



INSTITUTO FEDERAL
Catarinense



TECNOLOGIA E REDES DE COMPUTADORES

11^a EDIÇÃO

VANDERLEI FREITAS JUNIOR
JARDEL BATISTA GONÇALVES
ALESSANDRO FERMIANO AMBONI DA SILVA



INSTITUTO FEDERAL
Catarinense



TECNOLOGIA E REDES DE COMPUTADORES

11^a EDIÇÃO

VANDERLEI FREITAS JUNIOR
JARDEL BATISTA GONÇALVES
ALESSANDRO FERMIANO AMBONI DA SILVA

2025

Instituto Federal Catarinense

INSTITUTO FEDERAL CATARINENSE**REITOR**

Rudinei Kock Exterckoter

PRÓ-REITORA DE ENSINO

Liane Vizzotto

**PRÓ-REITOR DE EXTENSÃO, PESQUISA, PÓS-GRADUAÇÃO E
INOVAÇÃO**

Cleder Alexandre Somensi

**PRÓ-REITORA DE DESENVOLVIMENTO, INCLUSÃO,
DIVERSIDADE E ASSISTÊNCIA À PESSOA**

Iara Mantoanelli

PRÓ-REITOR DE ADMINISTRAÇÃO

Jorge Luís de Souza Mota

CÂMPUS SOMBrio**DIRETOR GERAL**

Victor Martins de Sousa

DIRETOR DE ENSINO, PESQUISA E EXTENSÃO

Mirian Rocho da Rosa Silveira

INSTITUTO FEDERAL CATARINENSE,
CÂMPUS SOMBrio
Av. Prefeito Francisco Lummertz Júnior, 931
CEP 88960-000 - Sombrio/SC
www.sombrio.ifc.edu.br

Direção Editorial	Vanderlei Freitas Junior
Capa e Projeto Gráfico	Claiton Andrade Junior
Editoração Eletrônica	Vanderlei Freitas Junior
Comitê Editorial	Armando Mendes Neto
	Cleber Luiz Damin Ferro
	Diego Monsani
	Guilherme Klein da Silva Bitencourt
	Jardel Batista Gonçalves
	Jéferson Mendonça de Limas
	Joédio Borges Junior
	Marco Antônio Silveira de Souza
	Matheus Lorenzato Braga
	Sandra Vieira
	Vanderlei Freitas Junior
	Victor Martins de Sousa
Revisão	Gilnei Magnus dos Santos
Organizador	Vanderlei Freitas Junior
	Jardel Batista Gonçalves
	Alessandro Fermiano Amboni da Silva

Copyright © Vanderlei Freitas Junior.

Todos os direitos reservados. Proibida a venda.

As informações contidas no livro são de inteira responsabilidade dos seus autores.



Ficha catalográfica elaborada pela *Biblioteca do IFC Sombrio*

T255 Tecnologias e Redes de Computadores / Junior; Jardel Batista Gonçalves; Alessandro Fermiano Amboni da Silva (org.). -- 11. ed. -- Sombrio : Instituto Federal Catarinense, 2025.

92 f.

ISBN 978-65-01-78131-0

1. Redes de computadores - Gerência. 2. Proteção de dados I.Freitas Junior, Vanderlei - 1980-. II. Título.

CDD: Ed. 21 -- 004.6

Agradecimentos

Agradecemos as valiosas contribuições de Claiton Andrade Junior, Diego Monsani, Coordenação do Sistema Integrado de Bibliotecas do IFC, além dos alunos e professores que contribuíram com suas pesquisas para o engrandecimento desta publicação.

**Esta é uma publicação do
Curso Superior de**



Sumário de artigos

Uma nova década.....	10
Análise de vulnerabilidades de acesso da rede sem fio de empresas na cidade de Araranguá-SC	11
Atuação Profissional dos Alunos Egressos do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal Catarinense - Campus Sombrio	31
Uma proposta de controle de acesso e fluxo de veículos e pessoas utilizando LoRa para propriedades de grande extensão	70

Sumário de Autores

Samuel Severino Paulo Figueiredo.....	11
Jéferson Mendonça de Limas	11
Marco Antônio Silveira de Souza.....	11
Andrey Schwanck Machado.....	31
Victor Martins de Sousa	31
Jeferson da Silva dos Santos.....	70
Marco Antônio Silveira de Souza.....	70
Matheus Lorenzo Braga.....	70

Uma nova década

Vanderlei Freitas Junior

Há dez anos iniciávamos um projeto pioneiro de divulgação científica no Instituto Federal Catarinense, Câmpus Sombrio, que hoje inaugura uma nova década de existência. O livro digital com estudos do curso de Redes nasceu para dar visibilidade à produção acadêmica de nossos estudantes, pesquisadores e docentes, e chega agora a um momento de transição igualmente histórico: a extinção do Curso Superior de Tecnologia em Redes de Computadores e o nascimento do Curso de Bacharelado em Análise e Desenvolvimento de Sistemas. Este movimento, mais do que uma simples mudança de nomenclatura, simboliza a evolução institucional e a capacidade de se reinventar diante das demandas sociais, acadêmicas e tecnológicas que nos cercam.

Importa destacar que, assim como nos primeiros anos, esta obra continua a motivar e reconhecer os esforços daqueles que, após intensas pesquisas, encontram aqui a oportunidade de eternizar seus resultados, tornando-se autores de capítulos e partícipes de uma trajetória coletiva.

Talvez de outro modo esse reconhecimento não se concretizasse.

Aproveitamos, portanto, este marco para agradecer a todos que acreditaram e seguem acreditando no valor desta iniciativa, certos de que ela continuará a cumprir seu papel essencial: unir memória e futuro em torno do conhecimento e da formação acadêmica.

Análise de vulnerabilidades de acesso da rede sem fio de empresas na cidade de Araranguá-SC

Samuel Severino Paulo Figueiredo¹, Jéferson Mendonça de Limas², Marco Antônio Silveira de Souza³

¹, Acadêmico do Instituto Federal Catarinense – Campus Sombrio – 88960000 – Sombrio – SC – Brasil

^{2,3}, Docentes do Instituto Federal Catarinense – Campus Sombrio – 88960000 – Sombrio – SC – Brasil

samuelseverino375@gmail.com, jeferson.limas@ifc.edu.br,
marco.souza@ifc.edu.br

***Abstract:** This study aimed to identify and analyze vulnerabilities in Wi-Fi networks of small food businesses in Araranguá, Santa Catarina. The research made it possible to assess the technologies used, the security protocols implemented, the access control policies, and the main weaknesses in the evaluated infrastructures. As a contribution, practical improvements were suggested, such as equipment updates, network segmentation, and the adoption of hotspots for customers with responsibility agreements. Finally, it is expected that implementing these measures will result in greater security and efficiency for these networks.*

Resumo: Este trabalho teve como objetivo identificar e analisar as vulnerabilidades em redes Wi-Fi de pequenos comércios alimentícios em Araranguá,

Santa Catarina. A pesquisa possibilitou levantar as tecnologias utilizadas, os protocolos de segurança implementados, as políticas de controle de acesso e os principais pontos de fragilidade das infraestruturas avaliadas. Como contribuição, foram sugeridas melhorias práticas, como atualização de equipamentos, segmentação de redes, além da adoção de hotspots para clientes com termos de responsabilidade. Por fim, espera-se que a implementação dessas medidas resulte em maior segurança e eficiência para essas redes.

1. Introdução

A segurança em redes Wi-Fi é cada vez mais essencial em ambientes comerciais, onde a conectividade sem fio facilita o dia a dia dos negócios e a experiência do cliente. Conforme mencionado por Santos (2024), além de pequenos comércios, como padarias, restaurantes e clínicas médicas, órgãos governamentais também disponibilizam acesso Wi-Fi ao público, seja para operações internas ou para oferecer conectividade aos cidadãos. No entanto, essa praticidade vem acompanhada de riscos: redes Wi-Fi, quando mal configuradas ou sem as proteções adequadas, tornam-se vulneráveis a ataques que podem comprometer informações sensíveis, incluindo dados financeiros e registros médicos.

A exposição a ataques como invasões e espionagem de dados se tornou um problema frequente e exige que essas empresas tenham uma postura ativa em relação à segurança digital. Quando a rede Wi-Fi não está adequadamente protegida, invasores podem explorar falhas e acessar informações que deveriam estar restritas, colocando em risco a privacidade e a integridade de dados que são fundamentais para a confiança dos clientes, além dos cuidados e responsabilidades digitais jurídicas abordadas por Ribeiro (2018).

