DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Cyber Awareness em ambientes Wi-Fi: um estudo utilizando portais cativos baseados em microcontroladores

Hyago Santana Mariano

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Cyber Awareness em ambientes Wi-Fi: um estudo utilizando portais cativos baseados em microcontroladores

Hyago Santana Mariano

Orientador: Prof. Dr. Daniel Chaves Café, FT/UnB

PUBLICAÇÃO: PPEE.MP.081

BRASÍLIA-DF, FEVEREIRO - 2025

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Cyber Awareness em ambientes Wi-Fi: um estudo utilizando portais cativos baseados em microcontroladores

Hyago Santana Mariano

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. Daniel Cahves Café, FT/UnB _____
Orientador

Prof. Dr. Aldo Henrique Dias Mendes, CNI _____
Examinador Externo

Prof. Dr. Edna Dias Canedo, UnB _____
Examinador interno

Prof. Dr. Laerte Peotta de Melo, UnB _____
Suplente

FICHA CATALOGRÁFICA

SANTANA MARIANO, HYAGO
Cyber Awareness em ambientes Wi-Fi:um estudo utilizando portais cativosbaseados em microcontroladores [Distrito Federal] 2025.
xvi, 60 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2025).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Conscientização cibernética	2. Segurança Wi-Fi
3. Portal Cativo	4. Microcontrolador
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

SANTANA MARIANO, H. (2025). *Cyber Awareness em ambientes Wi-Fi:um estudo utilizando portais cativosbaseados em microcontroladores*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 60 p.

CESSÃO DE DIREITOS

Hyago Santana Mariano
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho à minha avó, cuja sabedoria e carinho sempre foram fontes de inspiração e força. Seu exemplo de vida e sua dedicação à família são marcos que guiam minha jornada, e a ela sou eternamente grato por todo o amor e apoio.

Aos meus pais, que sempre me incentivaram a buscar o conhecimento e a enfrentar os desafios com determinação e coragem. Agradeço profundamente pelo apoio incondicional em todos os momentos da minha trajetória.

À minha família, que é meu alicerce e maior fonte de motivação. Cada um contribui para que eu siga sempre em frente.

E, por fim, aos meus amigos, que compartilharam comigo o aprendizado, as dificuldades e as conquistas. Com eles, aprendi a valorizar a colaboração, o espírito de equipe e a força coletiva. Proletarier aller Länder, vereinigt euch!

AGRADECIMENTOS

A Deus, toda a honra, toda a glória e todo o louvor.

À minha família, meu mais sincero agradecimento pelo apoio incondicional e por sempre estarem ao meu lado. A todos vocês, que com seu amor, força e dedicação, tornaram possível essa trajetória. Agradeço aos meus pais, que sempre me incentivaram a seguir meus sonhos e a nunca desistir, com seu exemplo de trabalho árduo e perseverança. À minha avó, que com sua sabedoria e carinho, sempre foi uma fonte de inspiração. Sou eternamente grato por tudo o que fizeram por mim.

Aos meus amigos, agradeço pelas horas de Counter Strike, onde, entre "headshots", "clutches"e "rushes", nossa amizade foi fortalecida. Cada round, cada vitória apertada e até as partidas com "eco"me ensinaram não só sobre a importância do trabalho em equipe, mas que ninguém vence sem paciência.

Agradeço imensamente ao meu orientador, Daniel Chaves Café, pela orientação, paciência e apoio ao longo de toda a pesquisa. Sua expertise e dedicação foram fundamentais para a realização deste trabalho.

Agradeço também ao Banco do Brasil, empresa onde descobri possibilidades para expandir meus horizontes. O apoio e a visão oferecidos pelo Banco do Brasil foram fundamentais para meu crescimento profissional e acadêmico, permitindo que eu desse esse importante passo na minha carreira.

A todos os alunos que responderam à pesquisa, meu muito obrigado. A contribuição de cada um de vocês foi essencial para o sucesso deste trabalho. Sem a participação ativa e sincera de todos, este estudo não teria a mesma relevância.

Por fim, agradeço a todos que, direta ou indiretamente, contribuíram para a realização deste estudo. Que as ideias aqui discutidas ajudem a expandir a conscientização sobre segurança cibernética, principalmente no uso de redes públicas de Wi-Fi.

RESUMO

Este artigo apresenta a implementação de um portal cativo em um microcontrolador para avaliar e melhorar a maturidade cibernética dos usuários em redes Wi-Fi públicas. Com o crescente uso dessas redes em locais públicos, muitos usuários ficam vulneráveis a riscos cibernéticos, como roubo de dados e ataques. A metodologia envolveu a criação de uma rede simulada com um ESP32, onde os usuários eram direcionados para um portal educacional sobre segurança cibernética ao fazerem login. A coleta de dados foi feita por meio de um questionário com 14 questões, utilizando uma escala Likert para medir as percepções e comportamentos dos usuários.Os resultados mostraram que, embora 95% dos participantes percebam as redes públicas como inseguras, poucos adotam práticas de proteção, como o uso de VPNs e verificação de certificados de segurança. O estudo destaca a importância de campanhas educativas contínuas para melhorar a conscientização e promover comportamentos mais seguros. A metodologia proposta oferece uma ferramenta eficaz para medir a maturidade cibernética e educar usuários sobre riscos e medidas de proteção.

ABSTRACT

This article presents the implementation of a captive portal on a microcontroller to assess and improve users' cybersecurity maturity on public Wi-Fi networks. With the growing use of these networks in public places, many users become vulnerable to cyber risks, such as data theft and attacks. The methodology involved creating a simulated network using an ESP32, where users were directed to an educational security portal upon logging in. Data was collected through a 14-question survey, using a Likert scale to measure users' perceptions and behaviors. The results showed that, although 95% of participants perceive public networks as insecure, few adopt protective practices such as using VPNs and checking security certificates. The study highlights the importance of ongoing educational campaigns to raise awareness and promote safer behaviors. The proposed methodology provides an effective tool for measuring cybersecurity maturity and educating users about risks and protective measures.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

As redes Wi-Fi públicas desempenham um papel cada vez mais relevante no dia a dia das pessoas, possibilitando acesso à internet em diversos locais, como cafés, praças, aeroportos e ônibus(Choi 2022). Essa conectividade onipresente é um marco na democratização digital, permitindo que indivíduos realizem atividades pessoais e profissionais de maneira conveniente e acessível(Golwala 2024). A capacidade de acessar informações, realizar transações financeiras, estudar e se conectar com pessoas ao redor do mundo tornou-se um dos pilares da vida moderna(George 2024). No entanto, por trás dessa praticidade e conveniência, existe uma série de riscos relacionados à segurança da informação, que frequentemente passam despercebidos pelos usuários dessas redes (Lotfy et al. 2021).

A ausência de protocolos robustos de segurança em muitas redes Wi-Fi públicas cria um ambiente propício para cibercriminosos explorarem vulnerabilidades. Tais vulnerabilidades podem ser exploradas de diversas formas, incluindo a interceptação de dados transmitidos entre o usuário e a rede ou até mesmo a criação de redes falsas que imitam redes legítimas (Hussain et al. 2024). Ataques como o Man-in-the-Middle (MITM) são exemplos de ameaças que podem comprometer dados sensíveis, como informações bancárias, credenciais de acesso e comunicações pessoais (Anand et al. 2018). Além disso, práticas maliciosas podem incluir a instalação de malwares nos dispositivos conectados, expondo os usuários a riscos ainda maiores de perda de dados e comprometimento de suas informações confidenciais (Le et al. 2022).

Apesar da gravidade desses riscos, a conscientização sobre eles é limitada. Muitos usuários, especialmente aqueles menos familiarizados com práticas de cibersegurança, adotam comportamentos negligentes, como a conexão a redes desconhecidas sem verificar sua legitimidade ou a utilização de dispositivos sem qualquer tipo de proteção, como antivírus ou firewalls. Essa desconexão entre a facilidade de acesso às redes Wi-Fi públicas e a falta de precauções adequadas reflete lacunas significativas no conhecimento dos usuários sobre os perigos inerentes a essas conexões. Essa realidade reforça a necessidade urgente de soluções educacionais que não apenas alertem os usuários sobre os perigos, mas também promovam boas práticas de segurança e a adoção de comportamentos mais conscientes (Hossain et al. 2019).

Com o objetivo de abordar essa problemática, este estudo propõe o desenvolvimento de um portal cativo educativo, implementado por meio de um microcontrolador ESP32, que simula uma rede Wi-Fi pública falsa. Essa solução tem como foco avaliar a maturidade em cibersegurança dos usuários e promover a conscientização por meio de uma experiência educativa. A escolha do microcontrolador ESP32 é fundamentada em sua acessibilidade, versatilidade e custo reduzido, o que o torna ideal para experimentos que visem reproduzir cenários reais de uso. O portal cativo proposto não apenas simula um ambiente de rede pública, mas também oferece aos usuários informações claras e objetivas sobre os riscos a que estão expostos e as melhores práticas para evitá-los.

Além de identificar lacunas de conhecimento e comportamentos de risco, este estudo visa estabelecer uma metodologia replicável para avaliar a segurança em redes públicas e oferecer recomendações práticas para mitigar vulnerabilidades. A replicabilidade dessa metodologia é um dos aspectos mais relevantes do estudo, pois permite que outras instituições, organizações e pesquisadores utilizem os resultados e ferra-

mentas desenvolvidos como base para iniciativas semelhantes. Assim, o impacto deste trabalho transcende o escopo acadêmico, oferecendo benefícios práticos e imediatos para a sociedade ao melhorar a conscientização sobre segurança da informação e a proteção de dados em ambientes digitais cada vez mais presentes no cotidiano das pessoas.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

A expansão acelerada das redes Wi-Fi públicas transformou profundamente a forma como as pessoas acessam a internet, criando uma infraestrutura de conectividade que está presente em quase todos os aspectos da vida moderna. Essa revolução digital democratizou o acesso à informação, permitindo a inclusão digital de milhões de pessoas ao redor do mundo, promovendo o desenvolvimento social, econômico e cultural.(Medeiros 2021) Redes Wi-Fi públicas são utilizadas diariamente por pessoas para atividades como navegação em redes sociais, realização de trabalhos remotos, envio de mensagens, acesso a serviços bancários e consumo de conteúdos audiovisuais. (Kapicak et al. 2024)

No entanto, essa conveniência vem acompanhada de desafios críticos relacionados à segurança da informação. Muitos usuários desconhecem ou subestimam os riscos associados ao uso dessas redes, que incluem a possibilidade de interceptação de dados, disseminação de malwares e roubo de informações pessoais e profissionais. A ausência de medidas de segurança robustas em muitas redes públicas amplia a vulnerabilidade a ataques cibernéticos. Um exemplo comum é o ataque Man-in-the-Middle (MITM) (Kampourakis et al. 2022), em que invasores interceptam e manipulam as comunicações entre dispositivos conectados. Além disso, redes Wi-Fi falsas (Singh et al. 2022), configuradas por cibercriminosos para enganar usuários, também representam uma ameaça crescente(Australian Federal Police 2023).

Esses riscos são agravados pela falta de conscientização e conhecimento técnico dos usuários, que frequentemente se conectam a redes públicas sem verificar sua legitimidade ou tomar precauções básicas, como o uso de VPNs ou softwares de segurança. Isso reflete uma lacuna significativa na educação sobre cibersegurança, que precisa ser abordada por meio de soluções práticas e acessíveis que promovam comportamentos mais seguros e informados. Este estudo se justifica pela necessidade de enfrentar esse cenário, desenvolvendo ferramentas que possam conscientizar os usuários e mitigar os riscos associados ao uso de redes públicas.

A proliferação das redes Wi-Fi públicas tem facilitado o acesso à informação e promovido a inclusão digital. Entretanto, o fator humano destaca-se como o elo mais vulnerável na segurança da informação, devido à falta de conscientização dos usuários sobre os riscos associados ao uso dessas redes, como a interceptação de dados e a disseminação de malwares. Além disso, tecnologias como portais cativos, embora projetadas para gerenciar o acesso, podem apresentar vulnerabilidades exploráveis por agentes mal-intencionados. Diante desse cenário, este estudo busca desenvolver estratégias educativas e ferramentas que elevem a conscientização dos usuários, visando mitigar os riscos associados à utilização de redes Wi-Fi públicas.

1.2 PROBLEMA DE PESQUISA

A crescente dependência de redes Wi-Fi públicas para atividades pessoais e profissionais reflete o papel central que essas redes desempenham no cotidiano moderno. No entanto, essa mesma popularidade as torna alvos atrativos para cibercriminosos, que exploram vulnerabilidades técnicas e comportamentais para conduzir ataques cibernéticos. Estudos apontam que a falta de conscientização dos usuários e a ausência de medidas de segurança robustas em redes públicas são os principais fatores que contribuem para incidentes de segurança (Ali et al. 2019).

Ataques como Man-in-the-Middle (MITM), phishing e a criação de redes falsas (honeypots) são algumas das ameaças mais comuns e eficazes exploradas por cibercriminosos. Esses ataques não apenas comprometem dados sensíveis, como informações bancárias e credenciais de login, mas também impactam a privacidade dos usuários e a integridade das comunicações. Pequenos negócios e indivíduos, em particular, enfrentam desafios ainda maiores devido à falta de recursos técnicos e financeiros para mitigar esses riscos.

Além disso, o comportamento dos usuários, muitas vezes motivado pela conveniência, contribui significativamente para o aumento das vulnerabilidades. A conexão a redes públicas sem a devida verificação, o compartilhamento de informações sensíveis e a ausência de práticas básicas de cibersegurança, como o uso de VPNs, são comportamentos recorrentes observados em estudos.

Outro ponto de preocupação é a dificuldade de educar os usuários sobre práticas seguras em um ambiente de rápida evolução tecnológica e aumento exponencial das ameaças. Embora existam esforços para promover a conscientização, como campanhas e treinamentos, a eficácia dessas iniciativas é limitada devido à falta de interatividade e personalização nas abordagens existentes.

Diante desse cenário, surgem os seguintes problemas de pesquisa que orientam este estudo:

Problema de Pesquisa 1: Como um portal cativo educativo, implementado com tecnologia acessível como o microcontrolador ESP32, pode aumentar a conscientização dos usuários sobre os riscos de segurança associados ao uso de redes Wi-Fi públicas?

Problema de Pesquisa 2: De que maneira um portal cativo educativo pode medir e avaliar a maturidade em cibersegurança dos usuários de redes Wi-Fi públicas, identificando lacunas de conhecimento e comportamentos de risco?

Para estruturar a análise e validação das hipóteses levantadas, este trabalho se propõe a explorar os seguintes pontos:

Hipótese 1: Usuários que interagem com um portal cativo educativo têm maior probabilidade de adotar práticas de segurança mais robustas ao utilizar redes Wi-Fi públicas.

Hipótese 2: A implementação de um portal cativo educativo pode fornecer dados quantitativos e qualitativos sobre os comportamentos dos usuários e seu nível de conscientização em cibersegurança.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Avaliar o comportamento e a maturidade em cibersegurança dos usuários de redes Wi-Fi públicas, promovendo a conscientização sobre riscos cibernéticos por meio de uma solução educacional replicável utilizando um portal cativo desenvolvido com microcontroladores.

1.3.2 Objetivos Específicos

- Desenvolver e implementar um portal cativo educativo que simule uma rede Wi-Fi pública falsa.
- Identificar lacunas de conhecimento e comportamentos de risco entre os usuários.
- Avaliar a eficácia do portal cativo em aumentar a conscientização sobre segurança da informação.
- Propor recomendações práticas para indivíduos e organizações sobre o uso seguro de redes públicas.
- Estabelecer uma metodologia replicável para avaliação de maturidade em cibersegurança utilizando tecnologias acessíveis.

1.4 TRABALHOS PUBLICADOS

Durante o desenvolvimento desta pesquisa, foi publicado um artigo científico intitulado "Measuring Public Wi-Fi Security Awareness via Captive Portal Connections Using a Microcontroller", que está diretamente relacionado à segurança cibernética em redes Wi-Fi públicas. Publicado no *9th Workshop on Communication Networks and Power Systems (WCNPS 2024)*, esse artigo apresentou a implementação de um sistema de portal cativo em microcontroladores como ferramenta para medir a maturidade cibernética de usuários ao utilizarem redes Wi-Fi públicas. O trabalho detalha a metodologia utilizada para a simulação de redes públicas, o uso do microcontrolador ESP32 e os resultados obtidos a partir da interação com os usuários em um ambiente controlado. O principal objetivo foi investigar a conscientização dos participantes em relação aos riscos associados a essas redes e propor boas práticas de segurança, promovendo uma maior conscientização sobre a proteção de dados e dispositivos em ambientes de conectividade aberta.

1.5 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está organizada em seis capítulos. No Capítulo 1, são apresentados a introdução, a motivação e justificativa, o problema de pesquisa, os objetivos, a metodologia utilizada e a estrutura do trabalho. O Capítulo 2 revisa a literatura sobre redes Wi-Fi públicas, cibersegurança e soluções educacionais. O Capítulo 3 detalha a metodologia de pesquisa, incluindo o desenvolvimento do portal cativo e os procedimentos experimentais. O Capítulo 4 apresenta os resultados obtidos e suas respectivas análises.

No Capítulo 5, as principais conclusões e recomendações são discutidas. Por fim, o Capítulo 6 explora as limitações do estudo e sugere direções para futuras pesquisas.

2 REVISÃO BIBLIOGRÁFICA

2.1 METODOLOGIA DE REVISÃO BIBLIOGRÁFICA

O presente estudo caracteriza-se como exploratório, com abordagem quantitativa, e adota a Teoria do Enfoque Meta Analítico Consolidado (TEMAC), conforme descrito por (Mariano e Rocha 2017). Essa metodologia organiza-se em três etapas principais: a preparação da pesquisa, a apresentação e inter-relação dos dados e, por fim, o detalhamento e construção de um modelo integrador validado por evidências. A TEMAC permite a análise sistemática de resultados provenientes de diferentes bases de dados científicas, assegurando diversidade e confiabilidade dos achados. Além disso, oferece um método estruturado para a seleção da literatura, combinando requisitos como precisão, validade, robustez, funcionalidade e eficiência em termos de tempo e custos (Adriaanse e Rensleigh 2013).

Na primeira etapa, a preparação da pesquisa concentra-se na definição criteriosa dos termos e palavras-chave que garantam uma cobertura abrangente do tema. Essa fase também abrange a escolha das áreas do conhecimento relacionadas e a execução de buscas em bases científicas utilizando strings de busca pré-elaboradas (Mariano e Rocha 2017). Em seguida, a segunda etapa dedica-se à organização e análise dos registros obtidos. Esses registros incluem fatores como os periódicos mais relevantes, a evolução do tema ao longo dos anos, os países e instituições que mais publicaram e a frequência de palavras-chave associadas ao tema (Mariano e Rocha 2017).

A terceira etapa aprofunda a análise dos dados, explorando a coautoria, padrões de citação e as principais linhas de pesquisa. Nessa fase, também são realizadas validações com base em evidências, e um modelo integrador é consolidado por meio da comparação dos resultados obtidos em diferentes fontes (Mariano e Rocha 2017, Adriaanse e Rensleigh 2013). Essa abordagem fornece uma visão ampla e detalhada do tema, contribuindo para a formação de uma base sólida para futuras investigações.

