “A introdução das Tecnologias Digitais da Informação e da Comunicação (TDIC) nas Escolas é desde vários anos, um facto consumado”.

Na atualidade, é observável que a publicação de fotos de estudantes de maneira ilegal é bastante comum, sendo que, em muitos casos, tal prática gera constrangimentos para as vítimas, dando origem a um ambiente de *cyberbullying*. Leite (2022, p. 9), observou que “na atualidade o *Cyberbullying* está em grande crescente, devido a essa expansão do acesso tecnológico e a privacidade da vítima estar vulnerável e mais acessível para o público virtual”.

Dado que a modalidade EJA abrange jovens e adultos que nem sempre tem acesso à tecnologia, porém com conhecimento limitado, eles eram os principais alvos da prática de *phishing*, que é a forma mais frequente de ciberataque. Para Nascimento, Santos e Edler (2022, p. 2229), “o cibercriminoso opera o uso do *phishing*, que é um neologismo da palavra americana ‘*fishing*’ que significa pescar. Que encaixa muito bem com o conceito do crime que é de ‘pescar vítimas’”.

Este método de ataque conhecido como *Phishing* é o mais popular, sendo amplamente utilizado. Um relatório da renomada empresa de segurança *virtual Kaspersky* revela que o Brasil lidera em número de vítimas desses ataques. Como apresentado pelas Figuras 1, 2, 3, 4 contidas logo abaixo:

**Figura 1-** Matéria sobre estatísticas de golpes online

Fonte: R7, 2023.

**Figura 3-** Matéria sobre proteção de golpes Virtuais

Fonte: G1, 2023.

**Figura 3-** Matéria sobre como identificar riscos na internet

Fonte: CNN Brasil, 2023. 2024]

**Figura 4-** Matéria sobre os principais riscos na internet em 2024

Fonte: Olhar digital, 2023.

As matérias das Figuras 1, 2, 3 e 4 expressam a situação atual da segurança digital no Brasil e fazem uma perspectiva pertinente sobre como lidar com esses desafios. Os quais são uma preocupação caso não ocorra uma conscientização a respeito da segurança digital.

Tendo em vista todos esses desafios que os discentes da EJA podem enfrentar, surge a questão que norteia esta pesquisa: de que maneira a falta de conhecimento sobre segurança digital entre adultos com pouca instrução afeta o uso das novas tecnologias, e como a conscientização e capacitação desses indivíduos podem contribuir para prevenir problemas e promover um uso mais seguro das TDICs?

## **1.2 Justificativa**

A constante inserção de novas tecnologias na sociedade, buscando facilitar a vida cotidiana, apresenta uma dualidade. Um exemplo notável é observado nos bancos virtuais, que proporcionam conveniência aos usuários ao eliminar a necessidade de longas filas para transações financeiras. Contudo, essa comodidade não está isenta de riscos, para enfrentar essa evolução, os criminosos adaptaram-se, tornando-se mais tecnológicos e recorrendo à engenharia social para alcançar seus objetivos, essa evolução tecnológica impulsionou o emprego da engenharia social, explorando abordagens físicas, online e psicológicas para atingir metas criminosas (PEDROSO, 2019). A conscientização dessas práticas criminosas é necessária para que o usuário possa acompanhar a evolução tecnológica de modo seguro tornando assim o entendimento desse conhecimento crucial para a prevenção e proteção contra potenciais ameaças.

No cenário digital, os criminosos permanecem à espreita, aguardando oportunidades para coletar informações e cometer diversos crimes com os dados obtidos, e com o avanço das tecnologias, mais pessoas estão sendo enganadas por armadilhas online para roubo de informações pessoais (ALVES E FREITAS, 2021). Essa ação criminosa, muitas vezes, resulta em danos materiais e psicológicos para os usuários, que frequentemente só percebem o crime muito tempo após sua ocorrência. Essa compreensão destaca a importância da conscientização sobre as práticas da engenharia social, visando uma navegação segura no mundo digital.

## **1.3 Objetivos**

### **1.3.1 Objetivo geral**

- Contribuir para a compreensão de métodos e aplicações que permitam um aprimoramento no entendimento sobre segurança de dados, capacitando o estudante da EJA da 10ª etapa em uma escola estadual do município de Coari/AM, a lidar com situações relacionadas a crimes virtuais e computacionais que possam surgir em seu ambiente social ou profissional.

### 1.3.2 Objetivos específicos

- Investigar os principais fatores que dificultam a compreensão e o entendimento sobre os aspectos da segurança digital.
- Identificar as principais ameaças que possam ter um impacto social e profissional na vida do estudante.
- Analisar os principais artefatos computacionais e suas vulnerabilidades em relação aos estudantes da modalidade EJA.
- Analisar os dados obtidos e propor soluções que possam se adequar a realidade do estudante.

### 1.4 Organização do Trabalho

Este capítulo inaugura a pesquisa ao apresentar o contexto amplo do tema escolhido, delineando a caracterização do problema investigado. Além disso, são explicitados os objetivos gerais e específicos que nortearam o desenvolvimento do trabalho, proporcionando uma visão geral da estrutura organizacional adotada.

No segundo capítulo, concentra-se grande parte da fundamentação teórica, construída a partir de pesquisas e análise extensiva de artigos científicos, livros e recursos governamentais. Este capítulo visa fornecer uma base sólida e embasada para a pesquisa, apresentando conceitos, teorias e abordagens relevantes ao tema.

O terceiro capítulo aborda a execução da pesquisa os métodos, procedimentos e ferramentas que foram empregados. Inclui a descrição das abordagens adotadas, as técnicas de coleta e análise de dados, bem como as estratégias de organização, como tabelas e reuniões.

No quarto capítulo, são delineados os resultados esperados do projeto, considerando tanto aspectos positivos quanto negativos. Além disso, são antecipadas possíveis dificuldades que podem surgir ao longo da pesquisa, proporcionando uma visão realista dos potenciais barreiras a serem enfrentadas.

O quinto capítulo está relacionado as considerações finais, evidenciando a relevância do tema de segurança digital para os discentes do EJA, ressaltando a necessidade de conscientização e preparo diante dos desafios tecnológicos. O

capítulo serve como conclusão abrangente, apontando para futuras pesquisas e consolidando a importância do estudo para a comunidade escolar.



## 2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica desempenha um papel fundamental em qualquer trabalho acadêmico, fornecendo o alicerce conceitual sobre o qual toda a pesquisa é construída. No contexto de um TCC, a fundamentação teórica é especialmente importante, pois ajuda a contextualizar o problema de pesquisa, embasar as hipóteses levantadas e orientar a análise dos dados.

### 2.1 Aspectos sociais da segurança digital

Devido ao fato de as mídias sociais estarem tão difundidas no cotidiano, elas assumiram outros papéis na interação social, incluindo a compra e venda de produtos. Isso criou uma alternativa simplificada para pessoas que buscam facilidades e comodidades, sem as complicações das lojas atuais facilitando os ataques virtuais.

Nos dias atuais, se tornou muito comum os compartilhamentos e exposição da vida pessoal através das mídias sociais. É uma variável crescente quando tratamos de exibição de fotos, vídeos, pensamentos e estilo de vida no ambiente virtual (SANTOS E RODRIGUES, 2023 p. 855).

Os métodos de ataques são diversificados e usam vários tipos de mídias, podendo abranger desde abordagens simples até as mais complexas. Hoje, a Internet conecta instantaneamente milhões de pessoas, trazendo benefícios, mas também criando riscos, já que qualquer pessoa conectada pode se tornar um alvo de atividades criminosas (NEVES, 2022).

Variando de acordo com o meio empregado e o alvo escolhido, independentemente da estratégia escolhida, o objetivo persiste inalterado: explorar a ingenuidade e vulnerabilidade das pessoas (PEDROSO, 2019). Grande parte dessa vulnerabilidade ocorre devido à carência das pessoas em se socializarem, tornando-as vulneráveis a pessoas que usam artifícios da engenharia social para se aproximar das vítimas.

## 2.2 O Ensino de Jovens e Adultos (EJA)

O público da (EJA) é caracterizado por sua diversidade, abrangendo diferentes idades, cada um com sua própria trajetória de vida, que inevitavelmente influencia sua experiência de aprendizado (AMARAL E PALOMAR, 2023).

Neste contexto, a educação revela-se como uma ferramenta transformadora, capaz de transformar os aprendizes para que se tornem agentes ativos na construção de um futuro mais significativo.

A alfabetização de adultos, por sua vez, deve ser entendida como um processo de conscientização, em que os educandos são estimulados a refletir sobre sua realidade e a buscar soluções para os problemas que enfrentam. Freire (1996, p. 32)

Portanto, é fundamental considerar a abordagem educacional libertadora, que concentra-se em capacitar os estudantes para uma análise crítica e reflexiva, visando não apenas o aprendizado, mas também a formação de cidadãos conscientes e participativos.

...(EJA) é uma modalidade de ensino ofertada para pessoas que não tiveram acesso a escola no período regular por algum motivo. Os alunos que frequentam a EJA geralmente são os de baixa renda, meninas que tiveram filho cedo, homens que trabalham no período diurno, jovens que foram excluídos da escola por diversos motivos, idosos que não tiveram oportunidade de estudar no período regular. (Beleza e Nogueira, 2020 p. 114).

A modalidade EJA é uma das que menos recebe atenção social do governo, contribuindo para um alto índice de evasão escolar e contribui muito para a desigualdade social, tornando-os principais alvos de golpes através de *phishing*. Araújo (2023, p.44) afirma que “ O *phishing* costuma se passar por mensagem de bancos, operadoras de celular, órgãos públicos, entre outros”.