Este trabalho tem como objetivo geral identificar e analisar vulnerabilidades em redes Wi-Fi de pequenos comércios alimentícios em Araranguá, Santa Catarina. Para isso, busca-se identificar a tecnologia Wi-Fi utilizada, os protocolos de segurança implementados, as políticas de controle de acesso de clientes, responsáveis pela manutenção da rede e possíveis vulnerabilidades. Com base nessa análise, serão propostas soluções para melhorar a segurança e a eficiência dessas redes.

O presente artigo organiza-se em cinco seções. Na primeira, apresenta-se a introdução, abordando o tema, o problema de pesquisa, os objetivos e a justificativa do trabalho. Na seção 2, é exposto o referencial teórico, no qual são discutidos os principais conceitos relacionados ao estudo, como redes Wi-Fi, protocolos de segurança e métodos de auditoria. A seção 3 detalha a metodologia adotada, incluindo o planejamento, as ferramentas utilizadas e os critérios estabelecidos para análise. Na seção 4, são apresentados os resultados obtidos nos testes de segurança, acompanhados de uma discussão sobre as vulnerabilidades identificadas e suas implicações. Por fim, na seção 5, encontram-se as considerações finais, com um resumo dos principais achados, as contribuições do trabalho e sugestões para pesquisas futuras.

2 Referencial teórico

2.1 Segurança da Informação

Segundo Whitman & Mattord (2018), a segurança da informação é fundamental para proteger dados e sistemas de acessos não autorizados, danos e interrupções. Essa área é frequentemente abordada através de três pilares: confidencialidade, integridade e disponibilidade, que juntos formam a tríade CIA conforme mencionado na figura abaixo.

Figura 1: Tríade da Segurança da Informação.



Fonte:DEB SOLUTIONSTI (2015).

Whitman & Mattord (2018) destacam que a confidencialidade trata sobre proteger informações sensíveis, garantindo que apenas pessoas autorizadas possam acessá-las. Para isso, utilizamos diversas técnicas, como criptografia e controle de acesso, além de autenticação para verificar a identidade dos usuários. Por exemplo, o uso de senhas e autenticação multifatorial são práticas comuns para manter a confidencialidade.

Para Stallings (2017), a integridade refere-se à precisão e confiabilidade das informações. Isso significa que os dados devem permanecer inalterados, exceto por aqueles que têm permissão para fazê-lo. Para garantir a integridade, aplicamos técnicas como hashing, que ajudam a detectar qualquer alteração nos dados. Essa proteção é especialmente crucial em áreas onde a garantia da informação é vital, como em transações financeiras e registros médicos.

Disponibilidade na visão de Whitman & Mattord (2018) permite que as informações e sistemas estejam acessíveis quando necessário. Para isso, é importante garantir que a

infraestrutura de TI funcione corretamente e que existam planos de recuperação em caso de falhas. Medidas como redundância, backups e monitoramento contínuo são práticas comuns que ajudam a manter a disponibilidade dos serviços.

2.2 Conexão Wi-Fi

Segundo Tanenbaum (2021), a conexão Wi-Fi como conhecemos surgiu no ano de 1997 com o padrão IEEE 802.11. O padrão inicial permitia uma conexão de até 2Mbps, sendo o ponto de partida para uma grande evolução que viria ao decorrer dos anos seguintes. Por volta de 1999 com o desenvolvimento do padrão 802.11b possibilitou-se conexões de 11Mbps, passando por versões como 802.11g, 802.11n, até chegar ao mais recente 802.11ax (Wi-Fi 6). As principais melhorias foram no aumento da velocidade de transmissão e na eficiência em redes com muitos dispositivos conectados.

Tanenbaum (2021) também reforça a importância das redes Wi-Fi no ambiente corporativo, pois permitem que funcionários, dispositivos e sistemas estejam sempre conectados, facilitando a colaboração e a comunicação, mesmo em locais de trabalho que são mais dispersos para uso de redes cabeadas.

2.3 Protocolos de segurança em redes Wi-Fi

Os protocolos de segurança Wi-Fi são essenciais para proteger as redes sem fio e garantir a confidencialidade, integridade e autenticidade dos dados transmitidos. Os principais protocolos são: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA-PSK (Pre-Shared Key). WPA2, WPA3 e, de acordo com Keller & Thomason (2021), a evolução dos protocolos de segurança Wi-Fi reflete a crescente necessidade de proteção em um mundo conectado. Enquanto o WEP era insuficiente para garantir a segurança, os protocolos mais

recentes, como WPA3, buscam fornecer defesas robustas contra um panorama de ameaças em constante evolução. A escolha do protocolo certo para uma rede Wi-Fi é crucial para garantir a segurança e a proteção dos dados.

2.4 Metodologia de *Pentest*

A metodologia de *pentest* utilizada neste trabalho é baseada na abordagem apresentada por Daniel Moreno em seu livro “*Pentest em redes sem fio (2018)*”, com a inclusão da etapa de Avaliação. As etapas utilizadas são: Planejamento, Descoberta, Avaliação, Exploração e Relatório, que serão detalhadas posteriormente.

Figura 2: Metodologia de *Pentest*



Fonte: O autor (2024).

De acordo com a figura 2, as metodologias de *Pentest* em redes Wi-Fi seguem um fluxo estruturado, que inclui etapas como planejamento, descoberta, avaliação, exploração e geração de relatórios. No planejamento é definido o escopo do teste e autorizada a pesquisa mediante um termo de aceite. A

descoberta envolve identificar redes, topologias e níveis de criptografia. A avaliação é uma etapa incluída especificamente para esta pesquisa, de forma autônoma, pois não é mencionada nos escopos de *Pentests* dos autores, no entanto foi necessária, pois define um panorama inicial da segurança digital nas empresas aplicadas. Após isso, a exploração busca comprovar a existência de vulnerabilidades, utilizando técnicas como ataques de força bruta e de desautenticação, visando validar o risco real para a rede. Por fim, os resultados são documentados para recomendações de mitigação.

Na abordagem de Moreno(2018) o *pentest* em redes Wi-Fi é uma prática essencial para identificar vulnerabilidades em redes sem fio e melhorar sua segurança. Por meio de ferramentas e técnicas específicas, o objetivo é simular ataques que possam explorar fraquezas em pontos de acesso, configurações de rede, protocolos de criptografia e dispositivos conectados. Durante o teste, são investigados diversos aspectos, como a força da criptografia (WEP, WPA, WPA2, WPA3), o isolamento entre clientes, a presença de redes ocultas e o uso de métodos de autenticação adequados. Essas práticas permitem que administradores de rede corrijam falhas antes que sejam exploradas por agentes mal-intencionados, garantindo maior proteção aos dados transmitidos nas redes sem fio.

2.5 Principais Ataques nas Redes Wi-Fi

Os ataques contra redes Wi-Fi, descritos por Moreno (2018), exploram diversas vulnerabilidades para comprometer a segurança e capturar informações sensíveis. Um exemplo é o ataque de desautenticação, que força a desconexão de clientes ao enviar requisições falsas, facilitando a captura de handshakes e a exploração de credenciais. Ainda, segundo Moreno (2018), os ataques de força bruta utilizam listas de senhas pré definidas, conhecidas como "wordlists", para realizar inúmeras tentativas de quebra de credenciais. O autor também menciona os ataques

"Man-in-the-Middle" (MitM), em que um invasor pode interceptar ou manipular comunicações entre dois dispositivos, especialmente em redes sem criptografia robusta. Por fim, Moreno descreve os ataques "Evil Twin", nos quais pontos de acesso falsos são configurados com nomes semelhantes aos de redes legítimas, enganando usuários e permitindo o monitoramento ou a manipulação do tráfego de dados.

3 Procedimentos Metodológicos

Este trabalho pode ser classificado como pesquisa aplicada, motivada pela necessidade de resolver problemas concretos e imediatos, com finalidade prática (Gil, 1999; Cervo; Bervian, 2002; Vergara, 2005). O foco da pesquisa é a análise de vulnerabilidades em redes Wi-Fi, visando garantir as configurações mínimas necessárias, com soluções práticas e eficientes que atendam às necessidades específicas dos comércios locais. Dessa forma, contribui para a proteção de dados e o aprimoramento da segurança digital nessas organizações.

No município de Araranguá existem atualmente cerca de 3.041 empresas cadastradas, conforme informações do sistema IPM da prefeitura. Entre os 17.600 trabalhadores empregados no município, aproximadamente 4.300 estão no setor varejista, com forte presença em pequenos comércios do ramo alimentício e supermercados (CAGED, 2022).

Para a realização desta pesquisa, entramos em contato com 15 empresas das cidades de Araranguá, via Whatsapp, obtendo-se retorno de 5 empresas. Após explicação dos objetivos e de como seriam realizados os testes, fomos autorizados a prosseguir por 3 empresas da cidade de Araranguá do setor de Varejo Alimentício. A escolha dos estabelecimentos para o escopo dos testes levou em consideração a logística para sua execução e principalmente a disponibilidade em participar.