2.1.1 Etapa 1: Preparação da Pesquisa

Os termos de busca foram definidos para cobrir os objetivos do estudo de forma abrangente e precisa, sendo as buscas limitadas aos últimos cinco anos (2019-2025) para garantir atualidade e relevância. Entre as palavras-chave utilizadas, destacam-se “Security Awareness”, “Wi-Fi Security”, “Wi-Fi Awareness”, “Captive Portal” e “Public Wi-Fi Networks”. As buscas foram realizadas em bases como Web of Science e Scopus, com ajustes nos termos para adequação aos filtros de cada base.

Conforme a figura 2.1, os resultados iniciais das buscas trouxeram 254 publicações para o termo “Security Awareness” na Web of Science, enquanto “Wi-Fi Security” obteve 9 publicações e “Wi-Fi Awareness” apenas 1. Os termos “Captive Portal” e “Public Wi-Fi Networks” resultaram em 5 e 8 publicações, respectivamente. Na base Scopus, “Security Awareness” gerou 3 publicações, enquanto “Wi-Fi Security” e “Wi-Fi Awareness” contabilizaram 5 e 6 publicações, respectivamente. Os termos “Captive Portal” e “Public Wi-Fi Networks” resultaram em 1 e 29 publicações. Após a remoção de duplicatas, foi consolidada

uma amostra de 326 publicações.

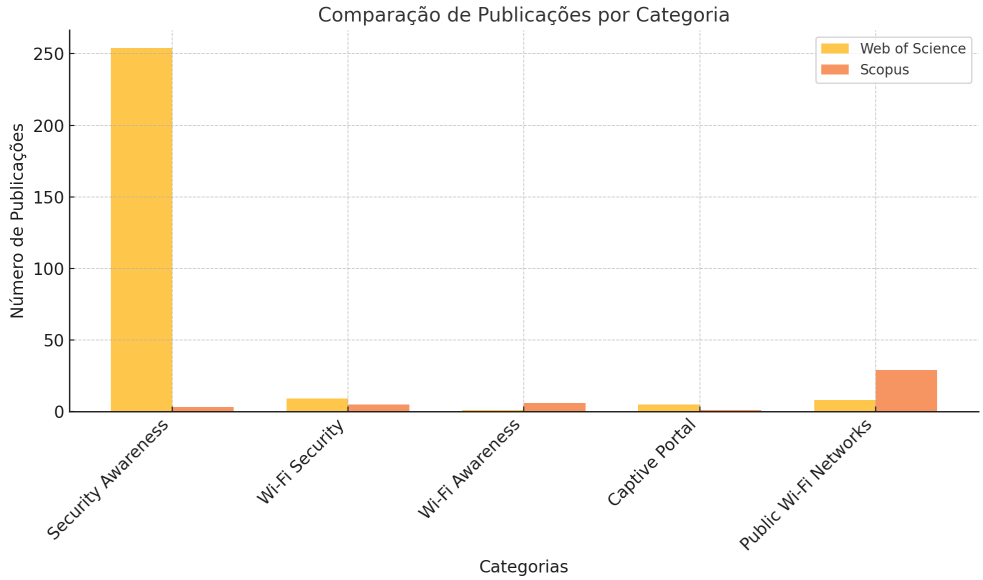

Figura 2.1: Comparação de bases

2.1.2 Etapa 2: Apresentação e Inter-relação dos Dados

A análise temporal das publicações revelou padrões distintos entre as bases de dados. Na Web of Science, o volume de publicações foi crescente até 2023, com 54 publicações em 2021, 75 em 2022, 64 em 2023 e 62 em 2024. Apenas 2 publicações foram identificadas em 2025, indicando possível atraso na indexação. Já na Scopus, o volume foi menor, com apenas uma publicação em 2021, três em 2022, seis em 2023, mas um crescimento significativo em 2024, com 18 publicações, e 10 já registradas em 2025. Esses dados sugerem um aumento no interesse acadêmico recente pelo tema conforme a figura 2.2.

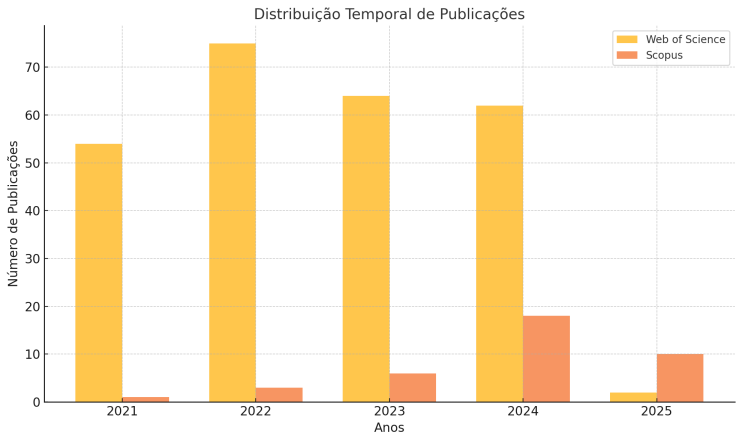

Figura 2.2: Comparação temporal de bases

Geograficamente, conforme Figura 2.3, os países que mais contribuíram para as publicações foram China e Estados Unidos, destacando-se tanto pela quantidade quanto pela diversidade temática. O Brasil, embora com menor volume de publicações, apresentou artigos relevantes, explorando temas como enge-

nharia social e impactos ambientais de redes Wi-Fi. Exemplos notáveis incluem estudos sobre estratégias de conscientização contra ataques de engenharia social e medições de radiação não ionizante em ambientes residenciais. Outros países, como Reino Unido, Índia e Alemanha, também contribuíram com volumes significativos de publicações, mas com foco mais distribuído em regulamentações e infraestrutura.

Quanto aos principais temas abordados, os artigos analisados enfatizaram segurança de redes, conscientização e uso de Wi-Fi público, enquanto termos como “Captive Portal” e “Wi-Fi Awareness” surgiram com menor frequência, mas foram destacados como áreas promissoras para estudos futuros.

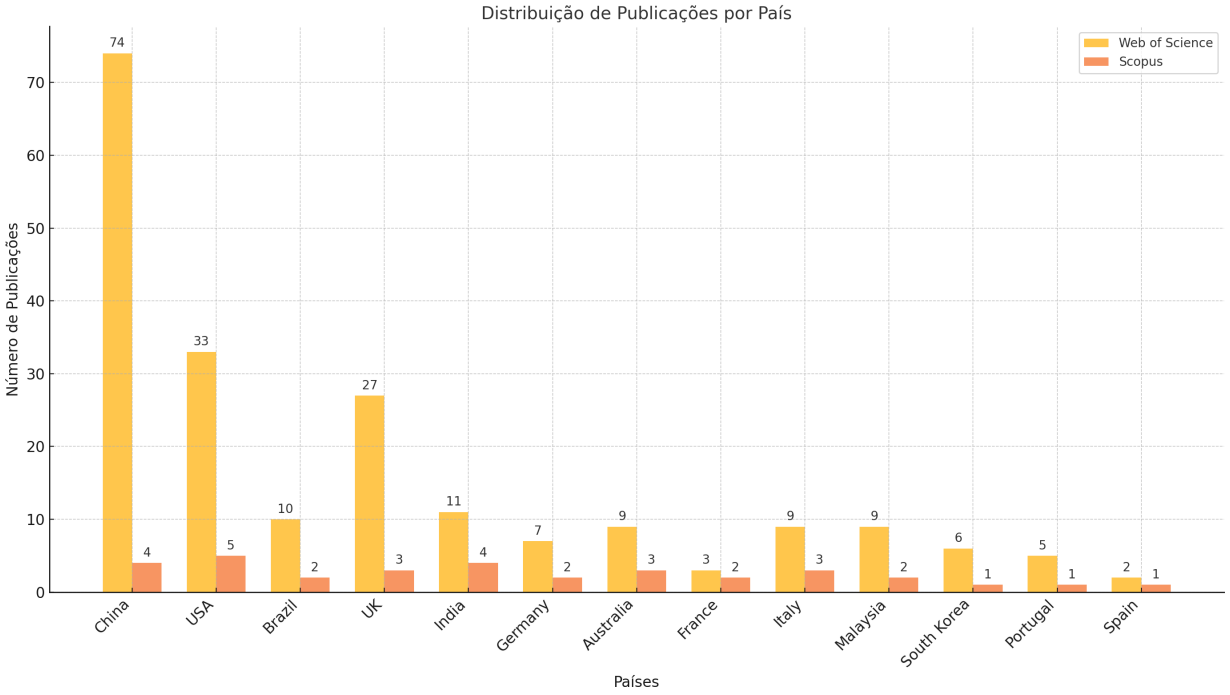

Figura 2.3: Comparação temporal de bases

2.1.3 Etapa 3: Detalhamento e Validação

Nesta etapa, foram realizadas análises detalhadas para identificar lacunas e validar as tendências observadas. O Brasil, apesar de contribuir com um volume reduzido, apresentou temas de alta relevância, como conscientização em engenharia social e impactos ambientais de redes Wi-Fi. O aumento no volume de publicações recentes, especialmente em 2024, indica um crescimento no interesse acadêmico pelo tema, especialmente quando associado a colaborações internacionais.

China e Estados Unidos continuam na vanguarda, tanto em volume quanto em diversidade temática, enquanto a América Latina surge como uma região com grande potencial para investimentos em pesquisa. Na Europa, a distribuição consistente de publicações reforça o interesse em regulamentações e infraestrutura. Esses dados validam a proposta original do estudo, destacando a necessidade de educação e de maior integração entre governos e instituições acadêmicas para preencher lacunas regionais.

O estudo apresentou um panorama abrangente da pesquisa sobre segurança em redes Wi-Fi públicas. Identificaram-se padrões globais e lacunas regionais, com destaque para a crescente relevância do tema nos

últimos anos. Embora o Brasil ainda tenha baixa representatividade em quantidade, a relevância temática de seus estudos é notável. A análise aponta para a necessidade de maior investimento em educação e colaborações acadêmicas internacionais, oferecendo direções concretas para futuras pesquisas. Além disso, o aumento no número de publicações em anos recentes reflete a crescente importância do tema no cenário global.

2.2 FERRAMENTAS E CONFIGURAÇÃO

A tecnologia de microcontroladores tem desempenhado um papel crucial em aplicações que demandam processamento eficiente, conectividade abrangente e custos acessíveis. No contexto deste estudo, o ESP32 foi escolhido devido à sua robustez, versatilidade e popularidade em projetos de Internet das Coisas (IoT). Esse microcontrolador é equipado com um processador dual-core Tensilica LX6, operando em frequências de até 240 MHz, o que garante alta capacidade de processamento para tarefas simultâneas. Além disso, ele oferece suporte nativo a Wi-Fi 802.11 b/g/n e Bluetooth 4.2, tornando-o uma escolha ideal para soluções conectadas que exigem flexibilidade e desempenho.

A escolha do microcontrolador ESP32 em detrimento de dispositivos como smartphones ou notebooks se deve à necessidade de um ambiente de teste controlado, autônomo e otimizado para a simulação da rede. O ESP32 permite a implementação direta do ponto de acesso Wi-Fi e do portal cativo sem depender de sistemas operacionais proprietários ou de aplicações de terceiros, garantindo maior flexibilidade, estabilidade e segurança na coleta de dados. Além disso, seu baixo consumo energético, custo reduzido e facilidade de programação viabilizam a replicação do experimento em diferentes cenários, tornando-o uma solução mais eficiente para a avaliação da conscientização em segurança cibernética.

A configuração do ESP32 neste projeto foi cuidadosamente projetada para maximizar o desempenho e a eficiência do dispositivo em simulações de redes Wi-Fi públicas. Uma antena externa de alta eficiência foi integrada ao dispositivo, aumentando significativamente o alcance do sinal e proporcionando estabilidade em ambientes de alta densidade de usuários. O armazenamento via cartão SD, acessível por meio do protocolo SPI, foi utilizado para hospedar os arquivos essenciais do portal cativo, como códigos HTML, CSS e JavaScript.

Um aspecto fundamental da configuração foi a implementação de alimentação portátil com uma bateria de ítio-polímero conectada via USB. Isso garantiu a mobilidade do dispositivo, permitindo sua utilização em vários cenários de teste sem depender de fontes de energia fixas. Essa flexibilidade é essencial para experimentos em campo, especialmente quando se busca replicar as condições reais de uso de redes Wi-Fi públicas.

O portal cativo foi configurado com foco em simular cenários realistas de redes públicas. Para isso, o ESP32 foi programado utilizando MicroPython, uma linguagem leve e altamente compatível com microcontroladores, que facilitou a criação de scripts de redirecionamento e controle de tráfego. A página inicial do portal foi projetada com interface responsiva, incorporando frameworks como Bootstrap e bibliotecas como jQuery para garantir acessibilidade e interatividade em dispositivos de diferentes tamanhos de tela.

A experiência do usuário no portal incluía uma série de elementos educacionais que destacavam riscos

comuns de segurança cibernética, como ataques de phishing, interceptação de tráfego (Man-in-the-Middle) e roubo de dados. Esses conteúdos foram apresentados de maneira didática, incentivando os participantes a refletirem sobre suas práticas de navegação.

Embora o sistema não armazenasse dados diretamente no ESP32, ele foi configurado para redirecionar os participantes a um formulário externo hospedado em uma plataforma de coleta de dados online. Esse formulário era usado para registrar respostas a questionários que avaliavam os níveis de conhecimento e percepções dos usuários sobre segurança cibernética. A escolha de um formulário externo garantiu a simplicidade do sistema no ESP32, permitindo que os recursos do microcontrolador fossem otimizados para outras tarefas.

Adicionalmente, o ESP32 foi configurado para emitir logs em tempo real por meio de conexão serial. Esses logs incluíam informações como o número de dispositivos conectados e informada no LED Shield. Essas informações foram valiosas para entender o comportamento geral dos participantes e ajustar o ambiente de teste para futuras sessões.

Um dos grandes diferenciais desta abordagem foi a combinação de elementos tecnológicos avançados com práticas educacionais interativas. Os usuários não apenas tiveram a oportunidade de vivenciar situações simuladas de risco, mas também receberam informações detalhadas sobre como proteger suas conexões, incluindo a configuração de VPNs, a verificação de certificados SSL e a adoção de senhas fortes. Este formato não apenas promoveu a conscientização, mas também incentivou a transformação de percepções em ações concretas, reforçando uma cultura de segurança entre os participantes.

2.3 REVISÃO CIENTÍFICA DA LITERATURA

A segurança em redes Wi-Fi públicas tem se tornado uma questão central no campo da cibersegurança, dada a dependência crescente de dispositivos conectados e a frequente utilização de hotspots em locais como aeroportos, cafeterias e espaços públicos. Embora essas redes ofereçam conveniência, elas introduzem vulnerabilidades que podem ser exploradas por atacantes para comprometer informações pessoais e empresariais. A literatura acadêmica fornece uma base robusta para compreender essas ameaças, as limitações das soluções existentes e as direções futuras para melhorar a segurança.

Os protocolos de segurança Wi-Fi, como o WPA e WPA2, foram introduzidos como uma resposta às vulnerabilidades do WEP, mas avanços nas técnicas de ataque rapidamente expuseram limitações significativas. O handshake de quatro vias, utilizado no WPA2, tem sido explorado em ataques de força bruta e interceptação (Zulkipli e Khusairi, 2024). Para mitigar esses riscos, o WPA3 foi desenvolvido com recursos como criptografia individualizada e proteção contra ataques offline, oferecendo maior robustez (Kwon e Choi, 2021). No entanto, estudos recentes apontam que vulnerabilidades de implementação e ataques de canal lateral continuam a comprometer a segurança dessas redes (“Bl0ck: Paralyzing 802.11 Connections”, 2023).

A exploração de vulnerabilidades técnicas não é o único problema enfrentado por redes Wi-Fi públicas. Ataques como Man-in-the-Middle (MITM), spoofing e Evil Twin continuam a ser altamente prevalentes. Ahadi et al. (2020) revisaram soluções para detecção de ataques Evil Twin, destacando a eficiência de

sistemas de detecção de intrusão (IDS) baseados em aprendizado de máquina. Em casos como o de um indivíduo na Austrália que utilizava redes Wi-Fi falsas para roubar dados de usuários desavisados (“Australian Man Charged for Fake Wi-Fi”, 2024), a facilidade com que SSIDs maliciosos podem ser configurados ressalta a necessidade de medidas de autenticação mais robustas.

Pesquisas comportamentais também são cruciais para compreender as vulnerabilidades associadas ao uso de redes Wi-Fi públicas. Maimon et al. (2022) destacaram que muitos usuários não adotam medidas básicas de proteção, como o uso de VPNs, mesmo estando cientes dos riscos. Essa lacuna comportamental é atribuída à conveniência percebida e à falta de conhecimento técnico. Em contraste, estudos como os de Turland et al. (2015) mostraram que intervenções simples, como o uso de "nudges"comportamentais para indicar redes seguras, podem influenciar positivamente a tomada de decisões dos usuários.

A integração de dispositivos IoT em redes públicas introduz novos desafios. Esses dispositivos ampliam a superfície de ataque, permitindo que atacantes explorem vulnerabilidades para acessar redes ou dados sensíveis. Sasi et al. (2024) destacaram que ataques direcionados a dispositivos IoT podem ser mitigados por soluções baseadas em blockchain e autenticação multifator. Essas tecnologias emergentes prometem maior resiliência contra ameaças, mas sua implementação em larga escala enfrenta desafios de padronização e custo.

Casos reais complementam as descobertas acadêmicas, demonstrando a gravidade das ameaças. Incidentes como o uso de redes Wi-Fi maliciosas em aeroportos australianos ilustram como dispositivos de baixo custo podem ser utilizados para comprometer informações pessoais e empresariais (The Australian 2023). Esse cenário reforça a necessidade de educar os usuários sobre comportamentos seguros e implementar soluções tecnológicas mais eficazes.

A educação dos usuários desempenha um papel crucial na redução de riscos associados ao uso de redes públicas. Abdulkader (2023) enfatizou que conveniência e economia de dados são fatores determinantes para o comportamento inseguro. Nesse contexto, programas de conscientização que combinem teoria com experiências práticas têm se mostrado altamente eficazes. Turland et al. (2015) demonstraram que intervenções educativas baseadas em simulações podem aumentar significativamente a compreensão e a adoção de medidas de proteção.

Apesar dos avanços, desafios persistem. A implementação de soluções escaláveis para proteger redes públicas enfrenta barreiras, incluindo custos elevados e falta de padronização global. Tecnologias como blockchain e inteligência artificial apresentam soluções promissoras, mas sua adoção generalizada requer colaboração entre governos, empresas e pesquisadores para garantir que as soluções sejam acessíveis e eficazes.

Conclui-se que a segurança em redes Wi-Fi públicas exige uma abordagem multidisciplinar que combine avanços tecnológicos, educação cibernética e regulações padronizadas. A literatura revisada destaca a importância de soluções integradas para mitigar os riscos e promover um ambiente digital mais seguro para todos os usuários.