Levando em consideração esta afirmação é fundamental que os discentes da EJA também desenvolver habilidades críticas para discernir informações online, considerando que o *phishing* muitas vezes se disfarça como mensagens de instituições confiáveis, como bancos e órgãos públicos, buscando enganar os

usuários. Isso destaca a necessidade de conscientização sobre segurança digital, não apenas no contexto educacional, mas também na esfera online, para evitar potenciais riscos.

### **2.3 Impacto psicológico dos crimes digitais**

O impacto psicológico dos crimes digitais é uma realidade cada vez mais evidente em nossa sociedade tecnologicamente avançada. Conforme destacado por Neves (2022, p.12), “Assim, o objetivo do ofensor é fazer passar-se pela entidade legítima através de uma justificação mais ou menos astuciosa, levando a que o indivíduo forneça um conjunto de dados e informações privadas”, esta, uma forma comum de ataque digital, não se limita apenas à obtenção de informações confidenciais; ele busca também manipular os usuários por meio de comunicações enganosas. Essa estratégia, muitas vezes, deixa as vítimas não apenas financeiramente prejudicadas, mas também emocionalmente abaladas.

O caminho da privacidade à proteção de dados pessoais é mais uma prova de que a dimensão individual da construção da personalidade depende que as condições de seu desenvolvimento estejam protegidas (SARLET E SAAVEDRA, 2020, p. 37).

A transição proposta por Sarlet e Saavedra (2020), do conceito de privacidade para a proteção de dados pessoais ganha relevância nesse contexto. O caminho da privacidade à proteção destaca a necessidade de resguardar as condições essenciais para o desenvolvimento individual, reconhecendo que a segurança digital não é apenas uma questão técnica, mas também um elemento vital para a integridade psicológica dos usuários.

Na análise da engenharia social, como observado por Pedroso (2019. p. 15), “Na análise acerca da engenharia social é possível observar que o fator humano é o vínculo mais frágil da segurança”, torna-se evidente que o fator humano é o elo mais frágil da segurança digital. Isso sublinha a importância de estratégias educacionais e conscientização para fortalecer não apenas as defesas contra crimes digitais, mas também para mitigar os efeitos negativos que esses ataques podem ter no bem-estar mental das vítimas.

## 2.4 Métodos de proteção de dados

É fundamental compreender que não existe uma infraestrutura de segurança da informação que possa assegurar proteção absoluta, pois sempre haverá possibilidades de erros, por mais improváveis que pareçam (PEDROSO, 2019).

Do ponto de vista humano, a Engenharia Social representa um dos principais desafios em relação à Segurança da Informação, uma vez que os engenheiros sociais podem empregar diversas técnicas para obter acesso a informações confidenciais das empresas. É crucial que os colaboradores recebam treinamento e estejam cientes da relevância da segurança da Informação, compreendendo o papel que desempenham na proteção das informações e na identificação de possíveis situações de risco para minimizar problemas (SOUZA, 2020).

O discernimento desempenha um papel crucial nessas situações. É essencial estar vigilante em relação a qualquer tipo de abordagem, independentemente do canal utilizado, seja por meio de e-mails, telefonemas, entre outros (ALVES, 2010).

## 2.5 Trabalhos Relacionados

O tema desta pesquisa está intrinsecamente ligado aos trabalhos correlatos, pois a proposta destes busca proporcionar novos debates sobre a segurança da informação, abordando não apenas novos conceitos sobre ameaças, mas também novos métodos de prevenção, oferecendo uma visão abrangente sobre o tema em questão.

Para a seleção dos trabalhos, foi utilizada a plataforma de pesquisa Google Acadêmico. A escolha desta plataforma se deu devido ao vasto acervo de trabalhos acadêmicos disponíveis. O critério para a seleção e pesquisa do conteúdo baseou-se principalmente em palavras-chave relacionadas ao tema proposto, tais como "segurança digital", "educação de jovens e adultos" e as principais ameaças virtuais, como "*phishing*" e "engenharia social". Foram escolhidos trabalhos redigidos em português brasileiro, com datas de publicação dos últimos 5 anos, que abordassem de maneira clara a segurança digital e seu impacto nas pessoas com pouca instrução em tecnologia.

### **2.5.1 Geraldo e Takeda (2019)**

Na publicação intitulada “Engenharia Social: Um Perigo Oculto Em Simples Técnicas” O autor fazendo uso de um método de pesquisa centrado na aplicação de um formulário eletrônico aberto na Internet. Esse questionário foi utilizado para coletar respostas que abordavam questões relacionadas à engenharia social, permitindo ao público em geral entender comportamentos cotidianos e, assim, evitar ser vítima dessas práticas.

O principal público-alvo dessa pesquisa compreende a população em geral, buscando disseminar conhecimentos sobre técnicas de engenharia social e promover a conscientização das pessoas em relação às ameaças do dia a dia.

Ao concluir a sua pesquisa ele pode constatar que, apesar dos esforços dos engenheiros sociais, uma parcela da população ainda apresenta vulnerabilidades significativas no que diz respeito à segurança. Também constatou a necessidade de expandir os trabalhos de conscientização dos usuários, tanto dentro quanto fora das organizações, visando promover uma conduta mais segura diante das ameaças da engenharia social.

### **2.5.2 Souza (2020)**

Na sua pesquisa intitulada “Usuário, o elo mais fraco da segurança da informação”, busca fazer uma pesquisa extensiva sobre vários autores buscando trazer a realidade da segurança digital buscando informar sobre estes riscos destacando o fato de que as empresas tem um alto investimentos em mecanismos de segurança e que muitas das vezes, podem não ser suficiente para garantir a segurança das informações empresariais.

O autor tem como público-alvo deste artigo as organizações brasileiras, buscando sensibilizar e instruir toda a equipe de colaboradores sobre a importância da segurança da informação. O autor destaca a necessidade de conscientizar os usuários sobre o papel crucial que desempenham nesse contexto e que muitas das vezes e negligenciado.

Ao concluir o seu artigo o autor destaca a importância da disseminação do tema entre todos os membros da organização, enfatizando a elaboração de Políticas

Internas de Segurança da Informação. Essas políticas devem orientar a conduta dos funcionários e colaboradores em relação ao tratamento das informações das empresas.

### **2.5.3 Alves e Freitas (2021)**

Em seu artigo intitulado “Segurança da informação e os desafios da nossa sociedade perante as novas tecnologias”, O estudo visa compreender os desafios da segurança digital frente às Novas Tecnologias, enfatizando a importância da proteção de dados na internet. A metodologia adotada envolveu uma análise reflexiva das práticas de segurança e estudos de casos de ataques cibernéticos, visando identificar vulnerabilidades e estratégias de proteção eficazes.

As análises revelaram a urgência de conscientização sobre os riscos online e a implementação de medidas robustas de segurança. Apesar dos benefícios da tecnologia, os perigos associados ao compartilhamento descuidado de informações exigem uma abordagem proativa na proteção dos dados pessoais.

Em conclusão, promover a educação em segurança cibernética e incentivar a adoção de práticas responsáveis de proteção de dados são cruciais para mitigar os riscos da internet e garantir um ambiente online seguro para todos.

### **2.5.4 Amaral e Palomar (2021)**

Na pesquisa intitulada “Os desafios de ensino aprendizagem na educação de jovens e adultos - os alunos eja no brasil”, é feita uma pesquisa bibliográfica que visa fazer um levantamento sobre as condições do ensino da EJA no brasil.

O estudo emprega uma pesquisa bibliográfica como metodologia, explorando recursos como livros, apostilas, sites e artigos, procurando relatar a história da EJA, identificar seus desafios, apontar conquistas discretas e destacar estratégias para proporcionar um ensino de qualidade adaptado às características específicas dos jovens e adultos que frequentam essa modalidade.

Ao concluir a sua pesquisa os autores reforçam a importância do desenvolvimento educacional desse grupo, oferecendo oportunidades para resgatar

o direito à educação, especialmente para aqueles que não tiveram acesso à escola em sua fase inicial.

### **2.5.5 Salviano, Santos e Silva (2022)**

Na sua pesquisa “Principais tipos de ataques *Phishing* e mecanismos de segurança”, faz uma abordagem profunda sobre a segurança da informação, com enfoque nos ataques de *phishing*, o seu principal público alvo inclui tanto pessoas quanto organizações, visando descrever os riscos associados a esse tipo de ataque, propondo boas práticas para reduzir as ocorrências e apresentar casos registrados, respaldando as informações com dados que evidenciem o aumento dos ataques de *phishing* ao longo dos anos, utilizando gráficos e tabelas.

Os autores, também abordam uma, pesquisa qualitativa/ descritiva, fundamentada em estudos teóricos e bibliográficos, com a coleta de dados proveniente de fontes como livros de autores renomados, sites governamentais e informações públicas.

Ao concluir a pesquisa, pode-se notar a falta de preparo e a vulnerabilidade significativa de muitos usuários a esse tipo de ataque, sendo este um dos maiores fatores que contribuem para o aumento desses tipos de ataques. Destaca-se, assim, a necessidade de maior conscientização e proteção no ambiente digital.

### **2.5.6 Neves (2022)**

No seu estudo “Vitimação por *Phishing*: um estudo empírico” buscou investigar as relações entre variáveis sociodemográficas, traços de personalidade e medidas preventivas com a probabilidade de ser vítima de ataques de *phishing*. Utilizando uma abordagem quantitativa, o estudo buscou compreender os fatores que contribuem para a vulnerabilidade das pessoas a esse tipo de crime cibernético.

A pesquisa adotou uma metodologia quantitativa, permitindo a análise estatística descritiva e inferencial dos dados coletados. A amostra foi selecionada com base nos objetivos e hipóteses do estudo, utilizando instrumentos específicos para a operacionalização das variáveis. Os dados foram coletados por meio de questionários e posteriormente analisados com o *software* IBM SPSS® 27,

possibilitando uma investigação aprofundada das relações entre as variáveis estudadas.