3.1 Ambiente de teste

Para o ambiente de testes foram utilizados os seguintes equipamentos:

1. Notebook Acer Aspire 5, com processador Intel Core i5 de 12th Geração, com 8GB de RAM e 500 GB de SSD.

Constitui a base de operações do ambiente de testes. Essa configuração assegura desempenho adequado para o processamento de múltiplas ferramentas simultaneamente.

2. Adaptador Wireless USB Intelbras WBN 241, suportando os Padrões IEEE 802.11b/g/n, com velocidade de até 150 Mbps.

Utilizado principalmente na atuação como NAT no ataque *Evil Twin* e geração de quadros no ataque de desautenticação.

3. Sistema Operacional Kali Linux versão 2024.3 nativamente

Sistema operacional com ferramentas já instaladas e pré-configuradas para testes de segurança.

4. Suite Aircrack-ng

Principal ferramenta utilizada, essencial em praticamente todas as etapas do *pentest*. Empregada para varredura e captura de pacotes, identificação de redes e execução de todos os ataques abordados neste trabalho.

5.NMAP

Ferramenta utilizada na etapa de descoberta para identificar dispositivos na rede, além dos serviços em execução e suas respectivas versões.

6. OpenVAS

Usado na última etapa da exploração, para varredura de vulnerabilidades expostas publicamente dos equipamentos identificados na rede.

3.2 Etapas da Pesquisa

Para a realização desta pesquisa elaboramos um fluxo de trabalho, conforme a figura 4, onde definimos as etapas a serem realizadas.

Figura 4: Fluxograma da metodologia aplicada.



Fonte: Adaptado de Rodrigues (2007).

Na etapa para definição de aquisição dos dados é definida as métricas necessárias para aplicação dos testes. Bem como a cidade de Araranguá devido a logística, o setor varejista alimentício, ao destaque regional do setor e os materiais necessários para aplicação dos testes, conforme já mencionado anteriormente.

Para a coleta de dados, iniciou-se o processo de *Pentest*. O planejamento, através do contato com o responsável pela empresa, realizado via WhatsApp e/ou e-mail, para solicitar a autorização formal para os testes de segurança. A assinatura do termo de aceite, no qual foram detalhados os procedimentos da atividade, os equipamentos e setores autorizados, bem como a

data e o horário para sua realização. A descoberta na rede, através de varreduras de equipamentos e serviços utilizando o NMAP, seguida da exploração dos ataques utilizando a ferramenta AIRCRACK-NG.

A Tabulação dos dados definiu a organização destes obtidos em tabelas, que serão abordados posteriormente. Na análise inicial, foram realizadas perguntas relacionadas a políticas e normas de segurança, incluindo práticas como segmentação de rede, existência de redes autenticadas para clientes, entre outros aspectos da segurança digital da empresa. Também, o resultado obtido na etapa dos testes práticos, onde foram realizados os ataques de força bruta, desautenticação, Man-in-the-Middle (MitM) e Evil Twin, conforme necessário em cada uma das empresas que autorizou os testes. Assim como os resultados obtidos através do OpenVAS para avaliar vulnerabilidades nos equipamentos das empresas.

Na etapa de análise dos resultados, foram destacadas as falhas encontradas e classificados seus níveis de criticidade, especialmente as apontadas pelo OpenVAS. Por fim, foi elaborado e entregue um relatório básico contendo recomendações de melhorias, como atualização ou inclusão de equipamentos, além de boas práticas de configuração, como uso de VLANs e segmentação de rede.

4 Resultados obtidos

4.1 Análise inicial

Na análise inicial foram identificadas as políticas e preocupações do cliente com a sua segurança digital, conforme pode ser visto na tabela 1. A avaliação e resultados da análise são baseados no Framework The NIST Cybersecurity Framework (CSF) 2.0.

Tabela 1: Análise inicial das empresas.

Requisitos	Respostas		
	<i>Empresa 1</i>	<i>Empresa 2</i>	<i>Empresa 3</i>
TI Fixo	Não	Apenas para manutenção	Não
HotSpot para Clientes	Não	Não	Não
Segmentação Interna (VLan)	Não	Mal aplicada	Não
Equipamentos próprios	Não	Sim	Não
Servidor Interno	Sim	Sim	Sim
Firewall	Não	Sim	Não
Backups Recentes	Não	Sim	Sim
Criptografia WPA2+	Sim	Sim	Sim
Geral	Segurança inexistente	Segurança média	Segurança mínima

Fonte: O autor (2024).

A Empresa 1 apresentou uma rede extremamente vulnerável, sem segmentação entre dispositivos internos e clientes, expondo todos os sistemas a acessos indevidos. O

servidor desatualizado e as câmeras encontravam-se na mesma rede, sem proteção através de firewall ou controle e acesso adequado. Além disso, não existia um responsável fixo pela manutenção, e o equipamento utilizado era pertencente ao provedor de internet, impossibilitando que fossem aplicadas melhorias de segurança de maneira mais eficiente.

Na Empresa 2 foram verificadas algumas medidas de segurança, como equipamentos próprios, firewall na rede, backups diários, políticas de segmentação e um responsável pelo suporte, embora não fixo na empresa. No entanto, essas medidas foram implementadas de forma incorreta, como pôde ser observado, a separação entre a rede dos clientes (2.4 GHz) e a dos caixas (5 GHz) era realizada através da frequência do WiFi. Não existia um Access Point dedicado exclusivamente para clientes, o que poderia permitir acesso indevido aos servidores por meio da rede dos caixas. Essa vulnerabilidade, entretanto, não pôde ser testada na prática devido à falta de compatibilidade do nosso equipamento utilizado com a rede Wi-Fi 5 GHz.

Já na Empresa 3, pode-se constatar que apresentava segurança mínima em sua rede, pois não era utilizada uma rede dedicada para os clientes. Embora possuíssem equipamentos próprios, esses eram compartilhados com outros moradores que compartilham o mesmo link de internet, o que configurava uma brecha de segurança grave. A parte da rede utilizada no comércio utilizava equipamento pertencente ao provedor de internet, restringindo a aplicação de políticas de segurança adequadas. Foi identificado um servidor na rede interna, na qual os clientes têm acesso, mas com regras de segurança configuradas que impediram o acesso durante os testes.

4.2 Ataques realizados

Nesta etapa, foram realizados os ataques práticos mencionados anteriormente, incluindo desautenticação, força bruta, Man-in-the-Middle e Evil Twin. Esses testes tinham como objetivo

identificar vulnerabilidades na rede e avaliar a eficácia das medidas de segurança implementadas, conforme mencionadas na tabela 2.

Tabela 2: Ataques realizados.

Ataque	Empresa 1		Empresa 2		Empresa 3	
	Realizado	Sucesso	Realizado	Sucesso	Realizado	Sucesso
	Não	—	Não	—	Não	—
Desautenticação	Sim	Sim	Sim	Sim	Sim	Sim
<i>Man in the Middle</i>	Sim	Não	Sim	Sim	Sim	Não
<i>Evil Twin</i>	Sim	Sim	Sim	Sim	Sim	Sim

Fonte: O autor (2024).

O ataque de brute force não foi aplicado em nenhuma empresa, pois a senha da rede Wi-Fi interna dos equipamentos testados e autorizados é compartilhada com os clientes, tornando-o desnecessário.

A técnica Man-in-the-Middle foi barrada tanto na Empresa 1 quanto na Empresa 3, devido ao uso de equipamentos de comodato e atualizados, que possuem restrições capazes de bloquear esse tipo de ataque. Na Empresa 2, entretanto, o ataque foi bem-sucedido, já que o equipamento utilizado estava desatualizado e vulnerável.

Já o ataque de desautenticação foi bem-sucedido em todas as empresas avaliadas. Essa vulnerabilidade está associada ao protocolo WPA2, que permite a desconexão forçada de dispositivos da rede, corrigida apenas com a adoção do WPA3.

Assim como o ataque de desautenticação, o Evil Twin foi bem-sucedido em todas as empresas, pois sua eficácia

depende da vítima se conectar à rede falsa criada pelo atacante. A utilização do ataque de desautenticação foi determinante para forçar os dispositivos a se reconectarem na rede falsa.

4.3 OpenVAS

O OpenVAS é utilizado nesta etapa para identificar falhas nos dispositivos da rede por meio de conexões e varreduras automatizadas, conforme a tabela 3.