2.4 TRABALHOS CORRELATOS

A segurança em redes Wi-Fi públicas tem sido amplamente estudada, dado o crescente uso dessas redes em locais como cafés, aeroportos e shoppings. Esses ambientes são frequentemente alvo de ataques de engenharia social, onde hackers exploram vulnerabilidades humanas para obter informações confidenciais. Segundo Guarezi (2019), a falta de conscientização é o elo mais fraco na segurança da informação, e a educação é essencial para mitigar riscos associados a esses ataques.(Guarezi 2019)

Ali et al. (2019) destacam os riscos de privacidade em portais cativos, mostrando que muitos usuários fornecem dados pessoais sem verificar a segurança da rede. Essa vulnerabilidade é exacerbada pela falta de informações claras sobre como proteger dados em ambientes de redes públicas. Os autores também enfatizam que a ausência de autenticação robusta nesses portais facilita ataques de phishing e roubo de credenciais, reforçando a necessidade de soluções educacionais e tecnológicas para mitigar tais riscos.(Ali et al. 2019)

Estudos de Vaccari et al. (2021) reforçam a necessidade de medidas preventivas, como o uso de certificados digitais, criptografia de ponta a ponta e autenticação multifator, para evitar que dispositivos IoT comprometidos propaguem ataques em redes públicas. Esses estudos destacam como a crescente integração de dispositivos IoT em redes Wi-Fi aumenta exponencialmente os vetores de ataque, tornando a educação dos usuários e a implementação de medidas de segurança ainda mais críticas.(Vaccari et al. 2021)

Outro aspecto relevante é abordado por Hammad e Ati (2020), que identificaram vulnerabilidades em redes Wi-Fi nos Emirados Árabes Unidos. Esses autores sugerem soluções como VPNs, protocolos de segurança como WPA3 e criptografia robusta para proteger dados contra interceptação maliciosa. Além disso, os autores ressaltam a importância de políticas de conscientização e treinamentos regulares para os usuários como elementos-chave para aumentar a resiliência contra ameaças cibernéticas. (Hammad e Ati 2020)

No contexto de educação e conscientização, Sombatruang et al. (2018) apontam que, embora muitos usuários reconheçam os riscos associados a redes públicas, poucos adotam medidas preventivas devido à conveniência dessas redes. Eles sugerem que campanhas educacionais mais dinâmicas, utilizando ferramentas interativas e simulações de cenários de ataque, podem ajudar a superar essa barreira, incentivando práticas mais seguras. (Sombatruang et al. 2018)

A implementação de soluções tecnológicas é discutida por Bauer et al. (2008), que propuseram um sistema de autenticação baseado em certificados SSL para mitigar ataques Evil Twin. Essa solução mostrou-se eficaz em cenários experimentais, alcançando uma taxa de detecção de 100%. No entanto, os autores também destacam que a eficiência dessas soluções depende de sua implementação em conjunto com uma educação adequada dos usuários. (Bauer, Gonzales e McCoy 2008)

Sun et al. (2020) expandem essa discussão ao explorar soluções que combinam aprendizado de máquina e blockchain para reforçar a segurança em redes Wi-Fi públicas. Esses autores propõem um sistema de autenticação distribuída que utiliza contratos inteligentes para verificar a identidade de dispositivos conectados, reduzindo riscos de ataques de impersonação e aumentando a confiabilidade das redes. (Sun et al. 2024)

Lotfy et al. (2021) examinaram a consciência dos usuários sobre vazamentos de privacidade em redes

Wi-Fi públicas, destacando que 85% dos usuários acessaram categorias de links indesejáveis, o que pode comprometer suas informações. Além disso, 90% dos usuários acessaram redes sociais, e 60% utilizaram mecanismos de busca. O estudo também sugeriu que decisores em universidades devem considerar o fechamento de sites específicos para proteger os recursos institucionais e minimizar riscos à privacidade dos usuários. (Lotfy et al. 2021)

Maimon et al. (2022) exploraram a importância da consciência situacional em comportamentos protetivos de usuários de Wi-Fi público. O estudo revelou que indivíduos mais atentos às condições do ambiente têm menos probabilidade de acessar contas pessoais em redes públicas e mais propensão a adotar medidas de segurança física, como cobrir a tela de seus dispositivos. O estudo também apontou que usuários com maior proficiência em informática são menos propensos a utilizar redes Wi-Fi públicas. (Maimon et al. 2022)

Em uma segunda fase, os autores utilizaram redes Wi-Fi honeypot para investigar o comportamento dos usuários em redes não seguras. Eles descobriram que as pessoas são mais propensas a acessar essas redes em locais com poucos funcionários presentes e onde não há Wi-Fi público oficial. Além disso, o número de funcionários no local foi associado a um aumento em comportamentos de segurança física, como ocultar a tela. Esses achados destacam a necessidade de campanhas educacionais que enfatizem a segurança tanto digital quanto física para minimizar a vitimização online. (Maimon et al. 2022)

Ahadi et al. (2020) fornecem uma visão abrangente sobre a detecção de ataques Evil Twin em redes Wi-Fi públicas. Esses ataques, que envolvem a falsificação de pontos de acesso legítimos por meio da manipulação do SSID e do endereço MAC, podem levar a graves ameaças, como ataques Man-in-the-Middle e interrupção de serviço. Os autores revisaram técnicas existentes e propuseram novos métodos baseados em aprendizado de máquina e sistemas de detecção de intrusão (IDS) para mitigar esses riscos. Eles também destacaram a importância de usar endereços IP externos e tempos de resposta (RTT) como métricas para identificar pontos de acesso maliciosos, reforçando a necessidade de soluções tecnológicas robustas para proteger usuários em redes Wi-Fi vulneráveis. (Ahadi et al. 2020)

O estudo de Abdulkader (2023) investigou o comportamento de risco associado ao uso de Wi-Fi público. Utilizando entrevistas qualitativas com 14 participantes, foi revelado que fatores como conveniência, economia de dados móveis e limitações de cobertura móvel são os principais motivadores para o uso de redes públicas. Contudo, muitos usuários demonstraram baixa consciência sobre riscos como ataques Man-in-the-Middle e "Evil Twin". O estudo destaca a necessidade de medidas educativas e tecnológicas para aumentar a segurança e reduzir o comportamento de risco nessas redes. (Abdulkader 2023)

Turland et al. (2015) apresentaram uma aplicação protótipo desenvolvida para promover a escolha de redes Wi-Fi seguras em dispositivos Android. Baseada em teoria comportamental e boas práticas de design em HCI, a aplicação utiliza "nudges" como codificação por cores e ordenação de listas para incentivar os usuários a selecionar opções mais seguras. Durante a avaliação, foi constatado que a codificação por cores foi especialmente eficaz em influenciar as escolhas dos usuários, especialmente quando combinada com a ordenação. Essa pesquisa contribui para a literatura ao demonstrar a efetividade de intervenções em cibersegurança que empoderam o usuário a tomar decisões mais informadas sobre segurança. (Turland et al. 2015)

Kwon e Choi (2021) discutem a evolução do Wi-Fi Protected Access (WPA), destacando as melho-

rias introduzidas no WPA3 para corrigir vulnerabilidades em versões anteriores. As melhorias incluem a proteção de tráfego de dados mesmo que a senha seja comprometida e a imunidade a ataques de adivinhação de senhas. Os autores também analisam como os algoritmos de segurança podem ser aprimorados, contribuindo para o fortalecimento da proteção em redes Wi-Fi. (Kwon e Choi 2020)

Zulkipli e Khusairi (2024) conduziram uma análise experimental das vulnerabilidades em redes Wi-Fi públicas, com foco em ataques como ARP spoofing, DNS spoofing e "4-way handshake". Utilizando quatro experimentos de teste, os autores avaliaram a eficácia desses ataques e propuseram técnicas de mitigação. Os resultados contribuem para o desenvolvimento de sistemas de defesa robustos, auxiliando na proteção contra acessos não autorizados e vazamento de dados. (Zulkipli e Khusairi 2024)

Nguu e Musuva (2024) investigaram o impacto de programas de conscientização em cibersegurança no comportamento de segurança em Wi-Fi. Utilizando uma metodologia de pesquisa-ação em uma empresa de FinTech no Quênia, os autores demonstraram que o treinamento em cibersegurança melhora significativamente as intenções comportamentais de segurança, especialmente em relação ao uso de redes Wi-Fi seguras. (Musuva et al. 2024)

Hossain et al. (2019) realizaram um estudo em Dhaka, Bangladesh, utilizando um dispositivo portátil de pentest para avaliar a consciência sobre segurança em redes Wi-Fi. O estudo destacou que muitos pontos de acesso são vulneráveis a ataques "Evil Twin" e propõe recomendações para mitigar essas ameaças, contribuindo para uma maior segurança em redes sem fio na região. (Hossain et al. 2019)

2.5 MEUS TRABALHOS E OS DEMAIS

O presente trabalho distingue-se no campo da segurança em redes Wi-Fi públicas por sua abordagem inovadora, integradora e acessível, utilizando microcontroladores para simulação de ataques e conscientização de riscos em um contexto educacional. Combinando práticas tecnológicas e pedagógicas, este estudo visa preencher lacunas na educação de segurança cibernética, oferecendo uma plataforma replicável e de baixo custo que se alinha aos desafios contemporâneos.

Estudos como os de Maimon et al. (2022) e Nguu e Musuva (2024) destacam a importância da conscientização situacional e de programas de treinamento na modificação de comportamentos de segurança. Este trabalho avança essas discussões ao criar experiências educacionais práticas por meio de um portal cativo implementado no microcontrolador ESP32, permitindo que os usuários interajam com cenários simulados de riscos reais, como ataques Evil Twin e captura de dados. A utilização de situações interativas promove um aprendizado ativo que vai além das abordagens meramente teóricas revisadas em estudos anteriores.

Diferentemente de soluções tecnologicamente complexas, como as propostas por Ahadi et al. (2020) e Zulkipli e Khusairi (2024), que empregam aprendizado de máquina e sistemas de detecção de intrusão, este trabalho utiliza tecnologias acessíveis. A escolha do microcontrolador ESP32 destaca-se pela combinação de custo reduzido, funcionalidade robusta e facilidade de implantação, o que possibilita uma reprodução ampla em contextos educacionais e experimentais. Essa abordagem reduz barreiras financeiras e operacionais, democratizando o acesso a ferramentas de conscientização em segurança cibernética.

O trabalho também avança ao integrar simulações de ataques reais com educação interativa. Enquanto estudos como os de Lotfy et al. (2021) analisaram o comportamento de usuários com base em dados de tráfego coletados passivamente, o presente estudo cria situações realistas por meio de redes honeypot e simulações de ameaças, oferecendo uma experiência mais imersiva e didática. Os dados coletados através de formulários externos complementam a avaliação ao incluir insights qualitativos sobre o nível de conscientização e as medidas adotadas pelos usuários, gerando uma visão abrangente e enriquecida.

Ao contrapor-se a estudos como o de Turland et al. (2015), que utilizam aplicações móveis para promover escolhas seguras, este trabalho adota uma abordagem integrada que combina educação e tecnologia em uma única plataforma. O uso do ESP32 para hospedar um portal cativo interativo demonstra como tecnologias acessíveis podem ser aproveitadas para oferecer experiências educacionais impactantes. Essa integração não apenas educa, mas também avalia a capacidade dos usuários de reconhecer e mitigar ameaças, promovendo mudanças comportamentais duradouras.

A relevância deste trabalho se estende ao campo da Internet das Coisas (IoT), conforme discutido por Sasi et al. (2024). As metodologias implementadas podem ser adaptadas para dispositivos IoT, ampliando o escopo de aplicação em cenários interconectados. O uso de taxonomias de ataques e contramedidas oferecidas neste estudo pode influenciar soluções futuras para fortalecer a segurança no ecossistema IoT, alinhando-se aos desafios emergentes em cibersegurança.

O trabalho também considera os avanços discutidos por Kwon e Choi (2021) sobre o WPA3, utilizando o portal cativo para demonstrar vulnerabilidades em protocolos legados e conscientizar os usuários sobre a importância de atualizações de segurança. Essa abordagem educativa complementa as melhorias tecnológicas ao capacitar os usuários a tomar decisões informadas em relação à proteção de suas redes.

Com base nos resultados apresentados, este trabalho oferece uma contribuição significativa ao unir educação interativa, tecnologia acessível e simulações realistas em um único framework. Ao posicionar-se como uma solução replicável e eficaz, ele atende às demandas crescentes de conscientização cibernética, contribuindo para uma maior resiliência em redes Wi-Fi públicas e estabelecendo uma base sólida para futuras pesquisas e aplicações em contextos educacionais e industriais.

3 METODOLOGIA

3.1 A ARQUITETURA

A arquitetura do sistema foi projetada para implementar um portal cativo em uma rede Wi-Fi pública utilizando o ESP32, permitindo avaliar a maturidade cibernética dos usuários ao interagirem com redes não seguras. O sistema cria um ponto de acesso Wi-Fi aberto, simulando um ambiente realista onde os usuários são automaticamente redirecionados para um portal cativo. Nele, seu comportamento de conexão é analisado, possibilitando a coleta de dados para avaliar sua conscientização sobre segurança digital.

A implementação do sistema foi organizada em três camadas principais. A Camada de Hardware é responsável pelo funcionamento físico do sistema, incluindo o microcontrolador e os dispositivos de armazenamento. A Camada de Rede gerencia a criação do ponto de acesso Wi-Fi, replicando o SSID da rede pública da Universidade de Brasília, além de administrar o portal cativo, que intercepta conexões e direciona os usuários para a página de autenticação. Já a Camada de Software engloba a interface do usuário e o processamento dos dados coletados, permitindo a análise do nível de conscientização em segurança cibernética com base no comportamento dos usuários.

O firmware foi desenvolvido utilizando a Arduino IDE, garantindo compatibilidade com bibliotecas voltadas para comunicação Wi-Fi e manipulação de redes, facilitando a implementação e otimização do sistema.

A Camada de Hardware utiliza o ESP32, um microcontrolador com conectividade Wi-Fi integrada e alto desempenho, que gerencia a criação do ponto de acesso e a execução do portal cativo. Os arquivos do sistema, como HTML, CSS e JavaScript, são armazenados na memória Flash e em um cartão SD, permitindo flexibilidade no armazenamento e facilidade na atualização do portal. A alimentação do sistema é realizada por uma fonte USB, garantindo operação contínua sem necessidade de intervenção manual. Além disso, foi implementada uma antena externa para ampliar o sinal Wi-Fi, aumentando a cobertura da rede e proporcionando maior estabilidade, mesmo em ambientes com múltiplos dispositivos conectados simultaneamente.

A Camada de Rede é responsável pela comunicação sem fio e pela interação dos usuários com o portal cativo. O ESP32 cria uma rede aberta que simula um SSID público comum, replicando redes frequentemente utilizadas em espaços públicos. Um servidor web integrado hospeda o portal cativo e processa as solicitações dos usuários, enquanto um redirecionamento DNS assegura que qualquer tentativa de navegação seja direcionada para a página de login do portal. Além disso, o sistema inclui um mecanismo de captura de informações de conexão, que registra o endereço MAC e o tempo de sessão dos dispositivos conectados, permitindo um monitoramento detalhado da interação dos usuários com a rede.

A Camada de Software é responsável pelo gerenciamento do portal cativo e pela análise das interações dos usuários. O portal foi projetado para simular páginas de login de redes públicas conhecidas, criando um ambiente confiável que incentiva os usuários a interagir como fariam em uma rede real. O sistema coleta dados de acesso, armazenando informações relevantes para a análise sem comprometer a privacidade

dos usuários. Além disso, um gerenciador de sessões monitora e controla os dispositivos conectados, garantindo que a rede funcione conforme o esperado. Para fins estatísticos, um contador de acessos foi implementado para registrar o número total de conexões ao portal cativo, permitindo avaliar a frequência de uso da rede simulada sem armazenar informações sensíveis dos usuários.

3.2 ESTRUTURA DO PROJETO

A organização do projeto segue uma estrutura bem definida para facilitar o gerenciamento dos arquivos e a manutenção do sistema. A Tabela 3.1 apresenta a distribuição dos diretórios e arquivos dentro do projeto, destacando suas respectivas funções.

Diretório / Arquivo	**Descrição**
`Sistema_WiFi_Seguro/`	Raiz do projeto
`|- assets/`	Arquivos estáticos do portal cativo
`|- bin/`	Arquivos compilados
`|- include/`	Arquivos de cabeçalho
`|- lib/`	Bibliotecas adicionais
`|- src/`	Código-fonte principal
`|- logs/`	Registro do número de acessos
`|- scripts/`	Scripts auxiliares (exclusão de dados)
`|- test/`	Scripts de teste
`|- arduino.ini`	Configuração da Arduino IDE

Tabela 3.1: Estrutura de diretórios do projeto

3.3 FLUXO DE EXECUÇÃO

O funcionamento do sistema segue um fluxo lógico bem estruturado, garantindo o correto estabelecimento da rede, a interação dos usuários e o gerenciamento dos acessos. A Tabela 3.2 apresenta as etapas essenciais que compõem esse fluxo.

Etapa	**Descrição**
1	Inicialização do ESP32 e configuração do ponto de acesso Wi-Fi falso.
2	Ativação do servidor web para hospedar o portal cativo.
3	Redirecionamento automático para a página do portal cativo.
4	Registro das interações dos usuários, armazenando apenas o número de acessos.
5	Incremento do contador de acessos.
6	Redirecionamento do usuário para uma página informativa ou de erro.
7	Execução periódica de um script para a exclusão de logs sensíveis.

Tabela 3.2: Fluxo de Execução do Sistema

3.4 GERENCIAMENTO DE DADOS E CONTADOR DE ACESSOS

Para assegurar a privacidade dos usuários ao mesmo tempo em que se registra a atividade no portal cativo, foram implementadas duas funcionalidades essenciais. A primeira é um mecanismo de exclusão periódica de dados sensíveis, que remove automaticamente arquivos de log armazenados no sistema, evitando a retenção indevida de informações e garantindo a proteção da privacidade dos usuários. A segunda é um contador de acessos, que permite monitorar a quantidade total de conexões realizadas ao portal cativo sem armazenar quaisquer dados pessoais ou identificáveis. Essa abordagem possibilita a análise do uso da rede sem comprometer a segurança e a confidencialidade das informações dos usuários, assegurando conformidade com boas práticas de proteção de dados.

3.4.1 Exclusão de Dados Sensíveis

Um script em Python remove periodicamente arquivos de logs armazenados, evitando a retenção de informações sensíveis.

Listing 3.1: Exclusão de dados sensíveis

```python
import os
for arq in os.listdir("./logs/"):
    caminho = os.path.join("./logs/", arq)
    if os.path.isfile(caminho):
        os.remove(caminho)
```

3.4.2 Contador de Acessos

O ESP32 registra o número total de acessos ao portal sem armazenar dados pessoais.

Listing 3.2: Contador de acessos no ESP32

```
#include <Preferences.h>
Preferences preferences;
void setup() {
    Serial.begin(115200);
    preferences.begin("acessos", false);
    int contador = preferences.getInt("contador", 0) + 1;
    preferences.putInt("contador", contador);
    preferences.end();
    Serial.printf("Acessos: %d\n", contador);
}
```

Essas soluções garantem privacidade, permitindo a análise do uso sem comprometer a segurança dos usuários.

3.5 O EXPERIMENTO

A pesquisa foi realizada no pátio da Faculdade do Gama (FGA) da Universidade de Brasília (UnB), local escolhido estrategicamente por ser frequentado por estudantes, professores e funcionários, o que possibilitava alcançar um público diverso, com diferentes níveis de conhecimento em segurança digital, como demonostrado na Figura 3.1. Essa escolha foi crucial para ampliar o impacto educacional da campanha, focada em conscientizar os participantes sobre os riscos associados ao uso de redes Wi-Fi públicas. O objetivo principal era criar um ambiente controlado que simulasse cenários de ciberataques comuns, permitindo analisar a suscetibilidade dos usuários e promover boas práticas de segurança.