Os resultados do estudo revelaram *insights* importantes sobre a vitimação por *phishing*. Fatores como características sociodemográficas e traços de personalidade demonstraram influenciar a probabilidade de ser vítima de ataques de *phishing*. Além disso, medidas preventivas, quando adotadas de forma eficaz, mostraram-se cruciais na redução da vulnerabilidade dos indivíduos a esse tipo de crime cibernético. Essas descobertas contribuem não apenas para a compreensão acadêmica do fenômeno, mas também para o desenvolvimento de estratégias de prevenção mais eficazes.

A Tabela 01 a seguir destaca os trabalhos correlatos que exploram a temática sobre a segurança digital no contexto da EJA. Nesta compilação, são apresentados os autores, os títulos, o grau de escolaridade dos discentes envolvidos e as áreas do conhecimento abordadas. Esta análise visa proporcionar uma visão abrangente das pesquisas relacionadas, oferecendo uma visão geral sobre o tema.

**Quadro 01 – Trabalhos Correlatos**

<b>Autor(es)</b>	<b>Público alvo EJA</b>	<b>Conscientização</b>	<b>Demonstrativo</b>	<b>Interação com o objeto da pesquisa</b>	<b>Elaboração de Material de Conscientização</b>
Geraldo e Takeda (2019)	-	X	X	-	-
Souza (2020)	-	X	X	-	-
Alves (2021)	-	X	-	-	-
Amaral e Palomar (2021)	X	-	-	-	-
Salviano, Santos e Silva (2022)	-	X	X	-	-
Neves (2022)	-	-	X	-	-
Este trabalho	X	X	X	X	X

**Fonte:** Autor (2024)



Esta pesquisa, alinhada com trabalhos correlatos, destaca-se por sua abordagem inovadora e foco específico na segurança digital na Educação de Jovens e Adultos (EJA) durante a 10ª etapa. Enquanto os estudos anteriores oferecem visões amplas sobre segurança digital, este trabalho mergulha nas particularidades dessa modalidade de ensino, considerando as vulnerabilidades socioeconômicas dos alunos. Essa diferenciação visa preencher uma lacuna de conhecimento, contribuindo para a compreensão mais profunda das ameaças digitais enfrentadas por esse grupo específico o EJA, e assim, proporcionar resultados valiosos para práticas preventivas e conscientização.

### 3 METODOLOGIA

Foi realizado uma pesquisa bibliográfica extensiva na plataforma *Google* acadêmico, levando em consideração os principais trabalhos acadêmicos alinhados com o tema da pesquisa, Segurança Digital na EJA, incluindo revisões literárias abordando pontos chaves para a pesquisa como métodos de prevenção, riscos de segurança digital e engenharia social.

Após a pesquisa bibliográfica, buscou-se instituições que contivessem turmas da EJA para a aplicação da pesquisa, realizando assim reuniões com o corpo docente da instituição, buscando um consenso para a realização da pesquisa. Foi apresentada a proposta da pesquisa sobre segurança digital para os alunos da EJA, e o cronograma de execução foi distribuído aos docentes da instituição, demonstrando o passo a passo como a pesquisa se daria na instituição.

#### 3.1 Plano de Pesquisa na Instituição selecionada

No decorrer de novembro, foi realizado, uma série de atividades para a pesquisa em segurança digital na EJA, iniciado com uma reunião no dia 17 de novembro de 2023, em que introduzimos a pesquisa, destacando sua relevância, objetivos e explicando o cronograma. Nesse encontro, aplicamos um questionário para coletar dados iniciais.

Em 24 de novembro de 2023, foi conduzimos uma sessão de Sensibilização sobre Segurança Digital, onde foi utilizado um retroprojeter para ilustrar riscos de compartilhar informações, ameaças virtuais como vírus de computador, as práticas de *phishing* e engenharia social, destacando métodos e práticas de como se prevenir destas ameaças.

A Reunião de Opinião aconteceu em 31 de novembro de 2023, esta reunião teve como foco principal a análise das respostas do questionário, expondo estes resultados para os discentes para obtenção de vivências a respeito da segurança digital, fazendo com que o discente se sinta à vontade para discutir sobre o tema.

A pesquisa realizada na Escola foi concluída em 01 de novembro de 2023 por meio de um debate sobre segurança digital. Durante essa interação, buscamos explorar as opiniões dos estudantes em relação às suas principais dificuldades no

tratamento de informações nas redes virtuais. Propusemos que os discentes expressassem suas opiniões diretamente sobre temas relevantes, visando, no futuro, auxiliar outros estudantes que possam enfrentar situações semelhantes. Essas contribuições serão utilizadas para a criação de materiais informativos direcionados ao público-alvo da EJA.

### **3.2 Métodos, Ferramentas e Técnicas utilizadas**

Esta pesquisa sobre segurança digital para alunos da EJA adota uma abordagem quali-quantitativa, combinando métodos qualitativos e quantitativos. Essa estratégia visa não apenas quantificar dados sobre a compreensão dos alunos em relação à segurança digital, mas também explorar de maneira qualitativa suas experiências, percepções e desafios específicos.

O trabalho científico, assim, poderá engajar escopos quantitativos, qualitativos ou quali-quantitativos com descrições exploratórias e de caráter explicativo tendo como argumento as teorias já existentes oriundas de assertivas científicas a determinado campo de pesquisa (Rodrigues, Oliveira e Santos, 2021 p.171).

A metodologia empregada segue a orientação de Rodrigues, Oliveira e Santos (2021), desta forma, será aplicada um questionário para estimar se os participantes da pesquisa seriam possíveis alvos de ataque e suas vulnerabilidades. Esta metodologia de pesquisa é baseada em uma abordagem pré-existente da teoria de Geraldo e Takeda (2019), incorporando elementos dessa metodologia para atender às necessidades específicas desta pesquisa.

Em complemento as atividades de revisão bibliográfica, optou-se por realizar uma atividade de campo, utilizando um formulário eletrônico com 19 (dezenove) questões, as quais, foram elaboradas para explorar situações comportamentais para a representação de parte da engenharia social. As questões elaboradas foram relacionadas a alguns tipos de ataques da engenharia social (Geraldo e Takeda, 2019, p. 246).

Se a intenção for ver e entender como os dados estão distribuídos em um grupo de amostras, então a pesquisa será vista como quantitativa (PITANGA, 2020). Desse modo, foi utilizado um questionário com 15 (quinze) questões para que os

discentes da EJA possam preencher com sim, não ou não sei informar, simulando situações corriqueiras do dia, explorando os principais ataques desde o método através de *phishing* e engenharia social. Os resultados obtidos foram quantificados e serão apresentados na seção resultado e discursões.

Durante o segundo momento, foi abordada uma metodologia qualitativa, realizando reuniões e debates para aprofundar a realidade dos principais riscos que envolvem os estudantes da EJA. Oliveira et al. (2020, p. 2), afirma que " Na verdade, uma pesquisa de natureza qualitativa busca dar respostas a questões muito particulares, específicas, que precisam de elucidações mais analíticas e descritivas", as reuniões foram fundamentais para explorar nuances e contextos específicos, proporcionando uma compreensão mais aprofundada dos desafios enfrentados pelos discentes.

Ao adotar uma perspectiva quali-quantitativa, e buscado não apenas quantificar dados, mas também compreender os contextos, motivações e percepções dos alunos da EJA em relação à segurança digital. A interseção dessas abordagens permite uma análise mais rica e contextualizada, considerando a complexidade do comportamento humano diante dos desafios cibernéticos.

### **3.2.1 Coleta de Dados**

A coleta de dados se deu por meio de questionário objetivo com questões semiestruturadas, baseado em estudos anteriores. O questionário avalia a probabilidade dos participantes de serem alvos de ataques virtuais por meio de esquemas de engenharia social, esta etapa contribuiu para a obtenção de dados relevantes.

### **3.2.2 Análise de Dados**

Após a coleta de dados, realizou-se uma análise para estimar a predisposição dos discentes da EJA a prováveis ataques cibernéticos e sociais, bem como as vulnerabilidades identificadas no questionário respondido.

### 3.2.3 Pesquisa-ação

Na pesquisa-ação, os estudantes da EJA serão envolvidos ativamente na identificação dos desafios enfrentados em relação à segurança digital, na concepção de estratégias de conscientização e na implementação de medidas preventivas. Por meio de questionários, reuniões e debates participativos, busca-se compreender as necessidades e experiências individuais dos alunos, permitindo uma análise mais aprofundada das questões de segurança digital e a co-criação de soluções eficazes.

### 3.3 Etapas do Projeto

**Primeira etapa:** Pesquisa Bibliográfica.

Através da plataforma *google* acadêmico foi feita uma pesquisa, análise e seleção de material já publicados trabalhos acadêmicos.

**Segunda etapa:** Reunião com os professores.

Interação direta com os educadores para se ter uma visão mais profunda sobre o problema observado, isso inclui debates sobre a segurança digital e computacional na EJA, podendo incluir sugestões de medidas de prevenção a serem incluídas, campanhas educativas e *insights*.

**Terceira etapa:** Aplicação de um questionário.

Usado para obter informações dos discentes sobre segurança digital.

**Quarta etapa:** Reuniões com os participantes.

Foi realizado sessões com interações diretas com os estudantes da EJA, tornando possível discutir de forma individual as suas preocupações e dificuldades em relação à segurança digital e computacional.

**Quinta etapa:** Debate com os discentes.

Para criação do cartaz, foram feitas discussões interativas para envolvê-los na criação do cartaz sobre prevenção de segurança digital. Isso permite que eles

compartilhem ideias, sugestões e experiências para garantir que o conteúdo seja relevante, eficaz e de fácil compreensão.