Tabela 3: Varredura OpenVAS

Falhas	Quantidade		
	<i>Empresa 1</i>	<i>Empresa 2</i>	<i>Empresa 3</i>
Falha leve	2	-	3
Falha média	-	-	1
Falha grave	2	-	-

Fonte: O autor (2024).

Foram identificadas falhas leves nas empresas 1 e 3, como ICMP habilitado, que não compromete o funcionamento da rede. Na empresa 3, houve uma falha média que permite desconexão da rede via DoS no access point. Já na empresa 1, foram encontradas falhas graves no servidor devido à versão extremamente desatualizada, possibilitando execução remota de comandos e instalação de backdoors para acesso futuro. Na empresa 2, o OpenVAS não conseguiu acessar os dispositivos da rede devido ao firewall configurado.

4.4 Conclusão dos testes

As políticas de segurança analisadas na fase inicial

tiveram impactos significativos nos testes. Embora nenhuma das empresas avaliadas tenham sido consideradas totalmente seguras, aquelas que demonstraram preocupações mínimas com a segurança obtiveram resultados melhores.

Na empresa 1, os resultados foram críticos, especialmente na varredura do OpenVAS. Já na empresa 2, o firewall da rede impediu a execução do teste, mas um access point desatualizado permitiu um ataque Man-in-the-Middle. Por fim, na empresa 3, foi identificado um servidor na rede dos clientes, porém com regras que impossibilitaram a conexão direta. Isso reforça a necessidade de implementar configurações básicas de segurança, que, apesar de simples, são altamente eficazes na proteção da infraestrutura.

5 Considerações Finais

As considerações finais deste trabalho destacam a relevância de avaliar a segurança das redes Wi-Fi em ambientes comerciais, evidenciando vulnerabilidades comuns, como o ataque de desautenticação e a eficácia de técnicas como Evil Twin em redes mal configuradas. As análises revelaram que a falta de atualização dos dispositivos e o compartilhamento de senhas com clientes aumentam significativamente os riscos de segurança.

Este estudo reforça a importância da adoção de boas práticas, como a implementação do WPA3, o uso de firewall para filtragem de conteúdo e conexões, a segmentação de redes e, especialmente, a utilização de equipamentos dedicados exclusivamente a clientes, garantindo maior proteção dos dados e minimizando vulnerabilidades.

Embora tenha existido certa dificuldade na análise de redes Wi-Fi 5GHz devido à incompatibilidade da antena utilizada, ao final da entrega do relatório com as propostas de melhorias para a segurança das redes, constatou-se que os

objetivos do trabalho foram atingidos com sucesso. Como sugestão para pesquisas futuras, considera-se a necessidade de avaliar a implementação das correções realizadas na rede, bem como realizar uma nova análise das infraestruturas existentes.

6 Referências

- DEB SOLUTIONSTI. Conheça a ISO 27000: a família de normas que abordam a Segurança da Informação. Publicado em: 21 jul. 2015. Disponível em: <https://debsolutionsti.com/iso-27000/iso-27000/>. Acesso em: 04 out. 2024
- HOCAYEN DA SILVA, Antônio João. Metodologia de pesquisa: conceitos gerais. Unicentro, 2014.
- Keller, Sarah & Thomason, Amanda. (2021). NIST Cybersecurity Framework: A Pocket Guide.
- MORENO, Rafael. PenTest: teste de penetração em redes sem fio. 1. ed. São Paulo: Novatec, 2018.
- PREFEITURA MUNICIPAL DE ARARANGUÁ. Dados sobre empresas e setores econômicos de Araranguá. Araranguá, 2024.
- RIBEIRO, Marcell Coutinho. Wi-Fi em estabelecimentos comerciais: cuidados com a segurança jurídica. Simply As, 05 fev. 2018. Disponível em: <https://simplyas.com/modbox/pt/wi-fi-em-estabelecimentos-comerciais-cuidados-com-seguranca-juridica/>. Acesso em: 26 jan. 2025.
- SANTOS, Samuel. Desafios de segurança em redes Wi-Fi públicas: como se proteger? DT Network, 14 jun. 2024. Disponível em: <https://dtnetwork.com.br/seguranca-em-redes-wi-fi-publicas/>. Acesso em: 26 jan. 2025.
- SERAFIM, Lurian Vieira. Análise de segurança em redes wireless por meio do teste de penetração. 2020. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade do Extremo Sul Catarinense, Criciúma, 2020.

- STALLINGS, William. Computer security: principles and practice. 4. ed. Upper Saddle River: Pearson, 2017.
- TANENBAUM, Andrew S.; WETHERALL, David J. Redes de computadores. 6. ed. São Paulo: Pearson, 2021.
- WHITMAN, M. E.; MATTORD, H. J. Principles of information security. 6. ed. Cengage Learning, 2018.

Atuação Profissional dos Alunos Egressos do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal Catarinense - Campus Sombrio

Andrey Schwanck Machado¹, Victor Martins de Sousa²

¹, Acadêmico do Instituto Federal Catarinense – Campus Sombrio – 88960000 – Sombrio – SC – Brasil

^{2, 3}, Docentes do Instituto Federal Catarinense – Campus Sombrio – 88960000 – Sombrio – SC – Brasil

andreyismjvm@hotmail.com, victor.sousa@ifc.edu.br

Abstract. *This article presents the results of the research that points the current professional situation of the graduates of the Higher Education Course in Computer Networks at the Instituto Federal Catarinense - Campus Sombrio. The ongoing need of technological advancement nowadays makes it important for an institution to know the progress of its former students' professional lives in order to assess the effectiveness of the course. Through research, analysis and discussion of data obtained through a formulary containing questions about academic training, professional performance and satisfaction with the course, it was possible to gather the graduates' opinions, in order to identify possible improvements for it.*

Resumo. *Este trabalho apresenta um resultado de pesquisa que aponta a atual situação profissional dos egressos do CST em Redes de Computadores do IFC - CS. A permanente necessidade de avanço tecnológico na atualidade torna importante para uma instituição saber o andamento das vidas profissionais dos seus ex-alunos para verificar a eficácia do curso. Através de uma pesquisa, análise e discussão dos dados obtidos por meio de um formulário contendo perguntas sobre formação acadêmica, atuação profissional e satisfação com o curso, foi possível angariar as opiniões dos egressos, com objetivo de identificar possíveis melhorias para ele.*

1. Introdução

Muitas tarefas são mais simples ou até possíveis graças à tecnologia da informação, que tem evoluído cada vez mais desde que o termo surgiu em meados do século XX, quando a tecnologia começou a permitir armazenar informações em computadores e não apenas em folhas de livros, cadernos, diários e jornais.

Desde então, a tecnologia foi evoluindo e permitindo que cada vez mais dados e diferentes tipos de informações pudessem ser armazenados, como imagens, vídeos e músicas com alta qualidade tanto em nossos próprios dispositivos quanto em servidores remotos, tornando possível o acesso imediato a uma informação que não está armazenada no próprio dispositivo utilizado.

Porém, esse avanço tecnológico, além de facilitar as nossas vidas, necessita de manutenção e aprimoramentos e por isso é importante a inserção de mais profissionais na área.

Esses profissionais desenvolvem processos que auxiliam no gerenciamento e funcionamento de estruturas de redes de computadores e na segurança dos dados.

Um dos objetivos do Instituto Federal Catarinense - Campus Sombrio (IFC - Sombrio) é formar esses profissionais. Sendo assim, se faz pertinente realizar uma pesquisa para identificar e estudar o impacto do curso na carreira dessas pessoas, ou seja, os egressos, após concluírem a formação. Para isso, será desenvolvido o trabalho através de uma pesquisa exploratória, com um formulário, questionando egressos do curso de Tecnologia em Redes de Computadores do IFC – Sombrio, a fim de pesquisar suas opiniões em relação ao curso e às suas carreiras dentro da área.

Espera-se que esta pesquisa produza alguns resultados significativos, como:

- Pesquisar os atuais cargos ocupados pelos egressos que atuam na área de TI;
- Solicitar sugestões sobre possíveis melhorias para o curso;
- Compreender melhor a eficácia do curso da perspectiva de quem já passou por todo o processo de formação.

O curso de Tecnologia em Redes de Computadores do IFC, Campus Sombrio, foi criado em 2010, com o objetivo de atender à demanda por profissionais qualificados na área de redes de computadores na região de Sombrio. O curso tem duração de três anos, com carga horária total de 2.400 horas distribuídas em seis semestres letivos.

A grade curricular do curso é composta por disciplinas teóricas e práticas, como: Fundamentos da Computação e Hardware, Programação, Sistemas Operacionais, Cabeamento Estruturado, Segurança e Gerência de Redes, Redes sem Fio, Arquitetura de Computadores, Banco de aDdos, entre outras.