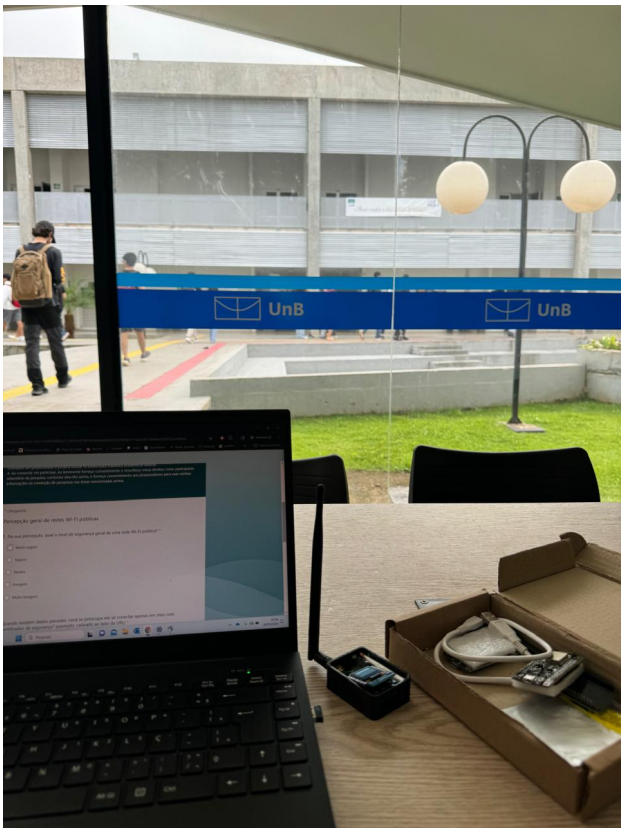

Figura 3.1: Experimento realizado na FGA

O experimento consistiu na criação de uma rede Wi-Fi pública falsa, utilizando o mesmo SSID (nome da rede) da rede legítima da UnB, como demonstrado na Figura 3.2. O SSID (Service Set Identifier) da rede falsa foi configurado para ter o mesmo nome da rede legítima da UnB. Esse procedimento faz parte da técnica de ataque conhecida como "Evil Twin"(Gêmeo Maligno). A ideia por trás dessa estratégia é criar uma rede Wi-Fi com um nome idêntico ao de uma rede confiável, de modo que os usuários desavisados, que anteriormente se conectavam à rede legítima, escolham automaticamente a rede falsa, sem perceber que estão conectando a uma rede insegura. Esse ataque tira proveito do comportamento comum dos dispositivos de se conectar automaticamente a redes previamente conhecidas, deixando os usuários vulneráveis a uma série de riscos cibernéticos, como roubo de dados ou ataques de man-in-the-middle (MITM). Nesse caso, o SSID falso agia como um "isca", capturando as conexões de dispositivos próximos, sem exigir autenticação inicial, o que tornava a rede ainda mais atraente para os usuários.

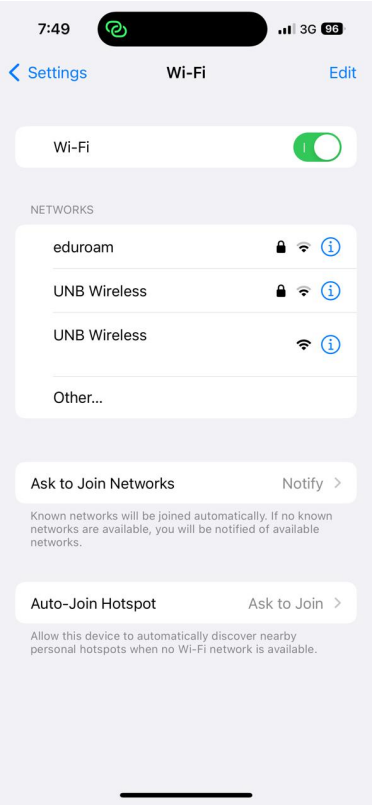

Figura 3.2: Exibição do SSID durante o ataque

Após a conexão à rede falsa, os participantes eram redirecionados para uma página de login que simulava um típico "Captive Portal", demonstrado na Figura 3.3. Esse tipo de página é comumente utilizado em redes Wi-Fi públicas para autenticação de usuários antes de permitir o acesso à internet. No experimento, o Captive Portal foi projetado para se assemelhar visualmente ao portal de login legítimo da UnB, incluindo o logo da universidade, o que tornava a página mais familiar e confiável para os participantes. A interface foi pensada para imitar de forma precisa a aparência da rede oficial, criando um ambiente que induzia os usuários a acreditarem que estavam acessando uma rede segura.

Além disso, a página de login oferecia opções para autenticação via redes sociais, como Instagram e Google, estratégias comumente usadas em muitas redes públicas para facilitar o acesso. Essas opções adicionavam um toque de familiaridade e conveniência, reforçando a ilusão de autenticidade do portal. Ao selecionar uma dessas opções e inserir suas credenciais, os usuários estariam, na verdade, entregando informações valiosas a um atacante. A página, portanto, atuava como uma ferramenta para coletar dados pessoais dos usuários de maneira fraudulenta, o que caracteriza um ataque de phishing.

Esse tipo de ataque é especialmente perigoso, pois engana os usuários ao se passar por uma rede legítima, comprometendo informações sensíveis sem levantar suspeitas. O Captive Portal, ao pedir credenciais pessoais, pode levar os participantes a um cenário onde suas senhas, dados de login e até mesmo informações de redes sociais sejam capturados e utilizados de forma indevida. Esse exemplo reforça a importância de estar atento ao tipo de rede à qual se conecta, pois, mesmo em um ambiente aparentemente seguro e familiar, como o da UnB, os riscos de segurança cibernética podem ser elevados, especialmente em redes Wi-Fi públicas.

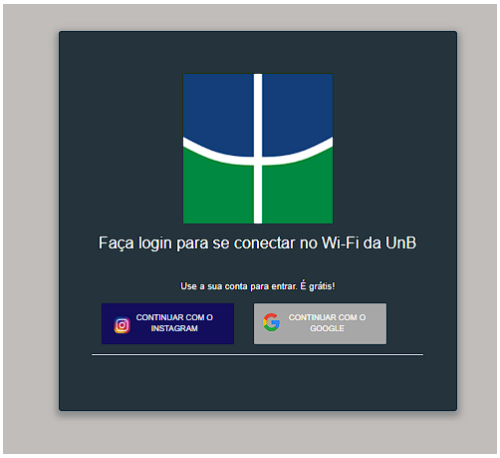

Figura 3.3: Exibição do SSID durante o ataque

Após preencherem o formulário falso, os participantes eram redirecionados para uma página educativa, demonstrado na Figura 3.4, que explicava o experimento e alertava sobre os riscos de redes Wi-Fi públicas. A página abordava boas práticas de segurança, como verificar a autenticidade das redes, usar VPNs, checar certificados de segurança e evitar inserir informações sensíveis. Além disso, fornecia orientações sobre como proteger dados pessoais e evitar fraudes.

Ao final do experimento, conforme ilustrado na Figura 3.5, os participantes eram convidados a responder a um formulário baseado em uma escala Likert. O objetivo era avaliar sua percepção sobre a segurança em redes públicas e suas práticas de proteção. Esse formulário, representado na Figura 3.6, permitiu medir o nível de maturidade cibernética dos participantes, fornecendo dados valiosos sobre o impacto da conscientização.

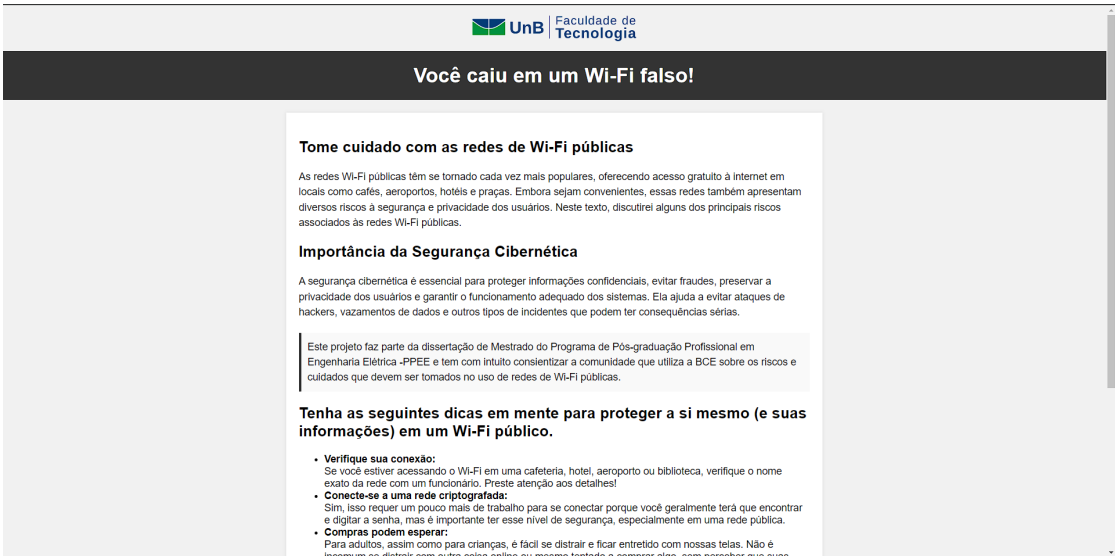

Figura 3.4: Topo da página de conscientização

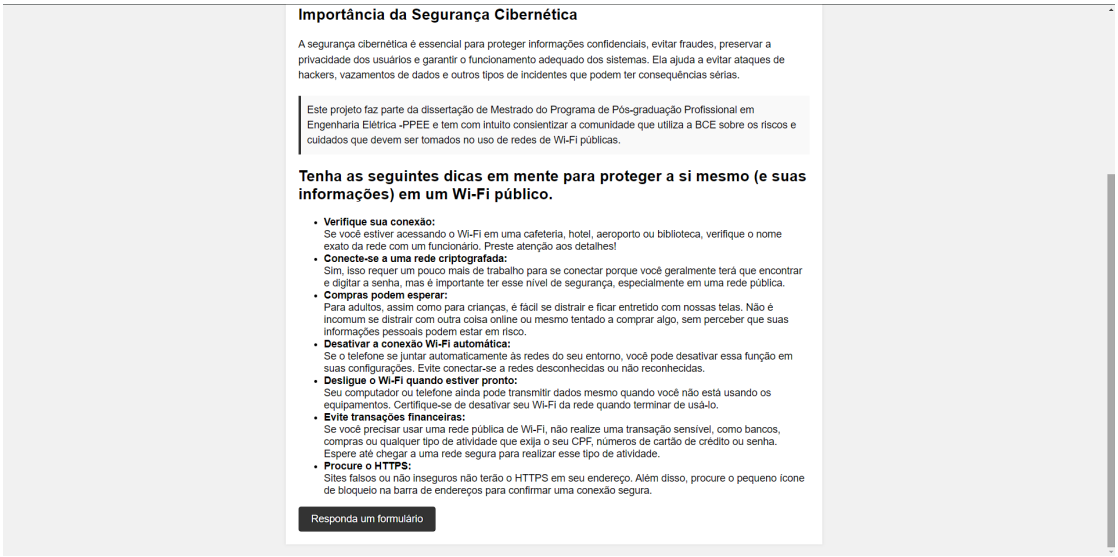

Figura 3.5: Fim da página de conscientização

A seguir, estão detalhadas as 14 perguntas aplicadas aos participantes:

1. **Percepção geral sobre redes Wi-Fi públicas:** A primeira pergunta buscou compreender a percepção inicial dos participantes sobre a segurança de redes Wi-Fi públicas. Foi solicitado que classificassem essas redes em uma escala de *"Muito seguro"* a *"Muito inseguro"*. Essa escala visava identificar a confiança geral dos usuários em redes públicas antes mesmo de receberem qualquer tipo de informação ou conscientização. A análise dessa percepção inicial é essencial para mapear o entendimento básico e as possíveis lacunas no conhecimento sobre os riscos associados a essas redes.

2. **Certificados de segurança:** Nesta questão, os participantes indicaram a frequência com que verificam a presença de certificados de segurança em sites acessados enquanto estão conectados a redes públicas. O certificado, geralmente representado por um ícone de cadeado ao lado da URL, indica que o site utiliza criptografia para proteger os dados transmitidos. As respostas variaram de *"Sempre"* a *"Nunca"*. Essa pergunta foi importante para avaliar o nível de atenção dos usuários ao identificar elementos básicos de segurança em ambientes digitais e sua conscientização em relação a conexões seguras.

3. **Informações pessoais compartilhadas:** Os participantes foram questionados sobre quais tipos de informações pessoais acreditavam ter compartilhado em redes Wi-Fi públicas. Entre as opções disponíveis estavam senhas, números de cartão de crédito, dados de identificação pessoal (como CPF e RG), informações empresariais e nenhuma informação. Essa questão foi elaborada para identificar a vulnerabilidade potencial dos usuários e os tipos de dados mais frequentemente expostos em ambientes públicos não seguros.

4. **Confiança em portais cativos:** Portais cativos, amplamente utilizados em redes públicas, como em aeroportos e cafeterias, exigem autenticação ou aceitação de termos de uso antes de conceder acesso à internet. A questão avaliou o nível de preocupação dos participantes com a segurança e autenticidade desses portais, utilizando uma escala Likert que variava de *"Concordo totalmente"*

a *"Discordo totalmente"*. Essa análise foi fundamental para entender o grau de confiança que os usuários depositam em portais que, em alguns casos, podem ser simulados por atacantes.

5. **Risco de roubo de dados:** A quinta pergunta investigou a percepção dos participantes sobre a possibilidade de roubo de dados em redes Wi-Fi públicas. Eles avaliaram a concordância com a afirmação de que informações pessoais poderiam ser interceptadas devido à ausência de criptografia e proteção adequada no tráfego de dados. Essa questão visava medir a consciência sobre vulnerabilidades técnicas em redes abertas.

6. **Medo de ataques de phishing:** Ataques de phishing, que utilizam técnicas de engenharia social para enganar usuários e obter informações confidenciais, foram o tema central desta questão. Os participantes indicaram seu nível de preocupação em relação a esses ataques ao utilizar redes públicas. Essa questão ajuda a avaliar o nível de conhecimento dos usuários sobre como os ataques de phishing podem ocorrer, especialmente em cenários de redes falsas.

7. **Risco de spoofing de redes:** O risco de falsificação de redes, ou spoofing, foi investigado para entender a percepção dos participantes sobre a possibilidade de se conectarem a redes falsas que imitam redes legítimas. Essa questão buscou avaliar o quanto os usuários estão cientes desse tipo de ataque e das consequências associadas.

8. **Infecção por malware:** Nesta questão, foi solicitado que os participantes indicassem seu nível de preocupação com a possibilidade de seus dispositivos serem infectados por malware ao se conectarem a redes Wi-Fi públicas. A preocupação com infecções por malware é crucial para medir a consciência dos usuários sobre como dispositivos conectados a redes não seguras podem ser vulneráveis a softwares maliciosos.

9. **Monitoramento por empresas ou governos:** Os participantes foram questionados sobre a crença de que informações ou comunicações realizadas em redes públicas poderiam ser monitoradas por empresas ou governos. Essa questão abordou aspectos mais amplos de privacidade e vigilância, buscando entender como os usuários percebem a segurança de suas atividades digitais em redes públicas.

10. **Ataques Man-in-the-Middle (MITM):** Os ataques do tipo Man-in-the-Middle (MITM), nos quais um atacante intercepta a comunicação entre duas partes, foram explorados nesta questão. Os participantes avaliaram seu temor em relação à possibilidade de suas comunicações serem interceptadas por terceiros enquanto utilizam redes públicas. Essa preocupação reflete o entendimento dos usuários sobre os riscos de comunicação não criptografada.

11. **Ações após suspeita de coleta de dados:** Os participantes foram convidados a indicar quais ações considerariam tomar caso suspeitassem que suas informações foram coletadas sem consentimento em uma rede pública. As opções incluíam desconectar da rede, alterar senhas, utilizar e-mails temporários, cancelar cartões de crédito, entre outras. Essa questão foi importante para avaliar a prontidão dos usuários em adotar medidas reativas para mitigar potenciais danos após um incidente de segurança.

12. **Segurança percebida em locais públicos:** A percepção de segurança ao utilizar redes públicas em ambientes específicos, como cafés, aeroportos e universidades, foi avaliada. Os participantes indicaram o nível de segurança que atribuíam a esses locais, permitindo identificar variações na percepção dependendo do ambiente e da familiaridade do usuário com ele.

13. **Responsabilidade das organizações:** Nesta questão, os participantes avaliaram se acreditavam que organizações que fornecem redes públicas deveriam ter a responsabilidade de alertar os usuários sobre os riscos envolvidos. Essa pergunta abordou a percepção dos participantes sobre o papel das empresas e instituições na promoção de práticas seguras e na educação digital.

14. **Conscientização comunitária:** Por fim, foi avaliado se os participantes acreditavam que a conscientização sobre os riscos associados ao uso de redes Wi-Fi públicas deveria ser mais amplamente disseminada na comunidade. Essa questão reflete a percepção de necessidade por iniciativas educacionais que abordem práticas seguras e riscos digitais em redes públicas.

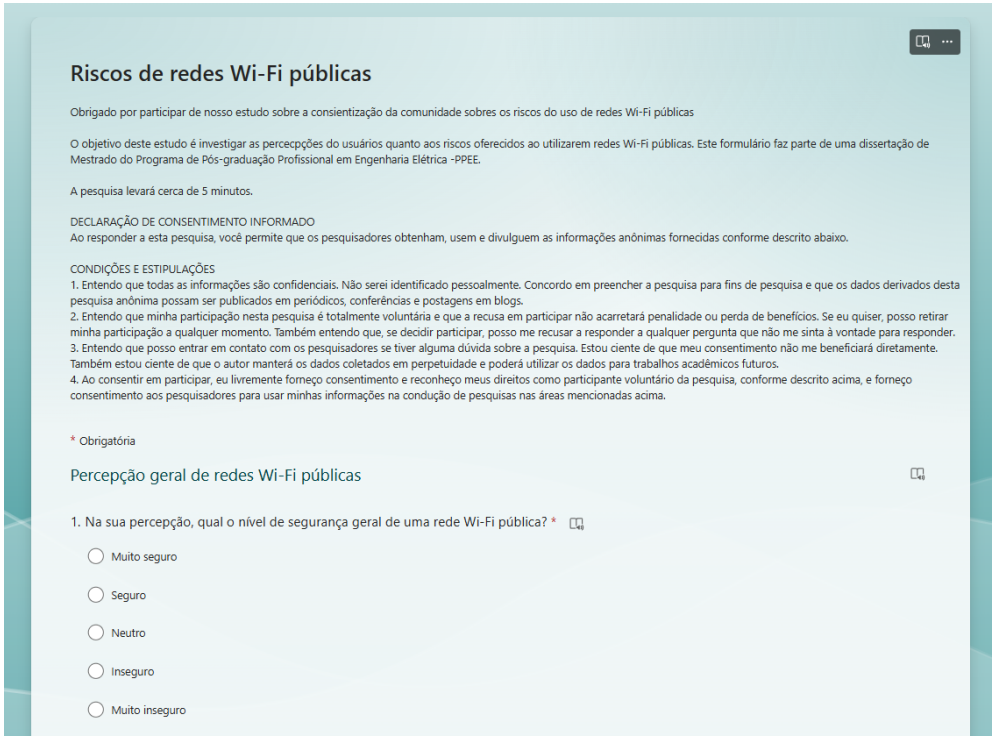

Figura 3.6: Formulário fornecido para avaliação

O dispositivo central do experimento, ilustrado na Figura 3.7, foi o ESP32, um microcontrolador reconhecido por seu alto desempenho e versatilidade. Amplamente utilizado em projetos de IoT, o ESP32 se destaca por sua capacidade de integração com Wi-Fi e Bluetooth. Sua escolha foi essencial para viabilizar o experimento, permitindo uma configuração adaptável e eficiente para simular cenários de ciberataques de forma realista e controlada.