**Sexta etapa:** Tabulação dos dados.

Organizar de forma sistemática os dados coletados com o questionário e as reuniões, para facilitar a compreensão dos dados e prepará-los para a análise.

**Sétima etapa:** Análise de Dados.

Analisar os dados obtidos para identificar padrões, tendências e insights relevantes para a pesquisa.

**Oitava etapa:** Confeção do cartaz educativo.

Combinação de todos os dados analisados, suas tendências e insights para criação de um material visual eficaz, trazendo conceitos da temática da pesquisa, como prevenção, vulnerabilidades no manuseio dos dados pessoais e o uso adequado das TDIC's, que serão expostos em elementos visuais de fácil compreensão para os próximos educandos da EJA.

## **4 RESULTADOS E DISCURSÕES.**

Após o fim de cada etapa do projeto, foram obtidos dados significativos que visam contribuir para um resultado favorável no fim do projeto, tornando assim cada etapa importante para alcançar o objetivo final, desse modo é possível examinar de perto a eficácia das estratégias aplicadas, visando aprimorar a conscientização e proteção dos discentes frente aos desafios digitais.

### **4.1 Questionário**

Participaram do questionário qualitativo 14 alunos da EJA, pertencentes à Turma 2 da 10ª etapa de uma escola estadual do município de Coari/AM, durante o dia 17 de novembro. Os participantes responderam o questionário com 15 quinze perguntas, forneceram respostas utilizando as opções "sim", "não" e, caso não possuíssem conhecimento ou experiência sobre determinada questão, selecionavam "não sei informar", conforme detalhado na Tabela 1.

**Tabela 1** – Agrupamento das perguntas com base nos tipos de vulnerabilidade na segurança digital.

<b>Perguntas por Tipos de vulnerabilidade</b>	<b>Sim</b>	<b>Não</b>	<b>Não sei informar</b>
<b>Contato Telefônico</b>			
1 - Costuma fornecer informações pessoais por meio de telefone?	3	11	0
2 - Esses números geralmente solicitam informações pessoais ou dados sobre onde você trabalha?	4	9	1
3 - Você costuma atender chamadas de números desconhecidos?	8	6	0
<b>Internet e Redes Sociais</b>			
4 - Você costuma compartilhar fotos com colegas de trabalho em suas redes sociais?	6	8	0
5 - Você costuma responder a pessoas desconhecidas que iniciam uma conversa nas redes sociais?	8	6	0
6 - Em seus perfis de redes sociais, você costuma informar o local onde trabalha e qual é o seu cargo?	1	13	0
7 - No seu ambiente de trabalho, você tem acesso às redes sociais (Facebook, Instagram, Twitter)?	3	11	0
8 - É possível encontrar informações sobre sua empresa ou local de trabalho na Internet?	3	9	2
<b>Phishing</b>			
9 - Você costuma assinar os e-mails que recebe, ou eles chegam sem que você tenha solicitado?	5	9	0
10 - Já aconteceu de você fazer o download de algum arquivo de um e-mail sem perceber?	3	9	2
11 - Você já recebe algum e-mail pedindo para fornecer informações pessoais, mesmo sem saber de onde esse e-mail veio?	3	9	2
12 - Você costuma receber mensagens de bancos e lojas?	4	9	1
<b>Engenharia social</b>			
13 - Você costuma ir a bares, academias ou outros lugares após o seu trabalho?	6	8	0
14 - Você costuma falar sobre o seu trabalho com amigos ou até mesmo com pessoas que você não conhece?	4	10	0
15 - Você costuma fazer amizades com facilidade?	8	5	1

**Fonte:** Autoria própria, 2024.

A apresentação dos resultados será fundamentada na categoria de resposta Sim, que foi o ponto de foco nas respostas obtidas. Posteriormente à categorização



dos dados, foram elaborados gráficos sumarizados, considerando o conjunto de dados agrupados conforme as falhas humanas, portanto e fundamental a análise de variáveis pré-determinadas para compreender seu impacto por meio de frequências e correlações estatísticas, permite ao pesquisador descrever, explicar e prever fenômenos (PITANGA, 2020).

#### 4.1.1 Resultados de possíveis ataques decorrentes de interação telefônica

A abordagem por telefone para obtenção de informações pessoais é uma tática comum, na qual os golpistas se passam por entidades legítimas para enganar as vítimas e obter dados sensíveis. Geraldo e Takeda (2019, p.249), afirmam que, “Recentemente, invasores utilizam esses meios para fazer vítimas, se passando por alguma pessoa e assim colocando seu plano em prática para enganar o alvo”. A Tabela 2, demonstra os dados adquiridos com o questionário.

**Tabela 2** – Demonstração das respostas que indicam possíveis ataques decorrentes de contato telefônica.

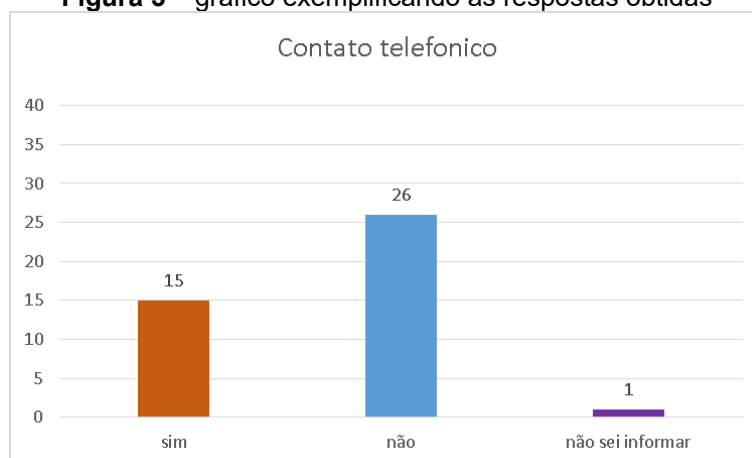
<b>Contato Telefônico</b>	<b>Sim</b>	<b>Não</b>	<b>Não sei informar</b>
Costuma fornecer informações pessoais por meio de telefone?	3	11	0
Esses números geralmente solicitam informações pessoais ou dados sobre onde você trabalha?	4	9	1
Você costuma atender chamadas de números desconhecidos?	8	6	0
<b>Soma das respostas que caracterizam sim, não e não sei informar</b>	<b>15</b>	<b>26</b>	<b>1</b>
<b>Total de todas as perguntas somadas e o seu valor (%)</b>	<b>42 = 100 %</b>		
<b>Condensação e apresentação dos resultados obtidos a partir de respostas que poderiam caracterizar ataques baseados em Abordagem Pessoal.</b>	<b>27%</b>	<b>64%</b>	<b>9%</b>

**Fonte:** Autoria própria, 2024.

Na análise da Tabela 2, foi somado o número de respostas "sim", totalizando 15 (quinze), o número de respostas "não", totalizando 26 (vinte e seis), e o número de respostas "não sei informar", totalizando 1 (um). A soma de todas as perguntas resultou em 42 (quarenta e dois) respostas, equivalente a 100% das perguntas. A compilação dos valores revela que 64% dos usuários responderam "não", indicando boas práticas de segurança dos dados e eficaz proteção contra ataques telefônicos. Isso é uma notícia positiva. No entanto, preocupa o fato de que 27% responderam

"sim", indicando possíveis vítimas. o gráfico em torre da figura 5, ilustras os valores obtidos.

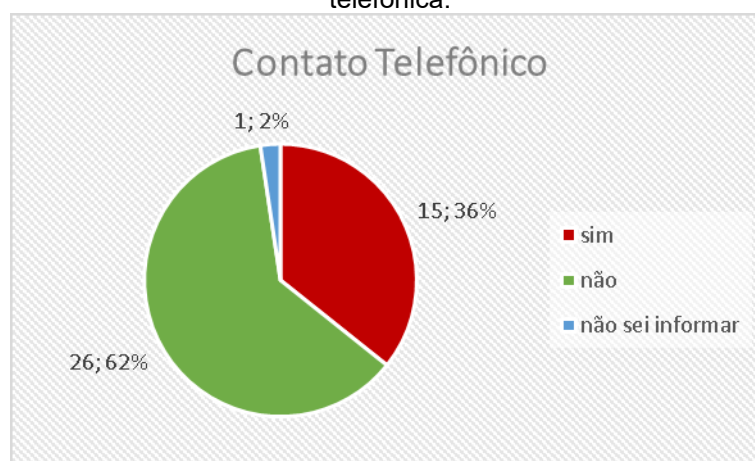
**Figura 5** – gráfico exemplificando as respostas obtidas



**Fonte:** Autoria própria, 2024.

Através de dados básicos da vítima, como nomes e endereços, é viável extrair informações cruciais ou até mesmo assumir falsamente papéis, como o de um gerente, para induzir a vítima, sem que ela perceba, a realizar transferências financeiras em ataques de engenharia social (Geraldo e Takeda , 2019), a figura 6 demonstra de forma resumida os dados obititos com a Tabela 2.

**Figura 6** – Resumo das respostas que indicam possíveis ataques decorrentes de interação telefônica.



**Fonte:** Autoria própria, 2024.

Os dados apresentados no gráfico da imagem 6, revela que 36% são potenciais vitimas, enquanto 62%, puderam mitigar possíveis ataques. Adicionalmente, 2% das respostas não têm certeza ou não se sentem informados sobre esse tipo de experiência.

#### 4.1.2 Resultados de possíveis ataques decorrentes internet e redes sociais

Neste tópico são apresentados os resultados obtidos das questões relacionadas a possíveis ataques provenientes da internet e das redes sociais, de acordo com a Tabela 3, a seguir.