O curso também exige o desenvolvimento e a defesa de um trabalho de conclusão de curso (TCC), em que haja um projeto prático ou teórico na área de redes de computadores, orientado por um professor do curso.

2. Referencial Teórico

Nesta seção é apresentada a revisão bibliográfica, onde será exposto o embasamento sobre os assuntos abordados no trabalho.

2.1 Redes de Computadores

Cada um dos 3 séculos anteriores foi dominado por uma nova tecnologia e a diferença de tempo entre o comando e o resultado está desaparecendo rapidamente graças à tecnologia que dominou esse século, a internet.

Quanto mais a tecnologia avança, maior a demanda por formas mais sofisticadas de processamento de informação.

Mesmo a indústria da tecnologia sendo algo ainda recente, já mostrou um espetacular progresso em pouco período. Nas primeiras décadas de existência dos computadores, onde estes eram muito centralizados, gigantes e eram adquiridos em apenas algumas dezenas por grandes empresas e instituições, hoje em dia são menores que selos postais, e produzidos em massa.

O que antes era um único computador atendendo todas as necessidades de uma organização, tornou-se em um grande número de computadores separados, porém interconectados. Esses sistemas são chamados redes de computadores (Tanenbaum, 2011, p. 1).

As redes de computadores servem para facilitar a comunicação e as tarefas do cotidiano, pois, através de um dispositivo conectado à internet somos capazes de conversar

com qualquer pessoa que possua um dispositivo também conectado à internet, acessar sites de venda, guardar e organizar informações através de textos, imagens, vídeos, áudios, assim como ter acesso à arte, ensino e entretenimento.

2.2 Profissional de Redes

O profissional de redes de computadores é responsável por garantir o funcionamento seguro e eficiente das redes de computadores de instituições, organizações e empresas.

Ao escolher essa carreira, o profissional poderá atuar com:

- Planejamento e design de redes, desenvolvendo projetos que atendam às necessidades dos clientes.
- Instalação e configuração de dispositivos de redes como switches, roteadores, servidores e firewalls.
- Manutenção e monitoramento contínuo do desempenho das redes para identificar e resolver problemas.
- Desenvolvimento e implementação de políticas de segurança de redes, para proteger as redes contra ameaças cibernéticas.
- Treinamento e suporte aos usuários para garantir o uso adequado da rede.

Segundo o Projeto Pedagógico do Curso Superior de Tecnologia em Redes de Computadores:

“O Tecnólogo em Redes de Computadores que atua nessa área desenvolve processos para gerenciamento de estruturas de redes de computadores, primando pela segurança na troca de informações, criando

processos para garantir um bom funcionamento da infraestrutura de comunicação de dados, voz e imagens; também estará apto a iniciar o seu próprio negócio como prestador de serviços, consultor, bem como continuar seus estudos em cursos de pós-graduação ou seguirem a área de pesquisa científica, trabalhando em instituições de pesquisa ou ensino voltadas para a área de Redes de Computadores. Poderá também prestar concursos em nível superior em diversas instituições públicas e privadas na sua área de atuação ou em áreas afins” (Fernandes; Oliveira, 2023, p. 30).

2.3 Egressos

Egresso, ou graduado, é o termo utilizado para designar um ex-aluno de um curso superior após ter concluído o curso.

“O profissional egresso do CST em Redes de Computadores deve ser capaz de processar as informações, extraídas de uma massa cada vez maior de dados, aquelas que pela sua natureza, interessam às organizações e/ou à sociedade como um todo, ter desenvolvido seu senso crítico e ser capaz de impulsionar o desenvolvimento econômico da região, integrando formação técnica à cidadania” (Fernandes; Oliveira, 2023, p. 28).

Além de serem importantes para o mercado de trabalho, pois estão preparados para lidar com os desafios de suas

respectivas áreas de atuação, eles também são importantes para uma instituição de ensino por serem uma das principais formas para se averiguar sobre a qualidade de seu ensino.

As instituições de ensino têm interesse em acompanhar esses egressos, pois se eles estão bem sucedidos em suas carreiras, pode ser um indicativo de que essa instituição oferece um ensino de qualidade. Mas se o egresso não consegue uma vaga ou não consegue desempenhar bem o seu papel, pode ser que haja algo que pode ser melhorado no processo de formação dessa instituição.

2.4 Mercado de Trabalho

A área de tecnologia se faz presente na maioria das empresas, e essa área tem muito a crescer ainda, tanto no número de vagas a serem oferecidas quanto na criação de novos cargos.

Em 2023, no Brasil, o setor de TI cresceu 21% comparado a 2022, que já tinha um crescimento de 22% em relação a 2021.

Em janeiro de 2023, a rede social LinkedIn, focada em negócios e empregos, divulgou um levantamento com os 25 cargos que, no Brasil, apresentaram maior crescimento na demanda nos cinco anos anteriores e as tendências para o futuro do mercado de trabalho. Entre os dez primeiros cargos da lista “Empregos em alta em 2023”, 6 são da área de tecnologia:

- Analista de privacidade, 1^a posição;
- Especialista em cibersegurança, 2^a posição;
- Engenheiro de cibersegurança, 6^a posição;
- Engenheiro de dados, 8^a posição;
- Analista de desenvolvimento de sistemas, 9^a posição;

- Pesquisador de UX (experiência do usuário), 10^a posição.

Uma pesquisa trimestral feita pela Advance Consulting mostrou que a área de TI fechou o 2º trimestre de 2024 com 22% de crescimento. O relatório também mostra que a falta de mão de obra qualificada continua sendo um problema na área.

4. Metodologia

O trabalho foi desenvolvido com um estudo de caso que passa pelas seguintes etapas, mostradas na Figura 1:



Figura 1 - Etapas da Pesquisa

O estudo de caso é uma forma de pesquisa científica que estuda o contexto de um assunto e suas variáveis com o objetivo de explicar, explorar ou descrever. O estudo de caso se caracteriza por ser um estudo detalhado e exaustivo de poucos ou apenas um objeto, e fornece conhecimentos profundos (Eisenhardt, 1989; Yin, 2009 apud Branski et al. 2010).

A primeira etapa foi uma revisão bibliográfica, em que foram pesquisados trabalhos relacionados para aprofundamento no universo estudado, no referencial teórico e para a execução de formulários.

O formulário enviado foi testado anteriormente com alguns egressos, para avaliar a eficiência dele. O formulário final foi enviado sem alterações em relação ao teste.

Este formulário de teste foi enviado para 4 egressos no dia 02/04/2024 e as respostas foram recebidas no mesmo dia. O formulário final foi enviado no dia 26/08/2024 com objetivo de obter respostas até o dia 08/09/2024. Com o objetivo de ampliar o número de respondentes, o prazo foi ampliado até 21/09/2024 visando maior adesão, totalizando assim, 35 respostas.

Na terceira etapa, foi realizada a análise dos dados coletados no formulário, que foram comparados através de gráficos.

Na quarta e última etapa, foi realizada uma discussão sobre a comparação realizada na etapa anterior.

Para Malhotra (2019), as características de um formulário são um conjunto de perguntas feitas com o intuito de obter informações dos entrevistados, contendo perguntas simples de serem respondidas para que o entrevistado responda o formulário inteiro, mantendo-se envolvido, reduzindo erros em suas respostas.

Este trabalho teve como base, um outro trabalho intitulado como “Atuação Profissional dos Alunos Egressos do

Curso Tecnologia em Redes de Computadores do Instituto Federal Catarinense, Câmpus Sombrio” desenvolvido no IFC em 2018. Este outro trabalho conseguiu captar 25 respostas de alunos formados no curso entre 2010 e 2016 (Marques; Beteli, 2018).

Portanto, este trabalho já possui um direcionamento desde o início e com isso foi possível adquirir 35 respostas de alunos formados até 2023.

A partir dos dados coletados, foi possível traçar um panorama geral sobre o perfil e a trajetória dos egressos do curso de Tecnologia em Redes de Computadores da IFC, Campus Sombrio, identificar os pontos fortes e aspectos a serem aprimorados no curso, as oportunidades e as dificuldades encontradas pelos egressos após sua conclusão.

4. Resultados e Discussões

Neste capítulo são apresentados os resultados e discussões acerca dos dados coletados no formulário, a fim de encontrar possíveis melhorias para o Curso Superior de Tecnologia em Redes de Computadores e a formação de seus acadêmicos.

4.1 Resultados do Formulário

O formulário está dividido em 3 segmentos, e dependendo do que o egresso respondeu na 7^a pergunta, este foi enviado para uma seção diferente do formulário. Todos os egressos responderam à primeira e à última seção do formulário. Dada essa informação, vamos começar a análise dos dados do formulário pela primeira seção.