Internamente, o ESP32 é equipado com um processador dual-core Tensilica Xtensa LX6, operando em frequências de até 240 MHz, o que garante processamento rápido e eficiente para lidar com múltiplas tarefas simultâneas. No contexto do experimento, essa capacidade de processamento foi crucial para gerenciar

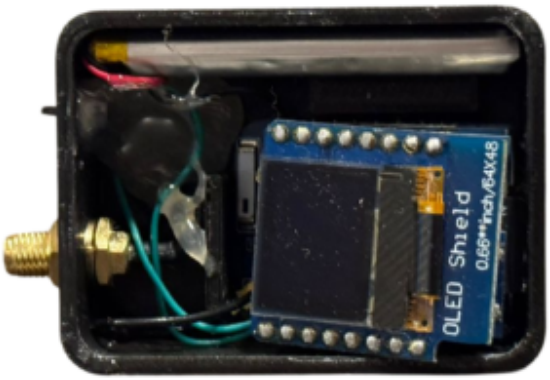

Figura 3.7: ESP32 desenvolvido

a operação do portal cativo, o servidor DNS local e o redirecionamento de tráfego, sem comprometer o desempenho ou a estabilidade do sistema. O processamento multitarefa permitiu que o ESP32 mantivesse a rede Wi-Fi ativa, redirecionasse as requisições dos usuários e monitorasse as conexões em tempo real, tudo de forma integrada. (Cameron 2023)

O ESP32 também possui 520 KB de SRAM (Static Random-Access Memory), que foi utilizada para armazenar variáveis e processar dados temporários relacionados às requisições feitas pelos dispositivos conectados. Além disso, o microcontrolador oferece suporte a 4 MB de Flash externa, utilizada no experimento para armazenar o firmware e os arquivos do portal cativo por meio do sistema de arquivos SPIFFS. Essa configuração garantiu que as páginas HTML, folhas de estilo CSS e scripts JavaScript necessários fossem carregados rapidamente, proporcionando uma experiência fluida aos participantes que interagiram com o portal.

O módulo de Wi-Fi do ESP32, ilustrado na Figura 3.8, suporta os padrões IEEE 802.11 b/g/n, permitindo que o microcontrolador funcione como cliente ou ponto de acesso (SoftAP). No experimento, foi configurado no modo SoftAP, permitindo que ele criasse sua própria rede Wi-Fi local. Essa funcionalidade foi essencial para replicar o ataque "Evil Twin", simulando uma rede confiável com o mesmo SSID da rede legítima da universidade. Essa característica do ESP32 garante a compatibilidade com uma ampla variedade de dispositivos móveis e laptops, tornando-o ideal para estudos como este.

Figura 3.8: Módulo WiFi do ESP32

Embora o ESP32 já tenha uma antena integrada, foi adicionada uma antena externa omnidirecional, conectada por um conector U.FL, com um ganho de 3 dBi, conforme demonstrado na Figura 3.9. Esse ganho ampliou consideravelmente o alcance do sinal Wi-Fi, permitindo cobrir até 30 metros, dependendo das condições ambientais, como obstáculos, interferências e a densidade de outros sinais. A antena foi posicionada estrategicamente para maximizar a cobertura no pátio da universidade, garantindo que o sinal fosse distribuído uniformemente, atendendo a usuários em movimento e assegurando uma experiência de conectividade estável em diferentes pontos do ambiente.

A escolha do ESP32 como dispositivo central do experimento deve-se à sua combinação de alto desempenho, versatilidade e custo acessível em comparação a outros microcontroladores, como o ESP8266 e modelos de outras marcas. Embora o ESP8266 seja uma opção mais econômica, o ESP32 oferece recursos adicionais que justificam seu investimento, como processador dual-core, maior número de GPIOs e suporte nativo a Bluetooth, ampliando as possibilidades de aplicação em projetos mais complexos. Além disso, quando comparado a microcontroladores de especificações semelhantes de outras marcas, o ESP32 frequentemente apresenta um preço mais competitivo, tornando-o uma escolha vantajosa para desenvolvedores que buscam equilibrar desempenho e custo em seus projetos.

Essa configuração foi crucial para simular as condições reais de redes Wi-Fi públicas, que frequentemente precisam oferecer boa cobertura em espaços abertos, onde a distribuição do sinal pode ser desafiadora. A antena externa permitiu otimizar o sinal para suportar múltiplas conexões simultâneas, garantindo uma experiência de navegação mais realista e representativa das redes públicas que são comuns em locais de grande circulação.

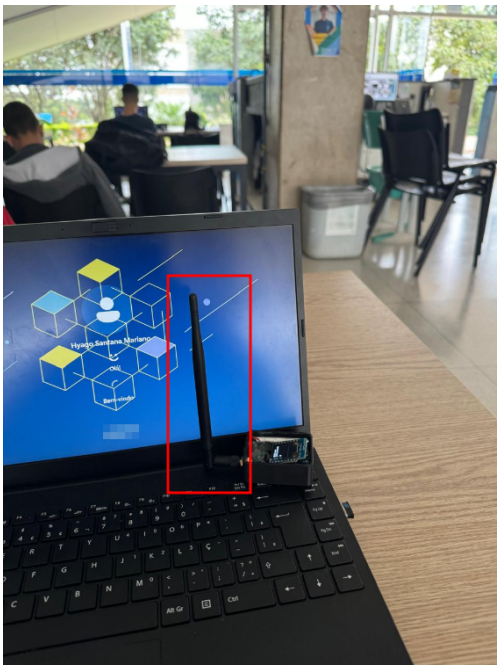

Figura 3.9: Antena no ESP32

Outro ponto importante do módulo Wi-Fi do ESP32 é o suporte a modulação QAM (Quadrature Amplitude Modulation) e ao modo de economia de energia Wi-Fi (Wi-Fi Power Save Mode), que otimiza o consumo energético durante a operação. Isso foi particularmente relevante no contexto do experimento, pois o dispositivo foi alimentado por uma bateria recarregável conectada por uma entrada mini USB, proporcionando autonomia suficiente para várias horas de operação contínua. Essa combinação eliminou a dependência de fontes de energia fixas, permitindo o reposicionamento do dispositivo para otimizar o alcance do sinal conforme necessário.

Para gerenciar os arquivos do portal cativo, foi integrado ao ESP32 um módulo SD que armazenou as páginas HTML, folhas de estilo CSS e scripts JavaScript necessários. O sistema de arquivos SPIFFS foi utilizado para organizar e acessar esses arquivos de forma eficiente. Além disso, um display OLED, conforme ilustrado na Figura 3.10, foi incorporado, permitindo o monitoramento em tempo real de informações críticas, como o número de conexões ativas e o status do sistema. Essa funcionalidade foi essencial para ajustes rápidos durante o experimento.

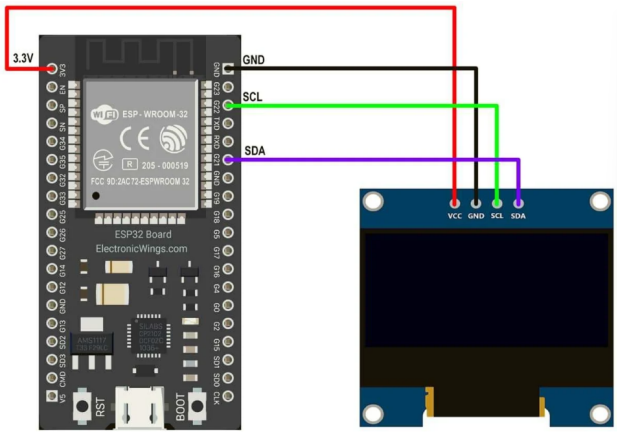

Figura 3.10: OLED Shield ESP32

Para redirecionar o tráfego dos dispositivos conectados, foi implementado um servidor DNS local, que direcionava todas as solicitações HTTP ao portal cativo. Esse redirecionamento replicava de forma realista um cenário de ataque, demonstrando como redes falsas podem capturar informações de usuários desavisados. Contudo, para assegurar a ética do estudo, o sistema foi configurado para descartar imediatamente quaisquer dados inseridos pelos participantes, garantindo que nenhuma informação sensível fosse armazenada ou utilizada.

O pátio da FGA, como espaço central da faculdade, proporcionou um fluxo contínuo de usuários de diferentes perfis. A proximidade com salas de aula e a biblioteca contribuiu para atrair participantes que buscavam conexão Wi-Fi para estudos, pesquisa ou comunicação. Essa localização estratégica foi crucial para ampliar o alcance e a representatividade do estudo, simulando com eficácia os riscos associados ao uso de redes públicas.

Combinando a robustez do ESP32 e a configuração detalhada de seus componentes — incluindo o módulo Wi-Fi, a antena externa, o display OLED, o módulo SD e a bateria recarregável —, o experimento conseguiu replicar de maneira eficaz os riscos associados ao uso de redes públicas. Essa abordagem não apenas educou os participantes sobre os perigos dessas redes, mas também reforçou a importância de

práticas seguras, como verificar certificados de segurança, utilizar VPNs e evitar o compartilhamento de informações sensíveis em ambientes não protegidos. A integração entre tecnologia, planejamento estratégico e objetivos educacionais resultou em uma solução prática, ética e altamente informativa para conscientizar a comunidade acadêmica sobre segurança digital.

4 RESULTADOS

Os resultados das 14 perguntas aplicadas aos participantes fornecem uma visão ampla sobre as práticas, percepções e lacunas de segurança cibernética ao utilizar redes Wi-Fi públicas. Este capítulo oferece uma análise aprofundada de cada aspecto identificado na pesquisa, destacando tendências comportamentais, falhas de percepção e oportunidades para melhorias em educação e infraestrutura de segurança.

4.1 ANÁLISE QUANTITATIVA DOS RESULTADOS

Os participantes demonstraram uma percepção generalizada de insegurança ao utilizar redes Wi-Fi públicas, mas os dados também revelam comportamentos contraditórios e lacunas importantes na adoção de práticas seguras. A seguir, são apresentadas as interpretações quantitativas de cada questão abordada na pesquisa:

4.1.1 Percepção de segurança geral das redes Wi-Fi públicas

A grande maioria (95%) considera as redes Wi-Fi públicas inseguras ou muito inseguras. Este dado demonstra que os participantes têm consciência dos riscos teóricos associados a essas redes. Entretanto, essa percepção de insegurança nem sempre se traduz em ações preventivas, como evitar transações financeiras ou o compartilhamento de dados sensíveis em tais redes.

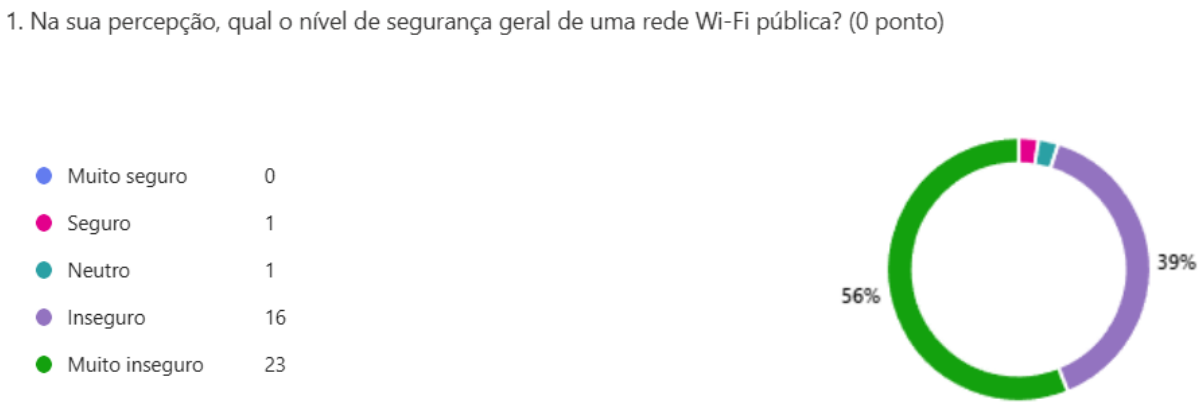

Figura 4.1: Percepção de segurança geral das redes Wi-Fi públicas

4.1.2 Conexão apenas em sites com certificados de segurança

A pesquisa revelou que 58% dos participantes raramente ou nunca verificam a presença de certificados de segurança antes de acessar sites em redes Wi-Fi públicas. Isso expõe um comportamento de alto risco,

pois a ausência de SSL/TLS aumenta a vulnerabilidade a ataques de interceptação e phishing.

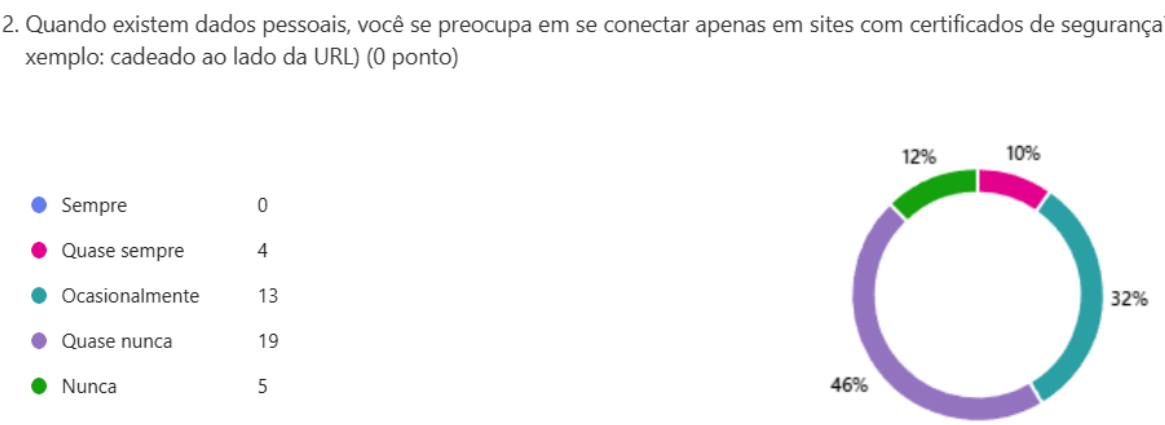

Figura 4.2: Conexão apenas em sites com certificados de segurança

4.1.3 Compartilhamento de informações pessoais em redes públicas

Os dados indicam que credenciais de contas online (38 pessoas), informações de identificação pessoal (33) e números de cartões de crédito (26) são compartilhados frequentemente em redes Wi-Fi públicas. Esse comportamento é altamente problemático, pois tais dados podem ser interceptados facilmente em redes não criptografadas.

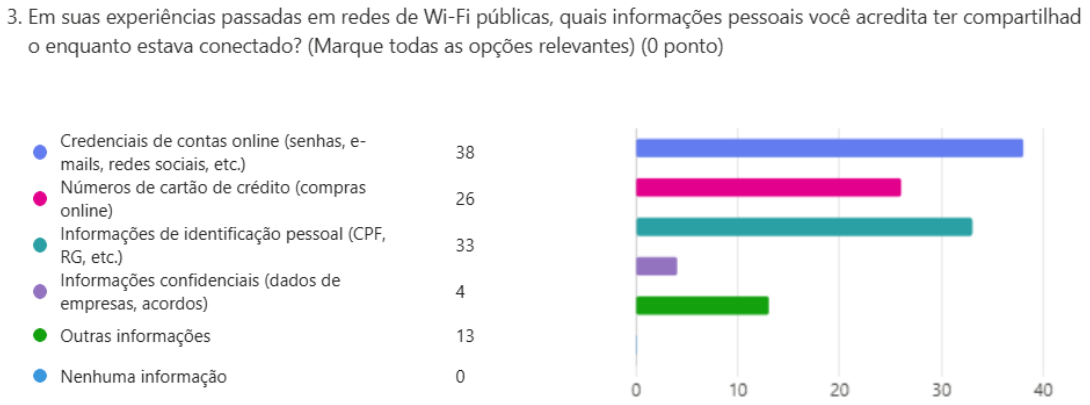

Figura 4.3: Compartilhamento de informações pessoais em redes públicas

4.1.4 Preocupação com a segurança dos captive portals

A maioria dos participantes (66%) não demonstra preocupação com a autenticidade e segurança dos captive portals utilizados para acessar redes públicas. Essa subestimação dos riscos é preocupante, considerando que portais falsos podem ser usados para roubar credenciais ou disseminar malware.

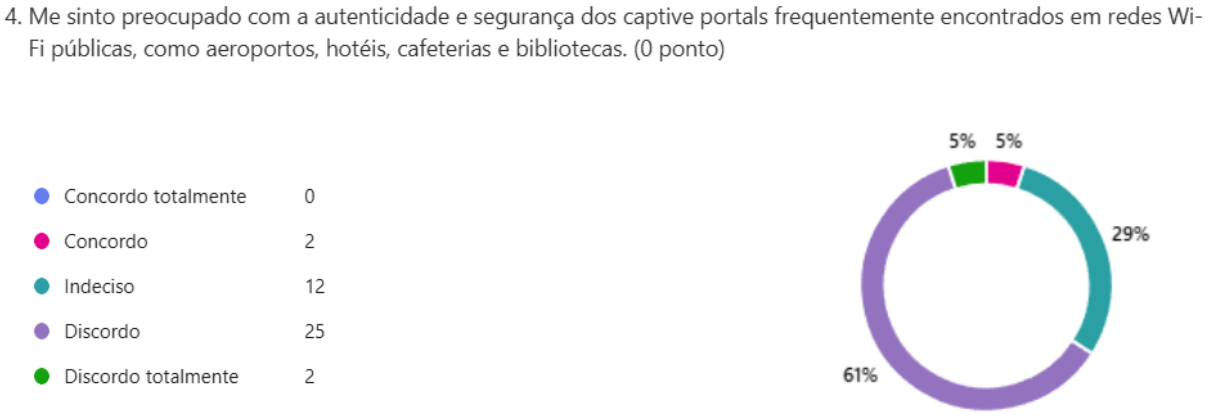

Figura 4.4: Preocupação com a segurança dos captive portals

4.1.5 Riscos de roubo de dados

Cerca de 80% dos participantes concordaram que redes Wi-Fi públicas, por serem desprotegidas, aumentam o risco de roubo de dados. Apesar disso, muitos não tomam medidas proativas, como o uso de VPNs ou a desconexão de redes após concluir o uso.