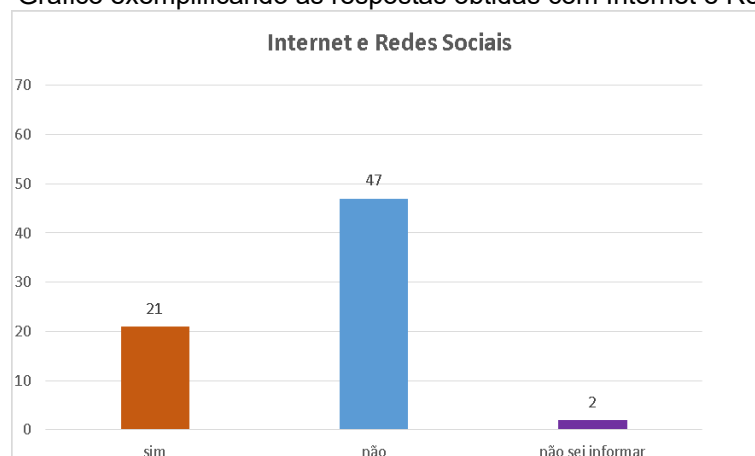
**Tabela 3** – Demonstração das respostas que indicam possíveis ataques decorrentes de internet e redes sociais.

<b>Internet e Redes Sociais</b>	<b>Sim</b>	<b>Não</b>	<b>Não sei informar</b>
Você costuma compartilhar fotos com colegas de trabalho em suas redes sociais?	6	8	0
Você costuma responder a pessoas desconhecidas que iniciam uma conversa nas redes sociais?	8	6	0
Em seus perfis de redes sociais, você costuma informar o local onde trabalha e qual é o seu cargo?	1	13	0
No seu ambiente de trabalho, você tem acesso às redes sociais (Facebook, Instagram, Twitter)?	3	11	0
É possível encontrar informações sobre sua empresa ou local de trabalho na Internet?	3	9	2
<b>Soma das respostas que caracterizam sim, não e não sei informar</b>	<b>21</b>	<b>47</b>	<b>2</b>
<b>Total de todas as perguntas somadas e o seu valor (%)</b>	<b>70 = 100%</b>		
<b>Condensação e apresentação dos resultados obtidos a partir de respostas que poderiam caracterizar ataques baseados em internet e redes sociais.</b>	<b>30%</b>	<b>67%</b>	<b>3%</b>

**Fonte:** Autoria própria, 2024.

Foi somado o número de respostas "sim", totalizando 21 (vinte e um), o número de respostas "não", totalizando 47 (quarenta e sete), e o número de respostas "não sei informar", totalizando 3 (tres). A soma de todas as perguntas resultou em 71 (setenta e um) respostas, equivalente a 100% das perguntas. A compilação dos valores revela que 67% dos usuários responderam "não", indicando boas práticas de segurança dos dados e eficaz proteção contra ataques por via da internet e dedes sociais, enquanto 30% responderam "sim", indicando possíveis vítimas. a figura 7 demonstra de forma resumida os dados obititos com a Tabela 3.

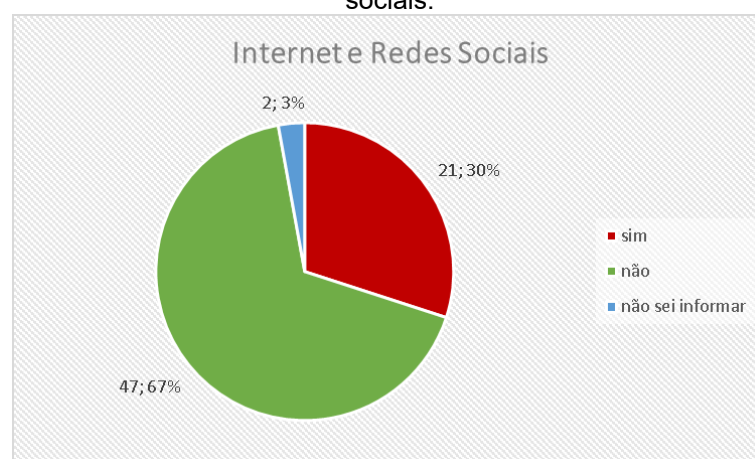
**Figura 7** – Gráfico exemplificando as respostas obtidas com Internet e Redes Sociais



**Fonte:** Autoria própria, 2024.

Vale resaltar que este gráfico faz relação com práticas relacionadas a internet e redes social podendo existir outras práticas como contato através de telefonemas e abordagens diretas através de contatos pessoais, Manter senhas pessoais e profissionais separadas pode criar dificuldades no acesso, especialmente para pessoas com pouco conhecimento em segurança de dados, aumentando o risco de diferentes formas de ataques (Geraldo e Takeda, 2019), a figura 7, demonstra de forma resumida os dados obtidos com a tabela 3.

**Figura 8** – Resumo das respostas que indicam possíveis ataques decorrentes de Internet e Redes sociais.



**Fonte:** Autoria própria, 2024.

Os dados apresentados no gráfico da imagem 8, revela que 30% são potenciais vítimas, enquanto 67%, puderam se defender de prováveis ataques. Adicionalmente, 3% dos respondentes não têm certeza ou não se sentem informados sobre esse tipo de experiência.

### 4.1.3 Resultados de possíveis ataques decorrentes de *phishing*

Resultados obtidos a partir das perguntas relacionadas a prática de *phishing*, a Tabela 4 demonstra os resultados.

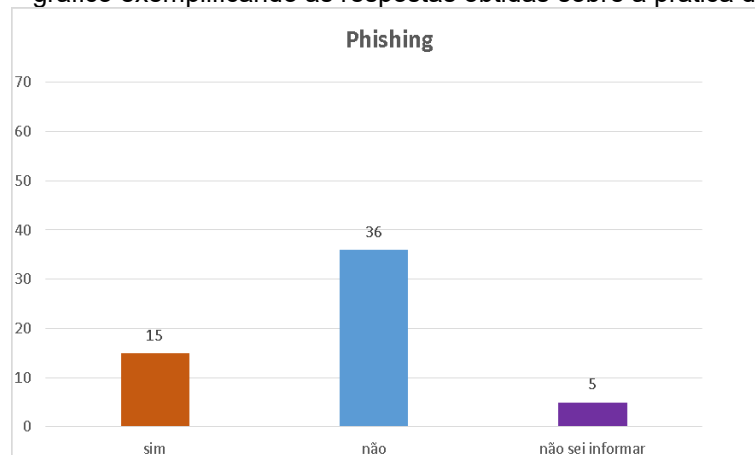
**Tabela 4** – Demonstração das respostas que indicam possíveis ataques decorrentes de *phishing*.

Phishing	Sim	Não	Não sei informar
Você costuma assinar os e-mails que recebe, ou eles chegam sem que você tenha solicitado?	5	9	0
Já aconteceu de você fazer o download de algum arquivo de um e-mail sem perceber?	3	9	2
Você já recebe algum e-mail pedindo para fornecer informações pessoais, mesmo sem saber de onde esse e-mail veio?	3	9	2
Você costuma receber mensagens de bancos e lojas?	4	9	1
Soma das respostas que caracterizam sim, não e não sei informar	15	36	5
Total de todas as perguntas somadas e o seu valor (%)	56 = 100%		
Condensação e apresentação dos resultados obtidos a partir de respostas que poderiam caracterizar ataques baseados <i>phishing</i>	27%	64%	9%

Fonte: Autoria própria, 2024.

Foi somado o número de respostas "sim", totalizando 15 (quinze), o número de respostas "não", totalizando 36 (trinta e seis), e o número de respostas "não sei informar", totalizando 5 (cinco). A soma de todas as perguntas resultou em 56 (cinquenta e seis) respostas, equivalente a 100% das perguntas. A compilação dos valores revela que 64% dos usuários responderam "não", indicando boas práticas de segurança dos dados e eficaz proteção contra ataques derivados de *phishing*, é que 27% responderam "sim", indicando possíveis vítimas desta prática. a figura 9 demonstra de forma resumida os dados obtidos com a Tabela 4.

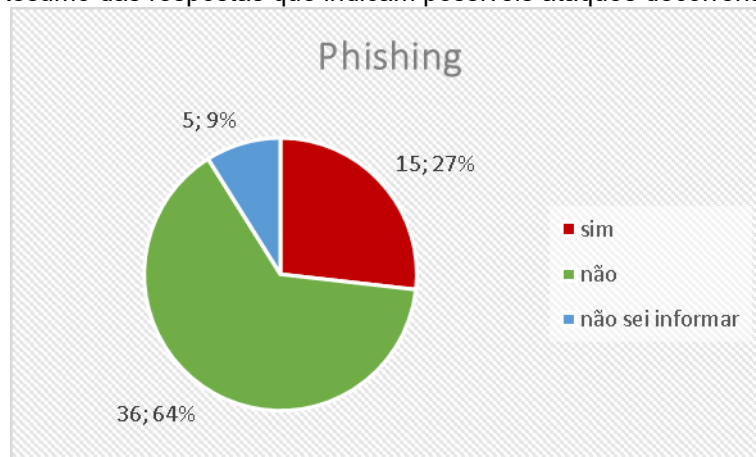
**Figura 9** – gráfico exemplificando as respostas obtidas sobre a prática de *Phishing*



Fonte: Autoria própria, 2024.

Estes resultados ressaltam a importância crucial de conscientizar e educar os docentes sobre os métodos e estratégias empregados pelos criminosos cibernéticos, como os sinais de phishing, mitigando os riscos e protegendo os usuários contra essa ameaça virtual, a Figura 10 demonstra de forma resumida os dados obtidos com a tabela 4.