4.1.1 Primeira seção do formulário

Em relação ao gênero, a maioria dos pesquisados são do gênero masculino (85,7%), no total de 30, e o gênero feminino (14,3%) corresponde a um total de 5 respondentes.

A Figura 2 mostra o gráfico relativo à cidade que os egressos respondentes residem atualmente. A cidade mais citada é Sombrio, representando 6 alunos egressos, correspondente a 17,1%. Em seguida temos 3 cidades dividindo a mesma porcentagem de 11,4%, correspondentes a 4 alunos: Araranguá, Balneário Gaivota e Torres. Logo em seguida, como terceira mais votada temos São Paulo com 3 alunos representando 8,6%. Com 2 alunos representando 5,7% temos Porto Alegre e Santa Rosa do Sul. Além dessas, as outras localidades citadas, com 1 aluno, são: Criciúma, Santa Cruz do Sul, Caxias do Sul, Içara, Gravataí, Ibirama, Praia Grande, Mampituba, Palmas (Paraná) e Itália.

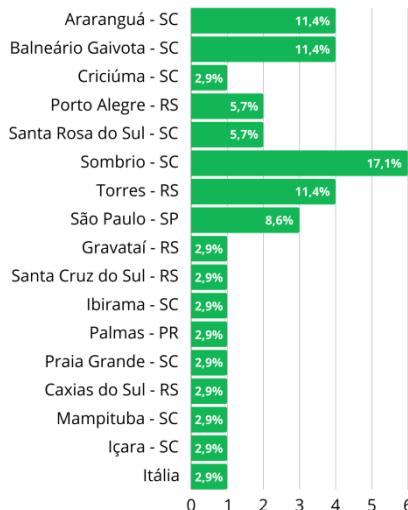


Figura 2 - Cidade em que reside atualmente

A Figura 3 mostra o gráfico relativo à cidade de residência antecedente à formação dos alunos egressos respondentes, onde novamente a alternativa mais citada por eles

foi Sombrio com 22,9 % dos alunos egressos respondentes, representando 8 respostas. A segunda cidade é Torres com 5 alunos, correspondendo a 14,3% . Na terceira posição, com 3 pessoas correspondendo a 8,6% dos alunos, temos Araranguá e São Paulo. Com 5,7% representando 2 pessoas, estão as cidades de Criciúma, São João do Sul, Santa Rosa do Sul e Porto Alegre. E finalizando, com apenas 1 pessoa sendo representado por 2,9%, temos Balneário Gaivota, Goiânia, Gravataí, Jacinto Machado, Mampituba, Passo de Torres, Praia Grande e Vacaria.

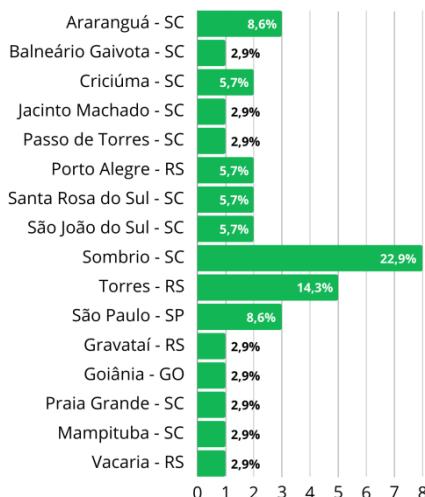


Figura 3 - Cidade de origem antes de concluir a graduação

O conhecimento adquirido pelos egressos antes de ingressar na faculdade é representado na Figura 4. Dezessete egressos, representando 48,6%, responderam com a alternativa “Sim, porém apenas conhecimentos básicos”. Outros 16 egressos, 45,7% dos votos, responderam com a alternativa “Sim, me matriculei para melhorar currículo ou expandir conhecimento”. Apenas 2 alunos, representando 5,7% dos egressos, responderam que não possuíam conhecimento antes de ingressar no curso de Redes de Computadores.



Figura 4 - Já possuía conhecimento na área de Tecnologia da Informação antes de ingressar na faculdade?

A Figura 5 apresenta os resultados da pergunta que questionava os ex-alunos sobre o preparo para o mercado de trabalho quando terminaram a faculdade. A maioria respondeu que estava razoavelmente preparada, representando 23 pessoas ou 65,7% dos egressos. Cinco egressos disseram estar muito preparados para o mercado de trabalho quando saíram da faculdade, representando 14,3% deles. Quatro egressos disseram estar pouco preparados, representando 11,4% deles. E finalmente 3 egressos responderam que não estavam preparados para o mercado de trabalho ao se formarem, 8,6%.

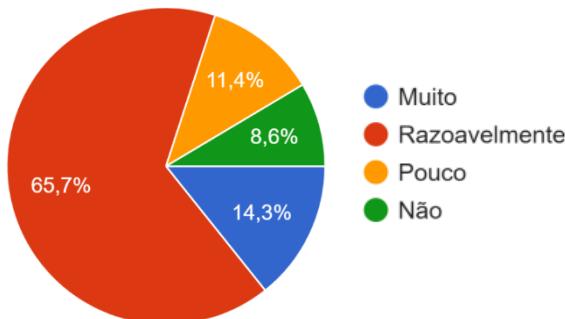


Figura 5 - Você estava preparado para o mercado de trabalho quando se formou?

Os resultados da 7^a pergunta, referente à atuação profissional dos egressos no momento em que a responderam são mostrados na Figura 6. A maioria dos egressos respondeu que está atuando na área de tecnologia da informação, com 57,1%, representando 20 pessoas. Doze pessoas, 34,3%, responderam que estão trabalhando fora da área de sua formação. Apenas 8,6%, 3 pessoas, responderam que não estão trabalhando no momento.

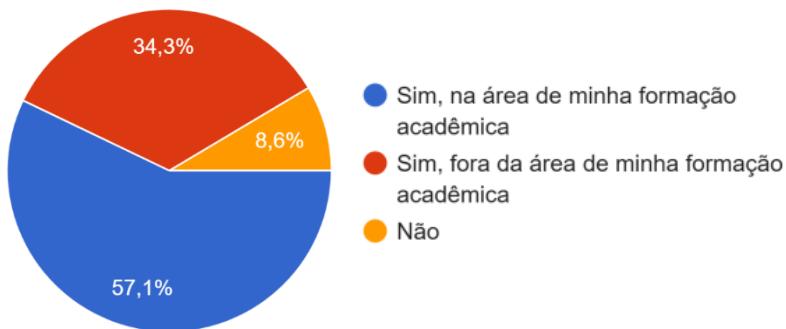


Figura 6 - Atualmente você está exercendo atividade profissional?

A 7^a pergunta divide o formulário em 3 segmentos, pois cada resposta leva o respondente a uma seção diferente do formulário. Cada seção possui perguntas referentes à alternativa escolhida na 7^a pergunta. Todos os egressos responderam à primeira e à última seção do formulário. A Figura 7 ilustra essa divisão com um fluxograma.



Figura 7 - Fluxograma Compacto do Formulário

Dada essa informação, vamos continuar a análise dos dados pela seção chamada “Você atua na área”.

4.1.2 Atuantes da Área de TI

A Figura 8 apresenta o gráfico referente à pergunta relacionada ao cargo ocupado pelo egresso. Dentre as 20 pessoas que entraram nessa seção, 5 respondentes, representando 25%, são correspondentes à alternativa “Suporte Técnico”. Em segundo lugar, 3 pessoas, 15%, disseram ocupar o cargo de Analista de Tecnologia da Informação. Em terceiro lugar, dividindo a mesma porcentagem de 10% e 2 pessoas, estão as alternativas “Administrador de Redes”, “Analista de Redes” e “Técnico em Informática”. Obtiveram apenas 1, representando 5% deles, as alternativas “Analista de Implantação”, “Analista de Segurança da Informação”, “Arquitetura de Redes”, “Consultor de TI”,

“Desenvolvedor Web” e “Laboratório de Tecnologias Educacionais (Escola do Estado de SC)”.

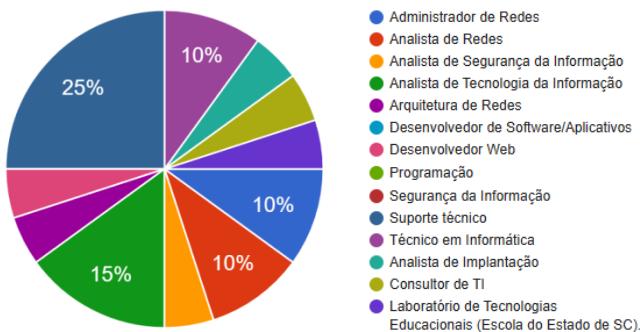


Figura 8 - Você atua em qual sub-área/cargo?