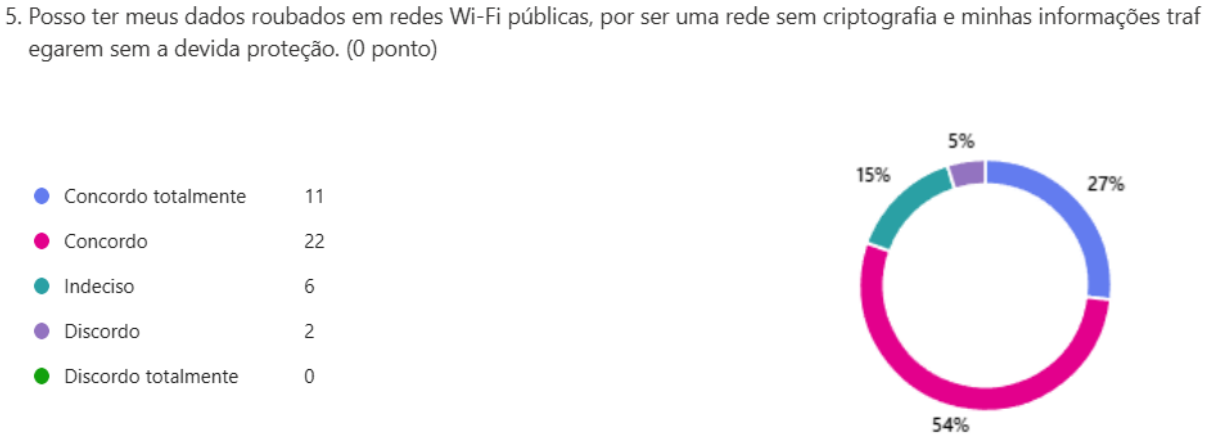

Figura 4.5: Riscos de roubo de dados

4.1.6 Preocupação com phishing

Quase metade dos participantes demonstrou indecisão ou falta de preocupação com ataques de phishing, o que reflete um desconhecimento sobre como tais ataques operam. Como phishing continua sendo uma das principais ameaças cibernéticas, isso representa uma vulnerabilidade crítica.

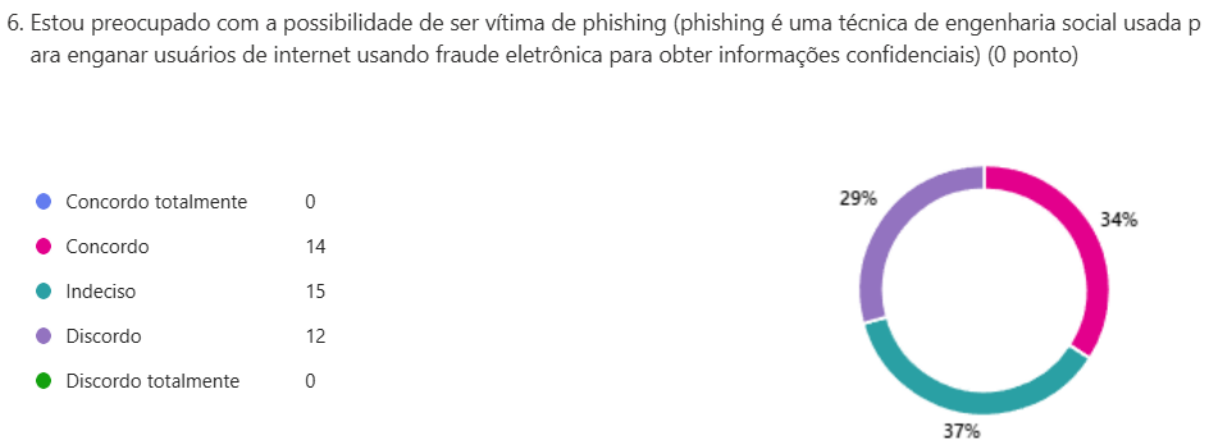

Figura 4.6: Preocupação com phishing

4.1.7 Risco de spoofing

O desconhecimento sobre spoofing é evidente, com 28 participantes indicando indecisão sobre esse risco. Spoofing ocorre quando redes falsas imitam redes legítimas para enganar usuários, capturando seus dados.

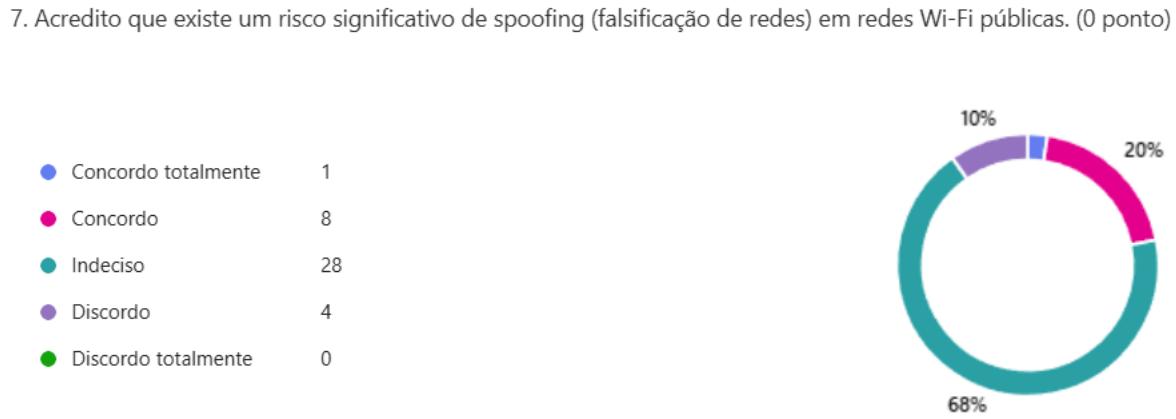

Figura 4.7: Risco de spoofing

4.1.8 Preocupação com malware e vírus

Apenas 31% dos participantes demonstraram preocupação significativa com a possibilidade de infecção por malware em redes Wi-Fi públicas. Essa baixa percepção de risco é preocupante, especialmente porque redes públicas podem ser utilizadas para disseminar malware de forma eficaz.

8. Estou preocupado com a possibilidade de meu dispositivo ser infectado por malware ou vírus ao usar redes Wi-Fi públ icas. (0 ponto)

Figura 4.8: Preocupação com malware e vírus

4.1.9 Monitoramento por governos ou empresas

Cerca de 63% dos participantes acreditam que suas informações podem ser monitoradas por governos ou empresas ao utilizar redes Wi-Fi públicas. Essa preocupação é válida, considerando que redes públicas podem ser exploradas para monitoramento de dados por terceiros mal-intencionados ou mesmo instituições legítimas.

9. Eu acredito que minhas informações podem ser coletadas ou monitoradas pelo governo ou empresas ao usar redes W i-Fi públicas. (0 ponto)

Figura 4.9: Monitoramento por governos ou empresas

4.1.10 Ataques de Man-in-the-Middle (MITM)

Poucos participantes demonstraram preocupação com ataques MITM, com 39 deles mostrando indecisão ou discordância. Isso é alarmante, considerando que ataques MITM são amplamente utilizados para interceptar comunicações em redes públicas e obter acesso a informações sensíveis.

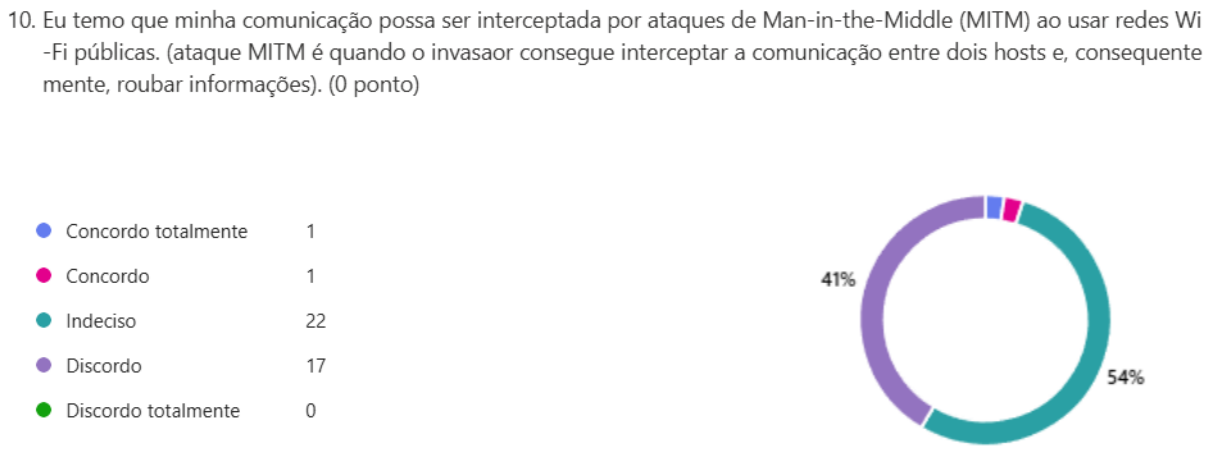

Figura 4.10: Ataques de Man-in-the-Middle (MITM)

4.1.11 Respostas a suspeitas de coleta indevida de informações

A desconexão imediata da rede foi a principal ação mencionada pelos participantes (40 pessoas), seguida pela troca de senhas (34). No entanto, poucas pessoas consideraram medidas mais abrangentes, como notificar autoridades competentes ou cancelar cartões de crédito comprometidos.

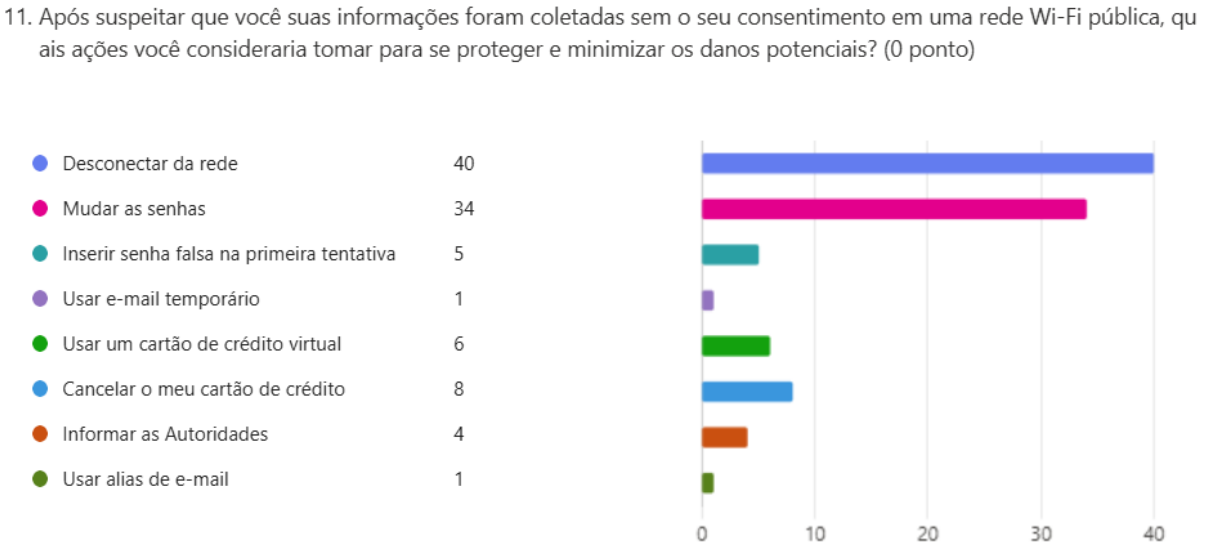

Figura 4.11: Respostas a suspeitas de coleta indevida de informações

4.1.12 Percepção de segurança em locais públicos

Cafés, aeroportos, shoppings e universidades foram amplamente percebidos como locais inseguros para o uso de redes Wi-Fi, com 83% dos participantes expressando essa visão. Essa percepção pode ser atribuída à falta de protocolos de segurança robustos nesses locais e à natureza desprotegida das redes públicas.

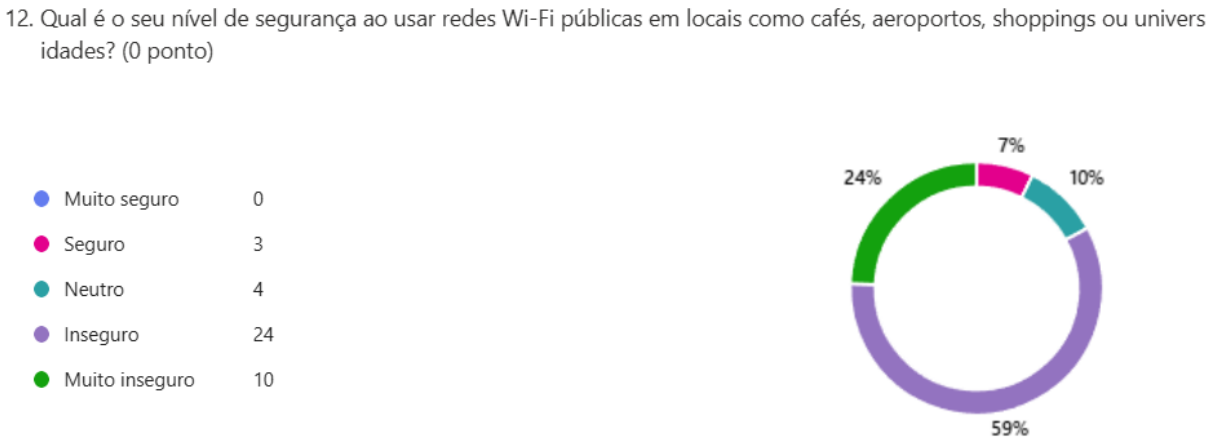

Figura 4.12: Percepção de segurança em locais públicos

4.1.13 Responsabilidade das organizações

Todos os participantes concordaram que organizações que oferecem redes Wi-Fi públicas têm a responsabilidade de informar os usuários sobre os riscos envolvidos. Essa unanimidade reflete a expectativa de que os provedores desempenhem um papel ativo na conscientização e segurança.

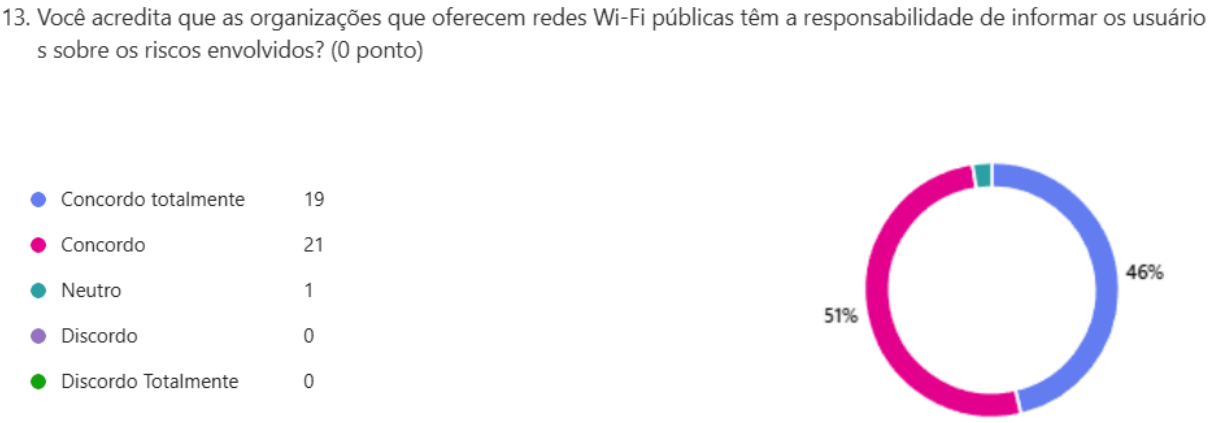

Figura 4.13: Responsabilidade das organizações

4.1.14 Conscientização na comunidade

Todos os participantes acreditam que a conscientização sobre os riscos das redes Wi-Fi públicas deve ser mais difundida na comunidade. Isso indica que os usuários reconhecem a importância de campanhas educativas que conectem informações práticas a exemplos reais de riscos e soluções.

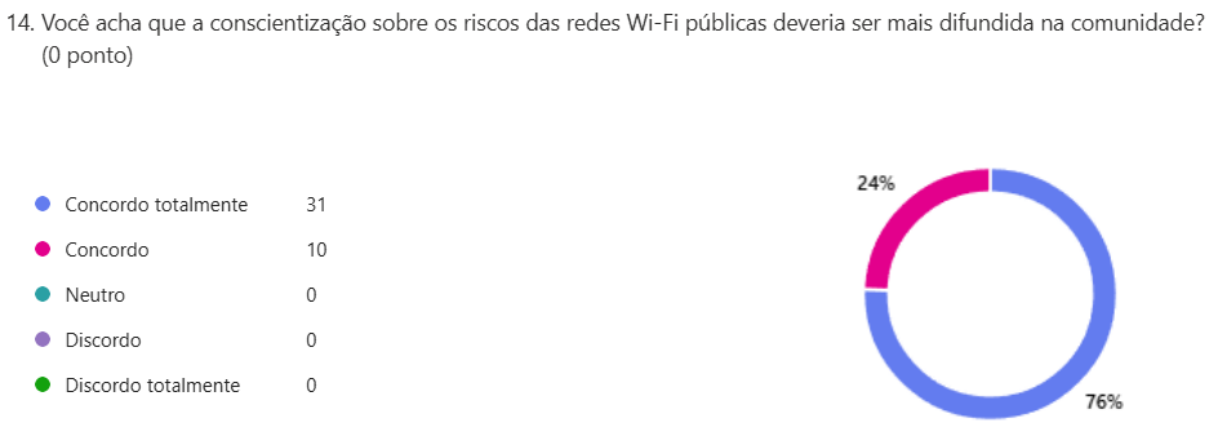

Figura 4.14: Conscientização na comunidade

4.2 ANÁLISE QUALITATIVA DOS RESULTADOS

A pesquisa revelou uma série de comportamentos e percepções que fornecem uma visão profunda sobre como os usuários interagem com redes Wi-Fi públicas, especialmente em relação aos riscos cibernéticos e à segurança online. Embora a maioria dos participantes tenha consciência dos perigos envolvidos, muitos não adotam as medidas necessárias para se proteger. A análise a seguir explora as implicações desses comportamentos, destacando as lacunas de conhecimento, as falhas nas práticas de segurança e as necessidades de intervenção educacional.

1. **Percepção Geral de Segurança das Redes Wi-Fi Públicas**
   A alta porcentagem (95%) de participantes que considera as redes Wi-Fi públicas inseguras reflete uma conscientização sólida sobre os riscos teóricos dessas redes. No entanto, o paradoxo se revela quando esse reconhecimento não resulta em comportamentos preventivos adequados. Isso sugere uma falha na tradução do conhecimento para a prática, revelando que, embora os usuários compreendam o risco teórico, não possuem confiança ou habilidades para adotar as práticas necessárias para proteger seus dados em tais ambientes.

   Esse fenômeno reflete uma lacuna crítica no entendimento prático da segurança digital. Os usuários sabem que as redes públicas oferecem riscos, mas muitas vezes não sabem como se proteger ativamente. Isso implica na necessidade urgente de abordagens educacionais mais eficazes, que não apenas expliquem os riscos, mas também capacitem os usuários com ferramentas concretas para mitigar esses perigos. Para promover mudanças comportamentais, as campanhas de conscientização precisam abordar a psicologia da segurança, focando não apenas na informação, mas também em como integrá-la à rotina do usuário de forma intuitiva.