**Figura 10** – Resumo das respostas que indicam possíveis ataques decorrentes de *phishing*.



**Fonte:** Autoria própria, 2024.

Os dados apresentados no gráfico da Figura 10, revela que 27% são potenciais vítimas, enquanto 64%, puderam se defender de prováveis ataques. Adicionalmente, 9% dos respondentes não têm certeza ou não se sentem informados sobre esse tipo de experiência.

#### **4.1.4 Resultados de possíveis ataques decorrentes de abordagem através de engenharia social**

Resultados obtidos com as respostas relacionadas à prática de engenharia social. A Tabela 5 demonstra os resultados.

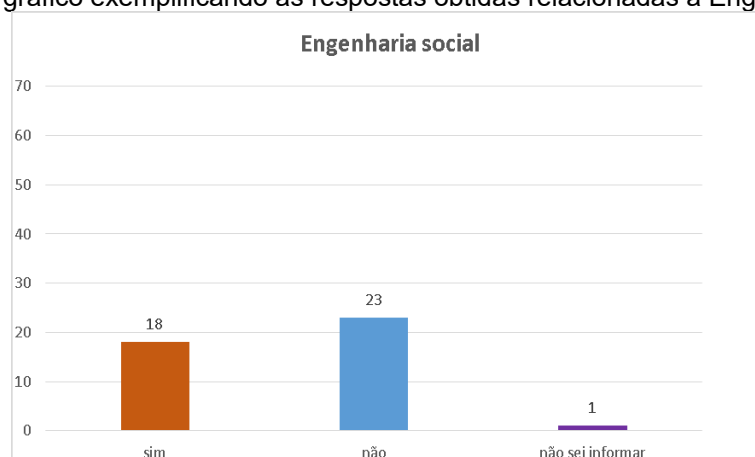
**Tabela 5** – Demonstração das respostas que indicam possíveis ataques decorrentes de engenharia social.

Engenharia social	Sim	Não	Não sei informar
Você costuma ir a bares, academias ou outros lugares após o seu trabalho?	6	8	0
Você costuma falar sobre o seu trabalho com amigos ou até mesmo com pessoas que você não conhece?	4	10	0
Você costuma fazer amizades com facilidade?	8	5	1
Soma das respostas que caracterizam sim, não e não sei informar	18	23	1
Total de todas as perguntas somadas e o seu valor (%)	42 = 100%		
Condensação e apresentação dos resultados obtidos a partir de respostas que poderiam caracterizar ataques de engenharia social	43%	55%	2%

Fonte: Autoria própria, 2024.

Foi somado o número de respostas "sim", totalizando 18 (dezoito), o número de respostas "não", totalizando 23 (vinte e tres), e o número de respostas "não sei informar", totalizando 1 (um). A soma de todas as perguntas resultou em 42 (quarenta e dois) respostas, equivalente a 100% das perguntas. A compilação dos valores revela que 55% dos usuários responderam "não", indicando boas práticas de segurança dos dados e eficaz proteção contra ataques derivados de *phishing*, é que 43% responderam "sim", indicando possíveis vítimas desta pratica, enquanto 2% responderam "nã sei informar" a Figura 11 demonstra de forma resumida os dados obititos com a Tabela 5.

**Figura 11** – gráfico exemplificando as respostas obtidas relacionadas a Engenharia Social

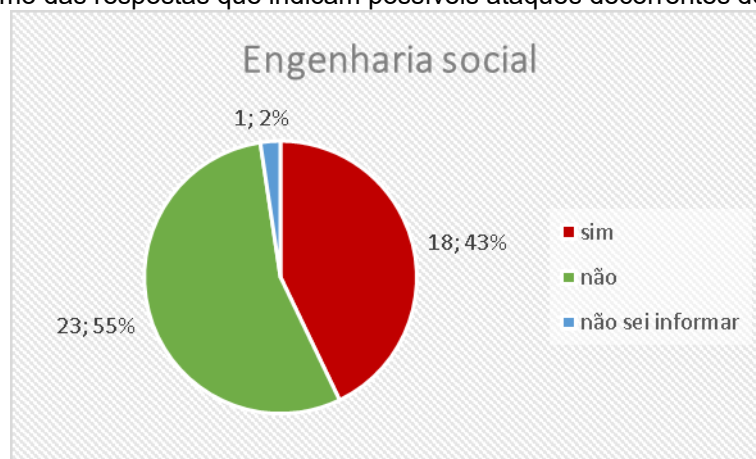


Fonte: Autoria própria, 2024.

Engenharia social explora pessoas que fazem amizades rapidamente, manipulando a confiança e explorando anseios sociais, como a necessidade de

interagir em um grupo ou dificuldades financeiras. A prática se aproveita da facilidade em estabelecer amizades, visando manipular a confiança das pessoas, (Geraldo e Takeda, 2019), a Figura 12, demonstra de forma resumida os dados obtidos com a tabela 5.

**Figura 12** – Resumo das respostas que indicam possíveis ataques decorrentes de engenharia social.

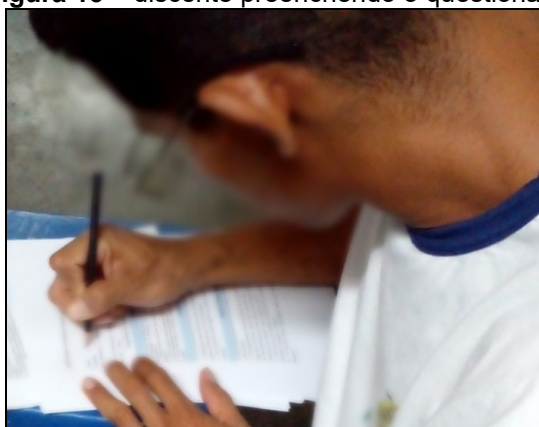


**Fonte:** Autoria própria, 2024.

Os dados apresentados no gráfico da Imagem 12, revela que 43% são potenciais vítimas quase a metade dos discentes, enquanto 55%, puderam se defender de prováveis ataques. Adicionalmente, 2% dos respondentes não têm certeza ou não se sentem informados sobre esse tipo de experiência.

Os dados obtidos com o questionário foram analisados e somados com os resultados das reuniões para se ter uma visão mais completa sobre as dificuldades dos educandos. A Figura 13, logo abaixo demonstra um dos discentes.

**Figura 13** – discente preenchendo o questionário



**Fonte:** acervo do autor



## **4.2 Reuniões**

O objetivo principal das reuniões realizadas nos dias 31 de novembro e 01 de dezembro foi promover uma discussão aprofundada sobre o tema de segurança digital. Nesses encontros, os alunos expressaram dúvidas, compartilharam experiências e discutiram questões relacionadas à segurança online.

O intuito era proporcionar um espaço de diálogo que permitisse compreender melhor as preocupações e vivências dos discentes em relação à segurança digital, contribuindo assim para a elaboração de estratégias e materiais informativos mais alinhados às suas necessidades e realidades. Abordando o princípio dialógico para superar concepções baseadas em um falso dualismo (PITANGA, 2020).

### **4.2.1 Resultado da reunião do primeiro dia**

Durante o primeiro dia, participaram um total de 5 discentes que compartilharam suas experiências. Houve um aluno que relutou em se expor; no entanto, ao longo da reunião, tornou-se mais à vontade, especialmente quando começou a compartilhar experiências pessoais.

O Grupo Focal utiliza então, da interação grupal para produzir saberes e apreender fatos e acontecimentos que poderiam ser menos acessíveis sem a interação vivenciada em um grupo específico, constituído com essa intenção. (Oliveira et al. 2020, p. 12).

Durante as entrevistas, a maioria dos alunos expressou uma preocupação comum relacionada a golpes, como fraudes bancárias e golpes por meio de aplicativos móveis. O Quadro 2 ilustra os principais riscos relatados pelos discentes.

Quadro 2 – Resultado das reunião e entrevista com discentes

QUADRO DEMONSTRATIVO DE EXPERIÊNCIAS					
Vivências Pessoais	Quant.	Característica	Engenharia social	Phishing	Abordagem virtual
Já foram vítimas de golpe relacionado a smartphone	4	Financeiro	X	X	X
Conhecem pelo menos uma pessoa que já foram vítima de algum tipo de ataque	4	Sequestro de informação	-	X	X
Já foram alvo de algum ataque relacionado a computadores	4	MSG desconhecidas	-	X	X
Não souberam responder	1	Nada	-	-	-

Fonte: Autoria própria, 2024.

O Quadro 2 apresenta uma síntese das experiências dos discentes em relação à segurança digital. Dos participantes, 2 alunos relataram ter sido vítimas de golpes financeiros, enquanto 4 conhecem alguém que foi alvo de algum tipo de ataque, destacando-se casos de sequestro de informação. Além disso, 4 alunos foram alvo de abordagens de engenharia social, principalmente por meio de mensagens desconhecidas. Uma pessoa não soube responder, pois não tinha noções sobre a temática de segurança digital. Na Figura 14 podemos ver o relato de um dos alunos.

Figura 14 – discente relatado as experiências sobre a segurança digital



Fonte: acervo do autor

Pode-se notar que a correlação entre as experiências dos participantes está entrelaçada com as principais práticas de crimes virtuais, engenharia social e *phishing*. Dentre as experiências propostas pelos discentes e destacada a seguintes:

- **Já foram vítimas de golpe relacionado a smartphone:** este se destacou pelo fato dele se um dos mais citados pelos discentes além de conter os principais pontos abordados na segurança digital, como o uso da engenharia social o *phishing* e ter uma abordagem através de meios virtuais.

Este ponto será aprofundado com mais detalhes no próximo tópico que irá descrever como ele irá contribuir para a criação do cartaz. Na Figura 15, pode-se notar uma aluna durante as entrevistas.