A pergunta seguinte questiona quanto tempo houve entre a formatura e o início da atividade profissional. Seus resultados são mostrados na Figura 9. A maioria, formada por 9 pessoas (45% dos resultados), já estava trabalhando antes de sua formação. Outros 7 egressos (35% dos votos) começaram a atuar na área em menos de 1 ano. Dividindo a mesma percentagem e montante e 1 voto, encontram-se as alternativas “Aproximadamente 1 ano”, “Aproximadamente 3 anos”, “Aproximadamente 4 anos” e “Mais de 4 anos”. Nenhum egresso respondeu “Aproximadamente 2 anos”.

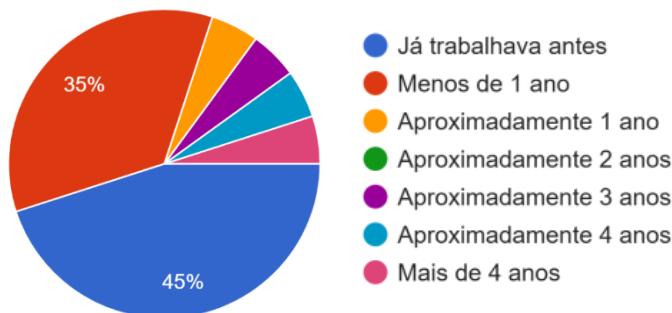


Figura 9 - Quanto tempo houve entre a formatura e o início de sua atividade profissional?

A Figura 10 refere-se aos resultados da pergunta que questiona em que tipo de organização o egresso está exercendo sua atividade profissional. A maioria, composta por 10 egressos, 50% deles, afirmou atuar em uma empresa privada. Outros 30%, compostos por 6, atuam em empresas públicas. Três destes, 15%, afirmam trabalhar em uma empresa própria. Apenas um egresso (5%) trabalha de forma autônoma.

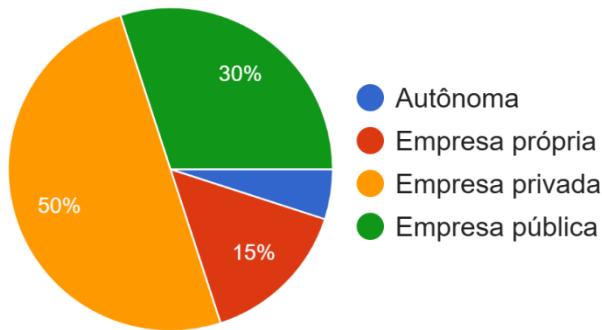


Figura 10 - Em que tipo de organização você exerce sua atividade profissional?

A Figura 11 apresenta os resultados da pergunta “Em sua visão, qual é a perspectiva profissional na sua área?” onde 12

egressos (60%), a maioria, apontaram a alternativa “Boa”, mas 6 egressos (30%) declararam “Ótima”. Apenas 2 egressos concordam que suas perspectivas em relação à área são razoáveis. Ninguém apontou “Desanimadora” ou “Não tenho condições de avaliar”.



Figura 11 - Em sua visão, qual é a perspectiva profissional na sua área?

Os dados apresentados na Figura 12 mostram os motivos de dificuldade que os egressos tiveram na contratação e/ou execução da profissão no mercado de trabalho. A maioria, composta por 8 pessoas, 40% dos respondentes, afirmou ter dificuldades por falta de experiência. Em seguida, 7 pessoas, 35% deles, disseram não ter passado dificuldades. Três pessoas, 15%, afirmaram ter dificuldades devido à falta de domínio de uma língua estrangeira. E 2 respondentes, correspondendo a 10%, disseram ter dificuldades relacionadas à forte concorrência para obter emprego.



Figura 12 - Teve dificuldades na contratação e/ou execução da profissão no mercado de trabalho?

A próxima pergunta questiona o egresso se o seu aprendizado na faculdade contribuiu para o seu desempenho profissional na área de tecnologia da informação. Seus dados são apresentados na Figura 13. A grande maioria respondeu que ajudou muito, com 70% dos respondentes, representando 14 pessoas. Apenas 25% deles, representando 5 pessoas, responderam que seus estudos contribuíram razoavelmente para a sua atuação profissional na área. Apenas 1 egresso disse que o curso contribuiu apenas um pouco para a sua atuação. Nenhum egresso disse que o curso não contribuiu para a sua atuação profissional na área.

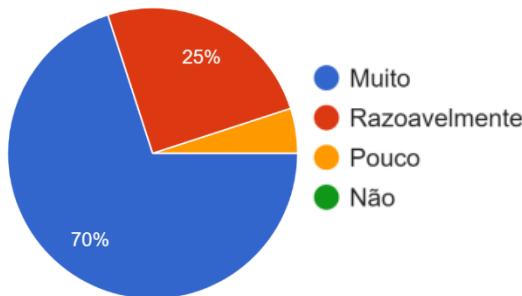


Figura 13 - A Formação Acadêmica contribuiu para o seu desempenho profissional na área de Tecnologia da Informação?

4.1.3 Não Atuantes da Área de TI

Esta seção corresponde à seção “Você não atua na área” conta com 12 respondentes.

A Figura 14 apresenta os resultados da questão “O principal motivo pelo qual você não exerce atividade profissional na sua área de formação é...” Desses 12 egressos, a metade, composta por 6 respondentes, disse que não atua na área por motivos particulares. Outros 5 respondentes, correspondentes a 41,7%, disseram que não atuam na área por encontrarem melhores oportunidades em outras áreas. E 1 pessoa (8,3%) disse não trabalhar na área por considerar o mercado de trabalho saturado.

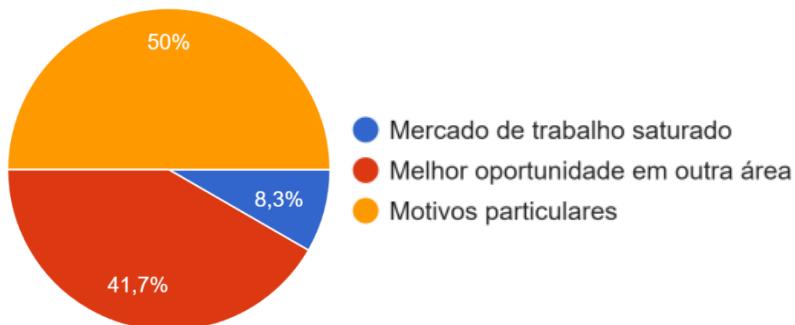


Figura 14 - O principal motivo pelo qual você não exerce atividade profissional na sua área de formação é:

A próxima pergunta questiona o egresso se a sua formação acadêmica o ajudou em seu desempenho profissional na sua área de atuação. A maioria, composta por 8 egressos, correspondendo a 66,7%, disse que sua formação acadêmica ajudou muito. Três egressos, 25%, disseram que a formação contribuiu razoavelmente. E 1 egresso, 8,3%, disse que ajudou pouco. Não houve respostas afirmando que seus aprendizados não serviram.

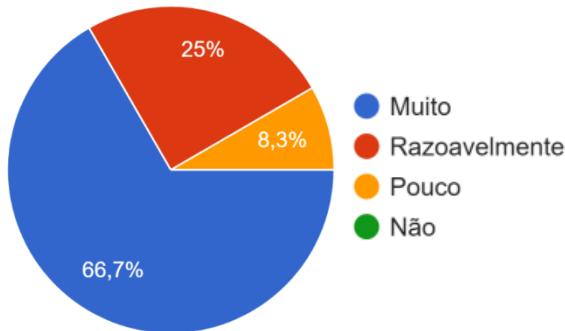


Figura 15 - A formação acadêmica contribuiu para o seu desempenho profissional na sua área?

4.1.4 Inativos Profissionalmente

Agora a análise será feita sobre a seção “Você não está exercendo atividade profissional atualmente” que contém apenas 1 resposta, de 3 egressos que passaram por essa seção, que possui apenas uma pergunta objetiva e opcional. Ao ser perguntado se gostaria de compartilhar com o IFC o porquê não atuar profissionalmente no momento, o egresso afirmou estar “trabalhando em dois projetos pessoais”.

4.1.5 Seção Final do Formulário

Essa é a seção final do formulário onde todos os egressos responderam, assim como a primeira, portanto, são analisadas as respostas de 35 respondentes.