2. **Conexão Apenas em Sites com Certificados de Segurança**
   O fato de 58% dos participantes raramente ou nunca verificarem os certificados de segurança ao acessar sites em redes Wi-Fi públicas evidencia uma falta de atenção aos detalhes cruciais de proteção online. Apesar de a maioria saber sobre a importância do SSL/TLS, muitos não incorporam essa prática de segurança de maneira consistente. Isso sugere uma deficiência na aplicação de boas práticas

de segurança e uma subestimação dos riscos associados à navegação em sites não criptografados.

Essa falta de atenção à segurança reflete uma falta de hábitos de verificação entre os usuários. Para promover a mudança, é necessário transformar a verificação dos certificados em uma ação automática, simples e parte do comportamento cotidiano, algo que deve ser trabalhado por meio de treinamentos mais interativos e campanhas educativas que mostrem as consequências concretas de uma navegação não segura. A educação deve tornar esse hábito parte do comportamento normal de uso da internet, transformando-o em algo intuitivo.

3. **Compartilhamento de Informações Pessoais em Redes Públicas**
   A alta taxa de compartilhamento de informações sensíveis, como credenciais de contas online, números de cartões de crédito e dados pessoais, revela uma profunda falta de percepção do risco por parte dos participantes. Embora muitos reconheçam os perigos das redes Wi-Fi públicas, continuam a expor suas informações a um risco considerável. Isso pode ser explicado pela falta de compreensão sobre como os ataques acontecem e a subestimação das consequências de uma violação de dados.

   Esse comportamento revela uma falta de internalização do risco. Para que a segurança se torne uma prioridade, os usuários precisam ser educados sobre as consequências reais do compartilhamento de dados sensíveis, e como esse comportamento pode resultar em danos significativos. A conscientização deve ser intensificada com exemplos reais de roubos de dados em redes públicas, além de demonstrar como práticas simples, como o uso de criptografia e VPNs, podem proteger os dados sem exigir grande esforço. A educação deve transformar a prevenção em uma prática intuitiva e natural.

4. **Preocupação com a Segurança dos Captive Portals**
   O fato de 66% dos participantes não demonstrarem preocupação com a autenticidade dos captive portals é indicativo de uma falta de conhecimento sobre como os atacantes podem se aproveitar dessas ferramentas para capturar credenciais ou espalhar malware. Embora os captive portals sejam uma prática comum em redes Wi-Fi públicas, os usuários parecem não compreender os riscos associados a essas portas de entrada, o que os torna vulneráveis a ataques sofisticados como o "Evil Twin"ou phishing.

   A falta de percepção sobre o risco de um portal falso sublinha a necessidade de educação mais aprofundada sobre os tipos de ataques que podem ocorrer em redes públicas. As campanhas de conscientização devem ser focadas em como identificar sinais de um portal falso, como a discrepância no nome da rede ou URLs suspeitas. Ao tornar essas ameaças mais tangíveis e visíveis, os usuários serão mais propensos a reconhecer os riscos e adotar práticas preventivas, como a verificação do endereço URL antes de inserir qualquer informação pessoal.

5. **Riscos de Roubo de Dados**
   A percepção de que as redes Wi-Fi públicas aumentam o risco de roubo de dados é amplamente reconhecida por 80% dos participantes, mas esse conhecimento não é traduzido em ações práticas, como o uso de VPNs ou o fechamento de sessões ao final do uso. Isso sugere que, embora os usuários estejam cientes dos riscos, eles subestimam a gravidade das consequências ou sentem que as medidas de proteção são difíceis ou inconvenientes de serem implementadas.

   Esse comportamento reflete uma falta de urgência em relação à proteção de dados. Para que mudanças significativas ocorram, é necessário criar um sentimento de urgência e relevância em torno da

segurança cibernética. As campanhas educacionais devem incluir exemplos práticos, demonstrando o impacto real de um roubo de dados em redes públicas e como ações simples, como o uso de VPNs ou a desconexão imediata após o uso, podem reduzir significativamente o risco.

6. **Preocupação com Phishing**
   A falta de preocupação com ataques de phishing, demonstrada por uma parte significativa dos participantes, revela um desconhecimento sobre como esses ataques operam e como podem ser facilmente disfarçados. Phishing continua sendo uma das ameaças mais comuns, mas a falta de atenção dos participantes para esse risco sugere que a educação sobre as táticas de engenharia social ainda é superficial.

   O phishing é uma ameaça insidiosa, pois os atacantes costumam usar métodos cada vez mais sofisticados para enganar os usuários. A conscientização precisa ser mais focada em exemplos concretos, mostrando como os ataques de phishing se disfarçam de emails legítimos, mensagens de texto ou sites falsificados. Além disso, é fundamental educar os usuários sobre como reconhecer sinais de phishing e adotar comportamentos de verificação (como sempre verificar o remetente de um email ou a URL de um site) para se proteger.

7. **Risco de Spoofing**
   A incerteza em relação ao risco de spoofing entre os participantes indica um desconhecimento fundamental sobre como as redes falsas podem imitar redes legítimas para capturar dados pessoais. O spoofing é uma ameaça difícil de ser percebida por usuários comuns, pois as redes falsas geralmente aparecem com nomes semelhantes às legítimas, criando uma falsa sensação de segurança.

   Esse comportamento demonstra a necessidade de uma conscientização mais técnica sobre os tipos de ataques que ocorrem em ambientes de redes públicas. Para que os usuários possam evitar cair em armadilhas de spoofing, é necessário educá-los sobre como verificar a autenticidade das redes Wi-Fi antes de se conectar, utilizando métodos como autenticação multifatorial ou a verificação do SSID da rede.

8. **Preocupação com Malware e Vírus**
   A falta de preocupação com malware em redes Wi-Fi públicas, observada em apenas 31% dos participantes, é um reflexo da subestimação da vulnerabilidade dos dispositivos em ambientes não seguros. Embora os riscos de malware sejam amplamente conhecidos, a ideia de que um dispositivo pode ser infectado em uma rede pública parece abstrata para a maioria.

   Para mudar essa mentalidade, é crucial aumentar a conscientização sobre como os dispositivos podem ser facilmente infectados por malware em redes não seguras. A educação deve incluir exemplos visuais e práticos, demonstrando como os ataques de malware ocorrem e como simples medidas preventivas, como a atualização constante de antivírus ou a utilização de VPNs, podem proteger o usuário.

9. **Monitoramento por Governos ou Empresas**
   A percepção de que suas informações podem ser monitoradas por governos ou empresas enquanto utilizam redes Wi-Fi públicas é compartilhada por 63% dos participantes. No entanto, a falta de ações concretas para proteger a privacidade online sugere que, embora os usuários se preocupem com o monitoramento, eles não sabem como implementar práticas de proteção de privacidade.

Esse comportamento reflete uma falta de habilidades para proteger a privacidade. Para que as pessoas se sintam mais capacitadas a proteger seus dados, é necessário educá-las sobre ferramentas acessíveis de privacidade, como o uso de VPNs, criptografia de ponta a ponta e navegação anônima. Além disso, é preciso desmistificar as soluções de segurança, tornando-as simples e acessíveis para todos.

10. **Respostas a Suspeitas de Coleta Indevida de Informações**
    A resposta reativa de desconectar-se da rede ou trocar senhas ao suspeitar de uma violação de dados é uma boa prática inicial, mas ainda reflete uma falta de planejamento estruturado para lidar com incidentes de segurança. Isso indica que os usuários não sabem como agir de forma abrangente em resposta a possíveis violações de dados.

    Uma abordagem mais eficaz seria educar os usuários sobre como adotar uma estratégia de resposta a incidentes, incluindo ações como notificar as autoridades, monitorar contas bancárias e revisar configurações de segurança. As campanhas educativas devem fornecer um plano de ação claro que ajude os usuários a responder de maneira mais eficiente e menos estressante a incidentes de segurança.

11. **Percepção de Segurança em Locais Públicos**
    A alta taxa de percepção de insegurança nas redes Wi-Fi de locais públicos, como cafés e aeroportos, revela uma sensação de vulnerabilidade coletiva. Embora os participantes saibam que essas redes são vulneráveis, muitos não sabem como se proteger ou se sentem desmotivados a adotar as medidas necessárias. Esse comportamento reflete um medo geral de ataques, que é muitas vezes impulsionado pela falta de confiança nas redes públicas.

    A solução aqui envolve aumentar a educação prática sobre como usar essas redes com segurança, como evitar transações sensíveis e o uso de VPNs para criar uma camada adicional de proteção. Além disso, é crucial educar os usuários sobre como minimizar a exposição a riscos, como desabilitar o compartilhamento de arquivos e desativar a conectividade automática a redes públicas.

12. **Responsabilidade das Organizações**
    A unanimidade de que as organizações devem informar os usuários sobre os riscos das redes Wi-Fi públicas reflete a percepção de que não é responsabilidade exclusiva do usuário garantir sua segurança. As organizações têm a obrigação de fornecer não apenas o serviço de internet, mas também educação e ferramentas para proteger os dados dos usuários.

    Esse desejo reflete um apelo por mais responsabilidades corporativas no campo da segurança cibernética. Para atender a essa demanda, as organizações devem não apenas fornecer acesso seguro, mas também promover campanhas educativas claras sobre segurança, além de implementar protocolos de segurança robustos para proteger as informações dos usuários.

13. **Conscientização na Comunidade**
    A totalidade dos participantes acredita que a conscientização sobre os riscos das redes Wi-Fi públicas precisa ser mais difundida na comunidade. Isso reflete uma necessidade coletiva de maior informação sobre os riscos e as práticas de segurança. Essa percepção sugere que, embora muitos indivíduos se sintam vulneráveis, eles também reconhecem que a solução não é apenas individual, mas comunitária.

Essa demanda por maior conscientização implica que, para haver uma mudança real no comportamento da sociedade, a educação sobre segurança cibernética deve ser coletiva e acessível, focando na disseminação de informações de forma ampla e eficaz. Isso inclui campanhas educativas em escolas, empresas e comunidades, além de envolver as organizações como facilitadoras dessa disseminação de conhecimento.

14. **Conscientização na Comunidade**

    A totalidade dos participantes (100%) acredita que a conscientização sobre os riscos das redes Wi-Fi públicas precisa ser mais difundida na comunidade. Isso reflete uma necessidade coletiva de maior informação sobre os riscos e as práticas de segurança no uso de redes públicas. Esse ponto revela que os usuários, ao reconhecerem os riscos associados às redes Wi-Fi públicas, esperam não só que os esforços educacionais se concentrem neles individualmente, mas também que essas informações sejam espalhadas de forma mais ampla para a comunidade.

    O fato de todos os participantes concordarem com a necessidade de mais conscientização indica que, além de se sentirem vulneráveis, eles também reconhecem que o problema é maior do que um simples fator individual. Há uma percepção compartilhada de que a segurança cibernética não é apenas responsabilidade do indivíduo, mas de toda uma rede de comunicação, onde o conhecimento precisa ser disseminado coletivamente. Essa busca por maior conscientização reflete um desejo de mudanças estruturais, com a percepção de que, para haver um ambiente mais seguro, a informação deve estar disponível de maneira acessível e disseminada entre todos os membros da sociedade, não apenas no nível individual.

    A unanimidade aqui também mostra que, embora as pessoas saibam que o problema é grande, elas não se sentem preparadas ou equipadas para enfrentá-lo sozinhas. Elas esperam que campanhas de conscientização não só forneçam dados, mas também ajudem as pessoas a se sentirem mais seguras ao adotar práticas de proteção de forma mais simples e direta. Além disso, essas campanhas precisam conectar o conceito de segurança com o comportamento do dia a dia, fazendo com que as pessoas vejam esses problemas como algo próximo, prático e que pode ser resolvido com medidas que fazem parte da rotina, como o uso de redes seguras, criptografia e conscientização sobre as ameaças.

5 CONCLUSÃO

A crescente utilização de redes Wi-Fi públicas em diversos espaços, como cafeterias, aeroportos e universidades, reflete a busca por maior comodidade e conectividade no cotidiano. Contudo, essa conveniência é acompanhada por sérias ameaças à segurança cibernética, que colocam em risco dados pessoais, privacidade e dispositivos dos usuários. Este estudo abordou essas questões por meio da criação de um portal cativo educacional utilizando um microcontrolador ESP32, com o objetivo de analisar o comportamento dos participantes e mensurar sua maturidade cibernética.

Recapitulando a introdução, o trabalho foi motivado pela necessidade de avaliar e melhorar a conscientização dos usuários quanto aos riscos das redes públicas. Para isso, foram estabelecidos cinco objetivos principais: (a) avaliar o comportamento dos usuários ao se conectar a redes Wi-Fi públicas; (b) analisar a eficácia de um portal cativo educacional na promoção da conscientização sobre riscos cibernéticos; (c) mensurar a maturidade cibernética dos usuários; (d) propor recomendações para boas práticas de segurança; e (e) sugerir uma metodologia replicável para estudos semelhantes. Este capítulo conclui o trabalho, refletindo sobre os resultados obtidos e destacando as contribuições teóricas e práticas, além de sugerir direções futuras para pesquisas nesta área.

5.1 PRINCIPAIS OBSERVAÇÕES

1. **Percepção geral sobre redes Wi-Fi públicas:** O comportamento dos usuários foi investigado por meio de um ambiente experimental no campus da Universidade de Brasília, onde uma rede Wi-Fi falsa com o mesmo SSID da rede institucional foi configurada. Os resultados mostraram que uma proporção significativa dos participantes não verificou a autenticidade da rede antes de se conectar, expondo-se às ameaças simuladas. Esta descoberta é consistente com estudos anteriores que indicam que a conveniência frequentemente supera as preocupações com segurança na tomada de decisão dos usuários.

   Além disso, foi possível observar que as diferenças de comportamento entre os grupos de participantes variaram de acordo com sua experiência prévia em segurança cibernética. Por exemplo, usuários com maior familiaridade com práticas seguras demonstraram maior resistência a se conectar à rede falsa, enquanto aqueles sem treinamento ou conhecimento específico foram mais propensos a cair no cenário simulado. Essa divisão reforça a importância de programas educativos continuados e adaptados a diferentes níveis de experiência.

2. **Efetividade do Portal Cativo Educacional:** O portal cativo foi projetado para informar os usuários sobre os riscos associados ao uso de redes públicas, como ataques Man-in-the-Middle (MITM) e roubo de credenciais, além de oferecer orientações práticas sobre medidas de segurança, como o uso de VPNs e autenticação em dois fatores. Os dados coletados indicaram que a experiência educacional aumentou a percepção de risco dos participantes e forneceu informações relevantes para a melhoria de suas práticas de segurança.

Ademais, o impacto do portal cativo foi mais perceptível entre os participantes que interagiram diretamente com os conteúdos educacionais disponibilizados. Esses usuários relataram maior intenção de implementar as boas práticas recomendadas, como evitar o compartilhamento de informações sensíveis em redes públicas e habilitar recursos de segurança adicionais em seus dispositivos. Isso sugere que a forma de entrega das mensagens educativas é um elemento crucial para seu impacto.

3. **Mensuração da Maturidade Cibernética:** A maturidade cibernética foi avaliada através de um questionário baseado em escala Likert, que abordou temas como compreensão de riscos de phishing, verificação de certificados de segurança e conhecimento de ataques MITM. Os resultados evidenciaram lacunas significativas, como a baixa atenção à presença de certificados de segurança e a ausência de preocupação com a autenticidade de portais cativos. Estes achados ressaltam a necessidade de educação continuada para aumentar a maturidade dos usuários.

   Foi também observada uma correlação entre idade e maturidade cibernética, com participantes mais jovens apresentando maior propensão a subestimar riscos. Por outro lado, participantes com mais experiência em ambientes corporativos demonstraram maior conscientização sobre medidas de segurança. Esse resultado indica que programas de treinamento específicos para diferentes faixas etárias e contextos de uso podem ser mais eficazes na promoção de boas práticas.

4. **Recomendações para Boas Práticas:** Com base nos resultados, foram sugeridas recomendações práticas, como evitar transações sensíveis em redes públicas, usar conexões seguras (VPNs), habilitar autenticação em dois fatores e verificar certificados de segurança. Também foi destacado o papel de provedores de redes públicas em promover boas práticas de segurança.

   Além disso, foram propostas soluções tecnológicas adicionais, como a implementação de redes Wi-Fi segmentadas com maior controle de acesso e o uso de sistemas automáticos para detectar conexões suspeitas. Essas medidas podem ser combinadas com campanhas educativas para maximizar sua eficácia.

5. **Proposição de Metodologia Replicável:**

   A configuração experimental com o microcontrolador ESP32 mostrou-se uma solução acessível e eficiente para simular cenários reais de risco. A abordagem pode ser replicada em outros contextos, incluindo ambientes corporativos e comunitários, ampliando seu alcance e relevência.

   A flexibilidade da metodologia permite adaptações para testar diferentes tipos de ataque ou avaliar grupos específicos, como crianças e idosos, que podem ter necessidades educativas distintas. Além disso, a natureza de baixo custo do ESP32 possibilita que instituições de ensino e organizações não governamentais implementem experiências similares sem onerar seus orçamentos.

5.2 CONTRIBUIÇÕES TEÓRICAS E PRÁTICAS

Este estudo fornece contribuições significativas para a literatura acadêmica e prática sobre segurança cibernética em redes Wi-Fi públicas. Em termos teóricos, explora uma metodologia inovadora baseada no uso de portais cativos educacionais integrados a microcontroladores para mensurar a maturidade ciber-

nética dos usuários. Tal abordagem preenche uma lacuna na literatura ao propor um modelo replicável e adaptável a diferentes contextos, permitindo a análise de comportamentos, percepção de riscos e práticas de segurança em ambientes de rede não protegidos.

Do ponto de vista prático, a implementação do microcontrolador ESP32 oferece uma solução tecnológica acessível e escalável para conscientização em segurança cibernética. Este dispositivo, amplamente utilizado em projetos de Internet das Coisas (IoT), possibilita a criação de um ambiente de simulação realista que expõe vulnerabilidades, educa os usuários no momento do risco e fornece orientações práticas para mitigação. A integração de conteúdos educativos em ferramentas de uso cotidiano, como redes Wi-Fi públicas, representa uma inovação pedagógica ao promover o aprendizado contextualizado.

Além da exposição ao risco simulado, a conscientização foi reforçada por meio de explicações detalhadas sobre boas práticas de segurança. Os usuários foram instruídos a adotar medidas como a verificação de certificados de segurança, o uso de VPNs para criptografar seus dados, a ativação da autenticação multifator para proteger contas sensíveis e a desativação de conexões automáticas a redes Wi-Fi abertas. O conteúdo apresentado buscou não apenas alertar sobre os perigos, mas também oferecer soluções práticas e acessíveis, possibilitando que qualquer pessoa pudesse reforçar sua segurança digital imediatamente.

Outro aspecto essencial da conscientização foi a aplicação de um questionário, no qual os participantes avaliaram seu próprio conhecimento e comportamento em relação à segurança cibernética. Essa etapa permitiu que refletissem sobre suas ações e percebessem lacunas em sua compreensão sobre o tema. Os resultados coletados evidenciaram que muitos usuários subestimam ameaças como ataques Man-in-the-Middle e se conectam a redes sem se preocupar com a autenticação da fonte. A partir dessas respostas, reforçou-se a importância de manter campanhas educativas contínuas para garantir que os usuários não apenas reconheçam os riscos, mas desenvolvam hábitos seguros no dia a dia.