**Figura 15** – discente relatando as suas experiências sobre segurança



Fonte: acervo do autor

#### 4.2.2 Reunião para planeja o um cartaz

Durante a última reunião em 01 de dezembro, os 11 alunos participantes colaboraram ativamente no planejamento de um cartaz destinado às salas de aula da EJA. Suas contribuições incluíram a definição dos tópicos que o cartaz deveria abordar, visando promover uma conscientização efetiva sobre segurança digital. Como discorre.

Nessa perspectiva, apontamos a importância da inserção de visões epistemológicas contemporâneas, pois estas têm consigo elementos que visam superar o pensamento moderno, dentre os quais: pensamento complexo e a utilização de operadores cognitivos como: os princípios dialógicos e da recursividade. Pitanga (2020, p. 198).

Ao incorporar visões epistemológicas contemporâneas, promovemos um ambiente de aprendizado que vai além do pensamento tradicional, estimulando a

compreensão complexa e o diálogo entre os estudantes, fundamentais para uma melhor interação entre a segurança digital e as metodologias de ensino fazendo com que os discentes participem das atividades, de acordo com a imagem 1

Ao final do último dia de reunião, foi proposto que os discentes opinassem sobre os temas, trazendo à discussão propostas para melhorar o entendimento e a conscientização de futuras turmas da EJA. Dentre os pontos escolhidos por eles, estão:

- Senhas e métodos de proteção.
- Compras online.
- Vírus e roubo de senhas.
- Mensagens de origem desconhecida pelo usuário.

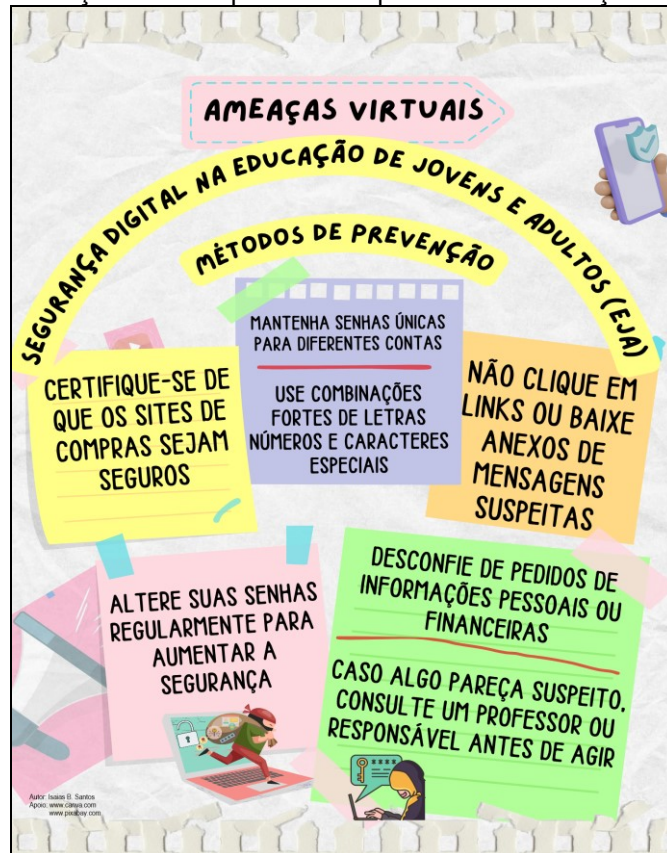
Esses pontos foram selecionados pelos estudantes, pois, ao estarem mais conscientes das práticas de violação de segurança no mundo virtual, acreditam que serão de grande ajuda para futuros estudantes da EJA. O cartaz produzido ficará na sala de aula da turma da EJA.

Os seguintes pontos foram destacados pelo questionário, tendo como agravante o fato de suas estatísticas terem afetado uma parte expressiva dos discentes de acordo com a figura1 e figura1 apresentadas anteriormente.

- *Phishing*
- *Engenharia social*

Com base nestes dados, pode-se reunir informações valiosas que, além de oferecer estatísticas relevantes, também contribuirão para a criação de um cartaz. Este tem como objetivo conscientizar de forma lúdica sobre os perigos que os discentes podem enfrentar ao utilizar algum tipo de tecnologia capaz de armazenar informações pessoais, a Figura 16 retrata o esboço do cartaz.

Figura 16 – esboço do cartaz produzido a partir das contribuições dos discentes.



Fonte: Autoria própria, 2024.

O cartaz aborda temáticas como compras online, a atenção necessária com as senhas de redes sociais e de dispositivos de comunicação, destacando a importância de evitar descuidos ao clicar em links de terceiros. Além disso, enfatiza a necessidade de confiabilidade ao lidar com informações pessoais, a Figura 17 demonstra o cartaz em sala de aula.

Figura 17 – Cartaz exposto em sala de aula.



Fonte: Autoria própria, 2024.

## 5 CONCLUSÃO E TRABALHOS FUTUROS

Diante dos dados obtidos e das pesquisas acadêmicas analisadas, é possível concluir que a temática de "Segurança Digital na Educação de Jovens e Adultos" revela desafios significativos. A vulnerabilidade expressa pelos discentes da EJA destaca a relevância de estratégias de prevenção e conscientização. A promoção da conscientização das pessoas com pouca instrução torna-se essencial para que os usuários possam mitigar riscos e vulnerabilidades exploradas pela engenharia social (Geraldo e Takeda, 2019).

Portanto a aplicação de métodos como reuniões e questionários evidenciou a necessidade de abordagens específicas, considerando a diversidade de experiências e conhecimentos dos alunos. Propõe-se a implementação de palestras regulares para conscientização, visando capacitar os membros da instituição a identificarem e evitar ataques dessa natureza (Geraldo e Takeda, 2019).

Os trabalhos correlatos examinados indicam que a segurança digital é uma preocupação crescente, exigindo soluções proativas. A abordagem dialógica e participativa adotada durante as reuniões está em consonância com propostas pedagógicas contemporâneas, reconhecendo a importância do envolvimento ativo dos alunos.

As limitações da pesquisa indicam uma notável evasão dos discentes ao longo do estudo, com uma variação considerável na quantidade de participantes desde o início até o término da coleta de dados. Essa evasão pode impactar a pesquisa de várias maneiras, incluindo a diminuição do tamanho da amostra e, conseqüentemente, a representatividade dos resultados. Além disso, a redução no número de participantes pode afetar a profundidade e a abrangência dos relatos de experiências, limitando a compreensão holística do fenômeno investigado.

...é imprescindível salientar que o Grupo Focal pode, então, ser conceituado como uma técnica de investigação que tem por finalidade precípua obter informações de natureza descritiva, oriundas da interação entre os participantes de um determinado grupo, durante a realização de um debate sobre assunto de interesse do pesquisador. Oliveira et al. (2020, p.12)

A criação do cartaz com foco nos pontos críticos, como *phishing* e engenharia social, é uma iniciativa valiosa para ampliar a compreensão dos discentes sobre os riscos digitais. Este estudo destaca a relevância contínua da educação em segurança digital na EJA e abre caminho para investigações mais aprofundadas e aprimoramento das estratégias preventivas através de debates e exposições.

Como trabalho futuro, propõe-se a continuidade dessas práticas preventivas, com destaque para a ampliação e adaptação das estratégias de conscientização por meio de interações pessoais e exposições. Isso implica na análise contínua de novas experiências e na adaptação de conceitos emergentes, considerando o constante avanço tecnológico. Novas abordagens podem ser desenvolvidas, incluindo a criação de materiais audiovisuais com conceitos simplificados e de fácil compreensão, especialmente direcionados aos discentes da EJA.

## REFERÊNCIAS

ALVES, William roger da silva; FREITAS, Marcio. SEGURANÇA DA INFORMAÇÃO E OS DESAFIOS DA NOSSA SOCIEDADE PERANTE AS NOVAS TECNOLOGIAS. **SEMINÁRIO DE TECNOLOGIA GESTÃO E EDUCAÇÃO**, v. 3, n. 1, 2021. Disponível em: <https://raam.alcidesmaya.edu.br/index.php/SGTE/article/view/336>. Acesso em: 15 ago. 2023.

AMARAL, Fabrícia Santana de Souza; PALOMAR, Meire Terezinha Müller. OS DESAFIOS DE ENSINO-APRENDIZAGEM NA EDUCAÇÃO DE JOVENS E ADULTOS - OS ESTUDANTES EJA NO BRASIL. **Revista Eletrônica FACP**, [S.I.], n. 23, 2023. Disponível em: <https://revistaunifacp.com.br/revista/index.php/reFACP/article/view/102>. Acesso em: 10 ago. 2023.8

ARAÚJO, Atalia de. EDUCAÇÃO FINANCEIRA NA EDUCAÇÃO BÁSICA: UMA PROPOSTA DIDÁTICA A PARTIR DO LETRAMENTO FINANCEIRO. **Universidade Federal do Tocantins**, [S.I.], 2023. Disponível em: <http://hdl.handle.net/11612/4695>. Acesso em: 20 ago. 2023.

APP-VR. Como se proteger de crimes virtuais? **G1**, Disponível em: <https://g1.globo.com/rj/sul-do-rio-costa-verde/especial-publicitario/aap-vr-associacao-dos-aposentados-e-pensionistas-de-volta-redonda/viver-saudavel/noticia/2023/11/16/como-se-proteger-de-crimes-virtuais.ghtml>. Acessado em 22 de Dez. 2023

BELEZA, Janderlane Oliveira; NOGUEIRA, Eulina Maria Leite. CONTEXTO HISTÓRICO DA EDUCAÇÃO DE JOVENS E ADULTOS NO BRASIL. **Revista Ensino de Ciências e Humanidades-Cidadania, Diversidade e Bem-Estar-RECH**, [S.I.], v. 4, n. 2, jul-dez, p. 107-126, 2020. Disponível em: <https://periodicos.ufam.edu.br/index.php/rech/article/view/7958>. Acesso em: 20 ago. 2023.

FONSECA FILHO, Clézio. HISTÓRIA DA COMPUTAÇÃO: O CAMINHO DO PENSAMENTO E DA TECNOLOGIA. **EDIPUCRS**, Porto Alegre, [S.I.], p.205, 2007.

FREIRE, Paulo. PEDAGOGIA DA AUTONOMIA: SABERES NECESSÁRIOS À PRÁTICA EDUCATIVA. São Paulo: Paz e Terra, 1996.

Garcia, Amanda. Especialista dá dicas de como educar filhos para que identifiquem riscos da internet, **CNN Brasil**. Disponível em: <https://www.cnnbrasil.com.br/nacional/especialista-da-dicas-de-como-educar-filhos-para-que-identifiquem-riscos-da-internet/>. Acessado em 22 de Dez. 2023.

GERALDO, Vinicius da Silva; TAKEDA, Fábio Bento. ENGENHARIA SOCIAL: UM PERIGO OCULTO EM SIMPLES TÉCNICAS. **Revista Interface Tecnológica**, [S.I.], v. 16, n. 1, p. 242-253, 2019. Disponível em:



<https://revista.fatectq.edu.br/interfacetecnologica/article/view/620>. Acesso em: 28 jul. 2023.

Gomes, Victor Lopes. Quais os principais riscos na internet em 2024? Hackers respondem. **Olhar Digital**, 10/12/2023 07h00. Disponível em: <https://olhardigital.com.br/2023/12/10/seguranca/quais-os-principais-riscos-na-internet-em-2024-hackers-respondem/>. Acessado em 22 de Dez. 2023

LEITE, Débora Cristina de Freitas. CYBERBULLYING E EDUCAÇÃO: PERSPECTIVAS DA PRODUÇÃO ACADÊMICA NACIONAL. **Centro Universitário Sagrado Coração – UNISAGRADO**, 2022. Disponível em: <https://repositorio.unisagrado.edu.br/jspui/handle/handle/1260>. Acesso em: 28 jul. 2023.

NASCIMENTO, G. A. de M.; SANTOS, J. N.; EDLER, G. O. B. A IMPORTÂNCIA DO COMBATE À DESINFORMAÇÃO E A ATUALIZAÇÃO DO CÓDIGO PENAL PARA CRIMES VIRTUAIS DE ENGENHARIA SOCIAL/PHISHING. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S.l.], v. 8, n. 11, p. 2225–2233, 2022. DOI: 10.51891/rease.v8i11.7809. Disponível em: <https://periodicorease.pro.br/rease/article/view/7809>. Acesso em: 28 jul. 2023.

NEVES, Raquel Alexandra Carvalho. VITIMAÇÃO POR PHISHING: UM ESTUDO EMPÍRICO. **Repositório Aberto da Universidade do Porto**, [S.l.], 2022. Disponível em: <https://hdl.handle.net/10216/145534>, Acesso em: 25 set. 2023.

OLIVEIRA, G. S.; CUNHA, A. M. O.; CORDEIRO, E. M.; SAAD, N. S. GRUPO FOCAL: UMA TÉCNICA DE COLETA DE DADOS NUMA INVESTIGAÇÃO QUALITATIVA? In: **Cadernos da Fucamp**, UNIFUCAMP, v.19, n.41, p.1-13, Monte Carmelo, MG, 2020. Disponível em: <https://revistas.fucamp.edu.br/index.php/cadernos/article/view/2208>. Acesso em: 22 jan. 2023.

PEDROSO, Reinaldo Vitor, et al. ENGENHARIA SOCIAL: O VÍNCULO MAIS FRÁGIL DA SEGURANÇA. **Universidade Federal de Minas Gerais**, 2019. Disponível em: <http://hdl.handle.net/1843/38347>. Acesso em: 04 ago. 2023.

PITANGA, Ângelo Francklin. PESQUISA QUALITATIVA OU PESQUISA QUANTITATIVA: REFLETINDO SOBRE AS DECISÕES NA SELEÇÃO DE DETERMINADA ABORDAGEM. **Revista Pesquisa Qualitativa**, [S. l.], v. 8, n. 17, p. 184–201, 2020. DOI: 10.33361/RPQ.2020.v.8.n.17.299. Disponível em: <https://editora.sepq.org.br/rpq/article/view/299>. Acesso em: 22 jan. 2024.

QUARESMA, Rafael De Jesus Correa et al.. A EDUCAÇÃO DE JOVENS E ADULTOS (EJA) E OS SUJEITOS DESSA MODALIDADE DE ENSINO. Anais VI CONEDU... Campina Grande: **Realize Editora**, 2019. Disponível em: <https://www.editorarealize.com.br/artigo/visualizar/58223>. Acesso em: 23 de Jan. 2024

RODRIGUES, Tatiane Daby de Fatima Faria; OLIVEIRA, Guilherme Saramago de; DOS SANTOS, Josely Alves. AS PESQUISAS QUALITATIVAS E QUANTITATIVAS NA EDUCAÇÃO. **Revista Prisma**, v. 2, n. 1, p. 154-174, 2021.

REUTERS, TECNOLOGI. Golpes online atingem 'níveis recordes' na América Latina com falta de segurança digital. **R7**. Disponível em: <https://noticias.r7.com/tecnologia-e-ciencia/latino-americanos-sao-vitimas-de-mais-golpes-online-com-falta-de-seguranca-digital-15082023>. Acessado em 22 de Dez. 2023.

SALVIANO, Edgard Mesquita; SANTOS, João Pedro Ribeiro; SILVA, Matheus Almeida. PRINCIPAIS TIPOS DE ATAQUES PHISHING E MECANISMOS DE SEGURANÇA. **Centro Universitário do Planalto Central Aparecido dos Santos**, 2022. Disponível em: <https://dspace.uniceplac.edu.br/handle/123456789/1611>. Acesso em: 02 set. 2023.

SANTOS, Tânia Cristina Alves dos; RODRIGUES, Karen Lúcia Abreu. IMPACTOS DAS REDES SOCIAIS EM RELAÇÃO À AUTOESTIMA E AUTOIMAGEM. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S.l.], v. 9, n. 3, p. 851-862, 2023. Disponível em: <https://periodicorease.pro.br/rease/article/view/8724>. Acesso em: 29 jul. 2023.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. FUNDAMENTOS JUSFILOSÓFICOS E ÂMBITO DE PROTEÇÃO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS. **Revista Direito Público**, [S.l.], v. 17, n. 18, p. 33-57, 2020. Disponível em: <https://hdl.handle.net/10923/18861>, Acesso em: 26 set. 2023.

SOUZA, Fábio Benedito de. USUÁRIO, O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO. **Revista Scientia Alpha**, [S.l.], v. 3, n. 03, 2022. Disponível em: <https://revista.alfaumuarama.edu.br/index.php/ras/article/view/34>. Acesso em: 01 set. 2023.

TRINDADE, Sara Dias; CARVALHO, Joaquim Ramos de. HISTÓRIA, TECNOLOGIAS DIGITAIS E MOBILE LEARNING: ENSINAR HISTÓRIA NA ERA DIGITAL. **Imprensa da Universidade de Coimbra/Coimbra University Press**, p.216, 2019. ISBN: 9892617045, 9789892617046, DOI: <https://88doi.org/10.14195/978-989-26-1705-3>.

## ANEXOS

## ANEXO A - TABELA ORIGINAL USADA POR GERALDO E TAKEDA (2019)

Perguntas por Tipos de Ataque	Sim	Não	Não sei informar
<b>Falhas Humanas</b>			
1 - A senha que você utiliza no seu local de trabalho para acessar as informações da empresa, você compartilha com outros funcionários?			
2 - Suas senhas pessoais são iguais às que você utiliza no trabalho?			
3 - Você costuma passar qualquer tipo de informações do seu local de trabalho para outras pessoas?			
4 - Você não utiliza as mesmas senhas para todas as suas contas?			
<b>Contato Telefônico</b>			
5 - Você costuma passar dados pessoais por telefone?			
6 - Geralmente esses números pedem informações pessoais ou alguma informação do seu local de trabalho?			
7 - Você costuma receber ligações de números que você não conhece?			
<b>Internet e Redes Sociais</b>			
8 - Você costuma postar fotos com seus colegas de trabalho nas redes sociais?			
9 - Você geralmente responde pessoas que te chamam no bate-papo para conversar, mesmo não conhecendo elas?			
10 - Nos perfis de suas redes sociais, você costuma colocar qual empresa você trabalha e qual o cargo que exerce?			
11 - No seu local de trabalho, você tem acesso as redes sociais (Facebook, Instagram, Twitter)?			
12 - É possível achar informações sobre sua empresa na Internet?			
<b>Phishing</b>			
13 - Geralmente, os e-mails que você recebe, você assinou eles para receber?			
14 - Alguma vez você já baixou algum arquivo de um e-mail que você recebeu sem perceber?			
15 - Você já recebeu algum e-mail pedindo para você passar dados pessoais, sendo que você não sabia qual a origem desse e-mail?			
16 - Você costuma receber e-mails de instituições financeiras e			

lojas?			
<b>Abordagem Pessoal</b>			
17 - Você costuma frequentar algum barzinho, academia ou qualquer outra coisa depois do trabalho?			
18 - Você gosta de conversar sobre o seu trabalho com seus amigos ou até mesmo pessoas que você não conhece?			
19 - Você é uma pessoa fácil de fazer amizade?			

**Fonte:** Geraldo e Takeda, 2019.