O impacto da conscientização foi potencializado pelo formato do experimento: ao invés de apenas transmitir informações teóricas, os participantes vivenciaram uma situação de vulnerabilidade antes de receberem as orientações corretivas. Esse método se mostrou eficaz ao estimular um aprendizado ativo e duradouro, tornando os usuários mais atentos e preparados para evitar ameaças reais. A simulação de risco, seguida de um aprendizado imediato, demonstrou ser uma estratégia poderosa para a promoção da cultura de segurança cibernética.

Adicionalmente, o estudo propõe um modelo metodológico sistemático e replicável para medição da maturidade cibernética, com potencial para aplicação em estudos futuros, programas de treinamento organizacionais e iniciativas de conscientização comunitária. Este modelo é fundamentado em princípios de usabilidade, acessibilidade e aplicabilidade, garantindo que os resultados obtidos sejam relevantes para diferentes perfis de usuários e organizações.

Entre as contribuições práticas destacam-se: (i) a validação do uso de portais cativos como ferramentas educacionais eficazes para aumentar a percepção de riscos relacionados a ataques como phishing, spoofing e interceptações do tipo Man-in-the-Middle (MITM); (ii) a coleta de dados empíricos sobre comportamentos e lacunas de conhecimento dos usuários em redes públicas, essencial para o desenvolvimento de campanhas educativas mais direcionadas; e (iii) a promoção de uma cultura de segurança digital que transcende o ambiente acadêmico, com impacto direto na redução de vulnerabilidades no uso de redes Wi-Fi públicas.

Por fim, o estudo ressalta a importância de políticas e práticas institucionais voltadas à segurança cibernética. Organizações que fornecem acesso Wi-Fi público, como universidades, aeroportos e cafés, podem adotar este modelo para implementar estratégias preventivas, promovendo um ambiente digital mais seguro e resiliente. Assim, esta pesquisa não apenas avança o entendimento acadêmico sobre o tema, mas também oferece soluções práticas para desafios contemporâneos de segurança da informação.

5.3 TRABALHOS FUTUROS

Com base nas limitações e nos achados deste estudo, algumas direções para pesquisas futuras incluem:

1. **Estudos de Longo Prazo:** Investigar o impacto de campanhas educacionais continuadas na mudança de comportamento dos usuários em relação a redes Wi-Fi públicas.
2. **Ampliação do Escopo:** Replicar o experimento em outros contextos, como espaços corporativos, escolas e comunidades vulneráveis, para identificar padrões específicos de comportamento.
3. **Tecnologias Emergentes:** Integrar inteligência artificial e aprendizado de máquina para personalizar conteúdos educacionais e prever comportamentos de risco.
4. **IoT e Redes Públicas:** Explorar as vulnerabilidades associadas a dispositivos IoT em redes públicas e propor soluções específicas para esses cenários.
5. **Criação de Ferramentas Interativas:** Desenvolver aplicações móveis que simulem ataques cibernéticos de forma gamificada, promovendo aprendizado prático e engajante.
6. **Aspectos Psicossociais:** Investigar os fatores psicossociais que influenciam a adesão a boas práticas de segurança, considerando diferentes perfis de usuários.
7. **Eficiência de Novos Modelos Educacionais:** Avaliar a eficácia de diferentes abordagens pedagógicas, como simulações baseadas em realidade aumentada, para ensinar práticas seguras em redes públicas.
8. **Análise Comparativa entre Regiões:** Investigar diferenças culturais e regionais no comportamento de usuários frente às ameaças cibernéticas, adaptando soluções de acordo com as necessidades locais.

5.4 CONSIDERAÇÕES FINAIS

Este estudo destacou a importância de conscientizar os usuários sobre os riscos associados ao uso de redes Wi-Fi públicas e a eficácia de uma abordagem educativa por meio de portais cativos implementados em microcontroladores. A simulação de cenários realistas de ameaça, como o uso de uma rede falsa, permitiu não apenas avaliar o comportamento e a maturidade cibernética dos participantes, mas também promover uma reflexão crítica sobre práticas de segurança no ambiente digital.

Os resultados indicaram que, apesar de uma consciência geral sobre a insegurança das redes Wi-Fi públicas, existe uma lacuna significativa entre a percepção de risco e a adoção de medidas práticas de proteção, como o uso de VPNs, autenticação de dois fatores e a verificação de certificados de segurança. Essa desconexão reforça a necessidade de iniciativas educacionais mais direcionadas, capazes de transformar o conhecimento em ações concretas. A pesquisa indicou que grande parte dos usuários reconhece a insegurança dessas redes, mas ainda assim continua a utilizá-las. Esse comportamento contraditório pode ser explicado por uma combinação de fatores psicológicos, sociais e tecnológicos, onde a conveniência percebida muitas vezes supera a percepção de risco. A ausência de consequências imediatas e a baixa compreensão técnica sobre ataques cibernéticos contribuem para a manutenção desse hábito, tornando a conscientização sobre boas práticas de segurança digital um desafio crucial.

Dentre os principais fatores que levam ao uso contínuo das redes Wi-Fi públicas, destaca-se o viés de otimismo, um fenômeno psicológico no qual os indivíduos acreditam que eventos negativos são mais propensos a acontecer com outras pessoas do que com eles mesmos. Esse viés faz com que muitos usuários minimizem os riscos associados a ataques como Man-in-the-Middle (MITM) e Evil Twin, confiando erroneamente que não serão alvos de cibercriminosos. Além disso, a falta de conhecimento sobre as vulnerabilidades dessas redes reduz a percepção de perigo, criando um falso senso de segurança.

Outro aspecto relevante é a pressão social e a necessidade de conectividade. Em muitos ambientes, especialmente em locais de estudo ou trabalho, o uso de Wi-Fi público é praticamente inevitável. Quando os indivíduos percebem que outras pessoas ao seu redor estão conectadas sem aparente prejuízo, a sensação de risco diminui. Esse efeito de conformidade social reforça o uso dessas redes, pois os usuários assumem que, se muitos as utilizam, o perigo deve ser mínimo ou inexistente.

Adicionalmente, muitos usuários adotam estratégias de mitigação de risco que, embora úteis, são insuficientes para garantir total segurança. Medidas como "não acessar bancos online"ou "evitar o uso de redes sociais"são frequentemente mencionadas, mas ignoram ameaças mais complexas, como o sequestro de sessões (session hijacking) e a interceptação de tráfego criptografado. O desconhecimento sobre a real eficácia dessas precauções leva a uma falsa sensação de proteção, incentivando o comportamento arriscado.

A análise dos dados coletados nesta pesquisa reforça a existência desse paradoxo. Embora a maioria dos participantes reconheça os riscos associados ao Wi-Fi público, apenas uma pequena fração adota medidas concretas para evitar a exposição de dados sensíveis. Isso demonstra que a conscientização por si só não é suficiente para modificar o comportamento dos usuários. Para enfrentar esse desafio, é fundamental que estratégias educativas considerem aspectos psicológicos e sociais, utilizando abordagens interativas e práticas que demonstrem, de maneira tangível, os perigos reais da navegação insegura.

Além disso, campanhas educativas que abordem o viés de otimismo e o comportamento automatizado de conexão podem ser mais eficazes do que simples alertas técnicos. Somente por meio de uma abordagem multidisciplinar será possível equilibrar a necessidade de conectividade com a segurança digital, reduzindo os riscos inerentes ao uso de redes públicas.

Entretanto, é importante destacar que os resultados desta pesquisa refletem o comportamento de um público específico: a comunidade acadêmica da Faculdade do Gama (FGA) da Universidade de Brasília. Dessa forma, os achados não podem ser generalizados para toda a população, pois fatores como nível de conhecimento técnico, perfil profissional e contexto socioeconômico podem influenciar a percepção e o

comportamento dos usuários em relação à segurança digital. Estudos futuros poderiam ampliar a amostra, incluindo diferentes perfis de usuários, a fim de obter uma visão mais abrangente sobre esse fenômeno.

A metodologia proposta, baseada no uso de microcontroladores de baixo custo, como o ESP32, demonstrou ser viável e replicável em diferentes contextos. A mobilidade e o baixo custo do dispositivo ampliam seu potencial de aplicação, permitindo que iniciativas semelhantes alcancem um público mais diverso e em maior escala. Além disso, a abordagem utilizada preserva a privacidade dos participantes, ao mesmo tempo que oferece um aprendizado significativo, alinhando-se às melhores práticas éticas de pesquisa. Ao oferecer informações diretamente após a interação com o portal cativo, os participantes puderam compreender os riscos enfrentados e, mais importante, aprender estratégias para minimizar sua exposição a essas ameaças. Essa abordagem educativa, que alia conscientização teórica a experiências práticas, demonstrou ser altamente eficaz na promoção de uma cultura de segurança digital.

Além disso, o estudo destacou comportamentos de risco prevalentes, como o compartilhamento de informações sensíveis, incluindo credenciais de acesso e dados financeiros, mesmo em redes sabidamente inseguras. Esse padrão reflete não apenas uma carência de conhecimento técnico por parte dos usuários, mas também uma confiança excessiva em ambientes digitais que, muitas vezes, são explorados por agentes mal-intencionados. É fundamental que essas vulnerabilidades sejam tratadas com estratégias educacionais contínuas e acessíveis.

Outro aspecto crítico identificado foi a falta de atenção dos participantes em relação à autenticidade de portais cativos e certificados digitais. Essa despreocupação pode tornar os usuários alvos fáceis de ataques como phishing e Man-in-the-Middle (MITM), destacando a importância de reforçar práticas básicas de verificação e validação antes de se conectar a qualquer rede pública. Apesar dessa fragilidade, o estudo revelou um ponto positivo: o desejo universal dos participantes de aprender mais sobre como proteger suas informações, o que reforça o potencial de iniciativas educativas direcionadas.

A relevância deste trabalho se estende além dos resultados imediatos. Ele não apenas identificou vulnerabilidades e comportamentos de risco, mas também demonstrou que é possível transformar interações simples em oportunidades de aprendizado significativo. O uso de tecnologias acessíveis, como o ESP32, abre caminho para a implementação de soluções similares em outros contextos, desde instituições acadêmicas até espaços públicos de grande circulação. Essa replicabilidade amplia o impacto potencial da metodologia e ressalta sua utilidade como uma ferramenta educacional e de conscientização.

Em suma, este estudo contribui de maneira relevante para o campo da segurança cibernética, ao explorar uma abordagem prática, acessível e educativa para melhorar a maturidade cibernética dos usuários de redes Wi-Fi públicas. Ao promover boas práticas e transformar o conhecimento em ações concretas, cria-se um ambiente digital mais seguro e resiliente, beneficiando não apenas os indivíduos, mas a sociedade como um todo. A conscientização e a educação permanecem como pilares essenciais para a construção de uma cultura de segurança cibernética robusta e eficaz, especialmente em tempos de crescente conectividade e dependência de redes digitais.

REFERÊNCIAS BIBLIOGRÁFICAS

Abdulkader 2023 ABDULKADER, M. *Why do people use public Wi-Fi?: An investigation of risk-taking behaviour and factors lead to decisions*. 2023.

Adriaanse e Rensleigh 2013 ADRIAANSE, L. S.; RENSLEIGH, C. Web of science, scopus and google scholar: A content comprehensiveness comparison. *The Electronic Library*, Emerald Group Publishing Limited, v. 31, n. 6, p. 727–744, 2013.

Ahadi et al. 2020 AHADI, S. A. A. et al. Overview on public wi-fi security threat evil twin attack detection. In: IEEE. *2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI)*. [S.l.], 2020. p. 1–6.

Ali et al. 2019 ALI, S.; OSMAN, T.; MANNAN, M.; YOUSSEF, A. On privacy risks of public wifi captive portals. *arXiv preprint arXiv:1907.02142*, 2019.

Anand et al. 2018 ANAND, G.; PRATHIBA, S. B.; GUNASEKARAN; PONMANI. Detection of man in the middle attacks in wi-fi networks by ip spoofing. In: *2018 Tenth International Conference on Advanced Computing (ICoAC)*. [S.l.: s.n.], 2018. p. 319–322.

Australian Federal Police 2023 Australian Federal Police. *Man Charged Over Creation of Evil Twin Free Wi-Fi Networks to Access Personal Data*. 2023. <https://www.afp.gov.au/news-centre/media-release/man-charged-over-creation-evil-twin-free-wifi-networks-access-personal>. Accessed: 2025-01-08.

Bauer, Gonzales e McCoy 2008 BAUER, K.; GONZALES, H.; MCCOY, D. Mitigating evil twin attacks in 802.11. In: *2008 IEEE International Performance, Computing and Communications Conference*. [S.l.]: IEEE, 2008. p. 513–516.

Cameron 2023 CAMERON, N. Esp32 microcontroller. In: *ESP32 Formats and Communication: Application of Communication Protocols with ESP32 Microcontroller*. [S.l.]: Springer, 2023. p. 1–54.

Choi 2022 CHOI, H. Risk taking behaviors using public wi-fi™. *Information Systems Frontiers*, Springer, p. 1–18, 2022.

George 2024 GEORGE, A. S. Bridging the digital divide: Understanding the human impacts of digital transformation. 2024.

Golwala 2024 GOLWALA, M. S. The developement of the internet and the beginnings of the digital revolution. *Studia Społeczne*, Wydawnictwo im. Prof. LJ Krzyżanowskiego WSM w Warszawie, v. 44, n. 1, p. 233–258, 2024.

Guarezi 2019 GUAREZI, J. Engenharia social: avaliação de riscos e vulnerabilidades tendo o fator humano como o elo mais fraco da segurança da informação. *Sistemas de Informação-Pedra Branca*, 2019.

Hammad e Ati 2020 HAMMAD, L. A.; ATI, M. Assessing security health of public wi-fi environments in the uae. In: *2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*. [S.l.]: IEEE, 2020. p. 1–6.

Hossain et al. 2019 HOSSAIN, I.; HASAN, M. M.; HASAN, S. F.; KARIM, M. R. A study of security awareness in dhaka city using a portable wifi pentesting device. In: *2019 2nd International Conference on Innovation in Engineering and Technology (ICIET)*. [S.l.: s.n.], 2019. p. 1–6.

Hossain et al. 2019 HOSSAIN, I.; HASAN, M. M.; HASAN, S. F.; KARIM, M. R. A study of security awareness in dhaka city using a portable wifi pentesting device. In: IEEE. *2019 2nd International Conference on Innovation in Engineering and Technology (ICIET)*. [S.l.], 2019. p. 1–6.

Hussain et al. 2024 HUSSAIN, K.; RAHMATYAR, A. R.; RISKHAN, B.; SHEIKH, M. A. U.; SINDIRAMUTTY, S. R. Threats and vulnerabilities of wireless networks in the internet of things (iot). In: IEEE. *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*. [S.l.], 2024. p. 1–8.

Kampourakis et al. 2022 KAMPOURAKIS, V.; KAMBOURAKIS, G.; CHATZOGLOU, E.; ZAROLIAGIS, C. Revisiting man-in-the-middle attacks against https. *Network Security*, MA Business London, v. 2022, n. 3, 2022.

Kapicak et al. 2024 KAPICAK, L.; STIPAL, J.; TRUBAK, K.; MACHNIK, P.; BURDIAK, P.; ROZHON, J. Misuse of wi-fi data to analyze user behaviour. In: IEEE. *2024 ELEKTRO (ELEKTRO)*. [S.l.], 2024. p. 1–6.

Kwon e Choi 2020 KWON, S.; CHOI, H.-K. Evolution of wi-fi protected access: security challenges. *IEEE Consumer Electronics Magazine*, IEEE, v. 10, n. 1, p. 74–81, 2020.

Le et al. 2022 LE, D. T.; TRAN, T. T.; DANG, K. Q.; ALKANHEL, R.; MUTHANNA, A. Malware spreading model for routers in wi-fi networks. *IEEE Access*, IEEE, v. 10, p. 61873–61891, 2022.

Lotfy et al. 2021 LOTFY, A. Y.; ZAKI, A. M.; ABD-EL-HAFEEZ, T.; MAHMOUD, T. M. Privacy issues of public wi-fi networks. In: SPRINGER. *The International Conference on Artificial Intelligence and Computer Vision*. [S.l.], 2021. p. 656–665.

Maimon et al. 2022 MAIMON, D.; HOWELL, C. J.; JACQUES, S.; PERKINS, R. C. Situational awareness and public wi-fi users' self-protective behaviors. *Security Journal*, Springer, p. 1–21, 2022.

Mariano e Rocha 2017 MARIANO, A. M.; ROCHA, M. S. Revisão da literatura: apresentação de uma abordagem integradora. In: *AEDEM International Conference*. [S.l.: s.n.], 2017. v. 18, p. 427–442.

Medeiros 2021 MEDEIROS, I. C. O ciclo da inclusão digital: Social-digital-social/digital inclusion cycle: social-digital-social. *Brazilian Journal of Development*, v. 7, n. 8, p. 75705–75714, 2021.

Musuva et al. 2024 MUSUVA, P. M. et al. Determining the efficacy of cybersecurity awareness programs on enhancing wifi security behaviour. In: IEEE. *2024 IST-Africa Conference (IST-Africa)*. [S.l.], 2024. p. 1–8.

Singh et al. 2022 SINGH, R.; THAKKAR, R.; THAKKAR, M.; ROTE, U.; PATIL, S.; INGLE, B. Wifi deauth and cloning using esp8266. In: IEEE. *2022 5th International Conference on Advances in Science and Technology (ICAST)*. [S.l.], 2022. p. 1–5.

Sombatruang et al. 2018 SOMBATRUANG, N.; KADOBAYASHI, Y.; SASSE, M. A.; BADDELEY, M.; MIYAMOTO, D. The continued risks of unsecured public wi-fi and why users keep using it: Evidence from japan. In: *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. [S.l.]: IEEE, 2018. p. 1–11.

Sun et al. 2024 SUN, P.; ALQAHTANI, S.; YOUSAF, F. Z.; OTROK, H. A survey on privacy and security issues in iot-based environments. *Journal of Network and Computer Applications*, Elsevier, v. 14, n. 2, p. 105–120, 2024.

The Australian 2023 The Australian. *Hackers Target Aussie Airport Wi-Fi Networks with $20 Device, Mobile Security Firm Zimperium Says*. 2023. <https://www.theaustralian.com.au/business/hackers-target-aussie-airport-wifi-networks-with-20-device-mobile-security-firm-zimperium-says/news-story/9df9c7b007fdbbfb1ac0b9adc4e0a103>. Accessed: 2025-01-08.

Turland et al. 2015 TURLAND, J.; COVENTRY, L.; JESKE, D.; BRIGGS, P.; MOORSEL, A. van. Nudging towards security: developing an application for wireless network selection for android phones. In: *Proceedings of the 2015 British HCI Conference*. New York, NY, USA: Association for Computing Machinery, 2015. (British HCI '15), p. 193–201. ISBN 9781450336437. Disponível em: <https://doi.org/10.1145/2783446.2783588>.

Vaccari et al. 2021 VACCARI, I.; NARTENI, S.; MONGELLI, M.; AIELLO, M.; CAMBIASO, E. Perpetrate cyber-attacks using iot devices as attack vector: The esp8266 use case. In: *CEUR Workshop Proceedings*. [S.l.: s.n.], 2021. v. 2940, p. 35–46.

Zulkipli e Khusairi 2024 ZULKIPLI, N. H. N.; KHUSAIRI, M. I. B. An experimental analysis for public wi-fi attacks. In: IEEE. *2024 IEEE 6th Symposium on Computers & Informatics (ISCI)*. [S.l.], 2024. p. 247–252.