A primeira pergunta desta seção é referente ao contato que os ex-alunos mantiveram com o IFC após a sua formação. Dos 35 respondentes, 19 deles, 54,3%, disseram não ter mantido mais contato com o IFC. Outros 13 egressos, 37,1%, disseram ter mantido contato com o IFC apenas em busca de informações em geral. Dividindo o mesmo montante de 1 voto e o mesmo percentual de 2,9%, estão as alternativas “Curso de atualização”,

“Participação de eventos” e “Procura dos serviços prestados pelo instituto”.



Figura 16 - Você tem mantido algum contato com o IFC - Campus Sombrio?

A próxima pergunta questiona os egressos sobre as suas opiniões em relação ao curso, ou seja, qual característica que a ele atribuem, sendo elas “Ótimo”, “Bom”, “Regular”, “Ruim” e “Péssimo”. Quase metade deles, 48,6%, representando 17 respondentes, disseram considerar o curso bom. Quarenta por cento dos respondentes desta questão, 14 egressos, disseram considerar o curso ótimo. Quatro egressos, representando 11,4% dos votos, disseram considerar o curso regular. Ninguém considerou o curso ruim ou péssimo.

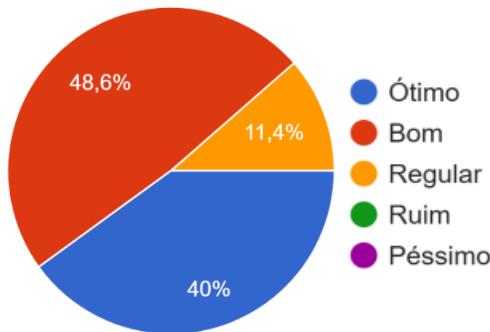


Figura 17 - Qual é o conceito que você atribui ao curso que concluiu?

A última pergunta é objetiva e oferece um espaço para os egressos sugerirem melhorias para o curso. Treze egressos não sugeriram melhorias e/ou já o consideram muito bom, porém um deles afirmou que o problema está nas “empresas que não pagam um salário justo”, além de “pouco incentivo para crescer na empresa”. Outro disse que “a experiência que costuma ser solicitada pelos recrutadores ocorre em diversas áreas, não somente na nossa, portanto, é algo que o curso não pode mudar”.

Considerando que a última pergunta é objetiva, na tabela a seguir, a análise será feita individualmente sobre cada comentário dos egressos, em ordem de resposta e desconsiderando os que não sugeriram melhorias.

Tabela 1. Sugestões dos alunos egressos

<p>Este comentário disse que ao invés de investir em um curso voltado para tecnólogo de redes, “investiria em uma engenharia de redes”.</p>
<p>Um egresso disse que entende as dificuldades, mas que pelo menos durante o seu tempo no curso, os professores deveriam exigir mais dos alunos.</p>

Este egresso disse que seria ideal no primeiro semestre, filtrar de quem está começando e de quem já tem conhecimento na área, para tentar igualar o ensino para todos.

Outro egresso sugeriu o uso de inteligências artificiais, diferenciando esses egressos no mercado de trabalho.

Este comentário diz que o curso foca no ensino de administração/gerenciamento de redes, porém a região possui vagas escassas e com pouca remuneração e diz ser mais plausível procurar cidades polos para exercer a profissão. Também sugeriu dar ênfase na parte de programação com linguagens como C# e Java, desenvolvimento web com FrameWorks como Angular, React e VUE, além do uso do banco de dados MySQL, já ensinado no curso, porém, integrado com os FrameWorks Spring Boot e Hibernate.

Neste comentário o egresso sugere ensinar mais sobre aplicação de conceitos em ambientes com equipamentos de diferentes fabricantes, dar mais destaque às topologias de provedores ISP, demonstrando as funções de seus serviços e equipamentos.

Um comentário sugere que o IFC desenvolva parcerias com prestadores de serviços locais, com um conceito mais “mão na massa”, ajudando assim tanto as parcerias quanto os alunos, simulando a experiência de trabalhar com redes.

Outro egresso sugere estudos de outras marcas de dispositivos de redes, pois aprendeu apenas sobre uma marca.

Neste comentário o egresso sugere maior contato com as empresas que oferecem serviços de comunicação, como

provedores, data centers, órgãos de regulamentação entre outros.

Outro comentário sugere a realização de mais eventos sobre tecnologia no campus.

Um egresso sugere uma aproximação menos abrangente e mais focada no que de fato será utilizado/necessário quando se trata de Redes de Computadores.

Outro egresso menciona a total dedicação de cada acadêmico ao aprendizado em tecnologia, “conceito que faz parte fundamental em nossas vidas, indiferente de quem quer que seja”.

Um comentário sugere ao IFC a inclusão de outros cursos e de mestrado.

Outro comentário sugere um foco na entrega de curso preparatório para certificação em paralelo ao currículo, sugere também um oferecimento de oportunidades de estudo em plataformas de aprendizado de grandes fabricantes e prestadores de serviço da área de redes.

Outro egresso disse que sentiu falta de mais aulas práticas, como em ambientes reais e laboratórios bem equipados.

Este comentário também menciona que sentiu falta de aulas práticas e que a teoria, embora importante, é facilmente encontrada na internet.

Outro egresso acredita que o IFC tenha um plano de ensino bem completo, porém teve duas dificuldades: (1) não teve muitos trabalhos escritos para contribuir na experiência para a produção do TCC e (2) a pesquisa para a instalação e integração de múltiplos serviços era por conta dos próprios alunos que não tinham boas referências e certos serviços continham apenas conteúdos de 10 a 15 anos.

O último comentário desta pesquisa sugere a diminuição de disciplinas obrigatórias, para que sejam oferecidas como cursos de extensão, abrindo espaço para as que necessitam de maior conhecimento técnico e aulas práticas.

4.2. Discussão

Os resultados indicam que a grande maioria dos respondentes é do gênero masculino. A maioria dos pesquisados já possuía conhecimento prévio na área e alguns já trabalhavam nela.

Os egressos vieram de várias regiões diferentes, a maioria é de Santa Catarina. Alguns vieram de outros estados como o Rio Grande do Sul e São Paulo. Após a formação, alguns encontram oportunidades em outros lugares, como o Paraná e até Itália. Ao todo 11 pessoas se mudaram após concluir o curso.

A maioria disse possuir conhecimentos razoáveis para o mercado de trabalho após concluir o curso e alguns estavam muito preparados. Isso pode estar relacionado à necessidade de aumento de aulas práticas ou pode simplesmente significar que algumas empresas exigem mais do que outras para a contratação.

A maioria dos egressos atua na área, o que indica que o curso possui uma boa matriz curricular e abrange os principais conhecimentos necessários para o mercado de trabalho.

Egressos que atuam fora da área disseram que sua formação acadêmica contribuiu para suas atividades profissionais.

Os principais cargos exercidos pelos pesquisados são: suporte técnico, técnico em informática, arquitetura de redes, analistas, consultores e administradores de TI e redes, além da área de segurança e desenvolvimento web. Isso evidencia que o campo oferece uma vasta gama de opções para atuação.

Pouco menos da metade obteve êxito em sua atividade profissional em menos de 1 ano após a formação.

Metade dos respondentes trabalha em empresa privada, os demais atuam em empresa pública, ou própria ou trabalho autônomo. Apesar de haver uma reclamação sobre o salário pago por empresas locais, a atuação em empresas privadas e públicas ainda são as opções mais comuns, por oferecerem mais segurança financeira e menos trâmites necessários para contribuir na área.

Mais da metade dos egressos atuantes da área a consideram boa para atuação e alguns egressos a consideram ótima.

Apesar da falta de experiência ter sido a principal dificuldade encontrada pelos egressos na contratação e/ou atuação, a maioria afirmou que sua formação acadêmica contribuiu muito no mercado de trabalho.

Alguns egressos encontraram melhor oportunidade em outra área, outro egresso disse considerar o mercado saturado, mas considerou o curso ótimo e afirmou que ele contribuiu muito na sua atuação profissional fora da área.

A percepção dos respondentes em relação ao curso é positiva, pois a maioria o considerou ótimo ou bom. Poucos consideraram o curso regular.

Dentre as principais sugestões dos egressos estão o aumento de aulas práticas, variação de marcas de equipamentos que são ensinados no curso, ensino do uso de inteligências artificiais, ensino focado no que principalmente será utilizado no exercício profissional, parcerias com empresas locais, maior exigência e amparo dos alunos por parte dos professores, dando atenção a quem entende menos do assunto e exigindo mais dos alunos. Houve uma recomendação de linguagens de programação e softwares específicos para o ensino no curso.

5. Considerações Finais

A realização desta pesquisa utilizando o método de formulário buscou atender aos objetivos do estudo, que eram pesquisar os cargos atualmente ocupados pelos egressos que atuam na área de TI, obter sugestões de possíveis melhorias para o curso e compreender melhor a eficácia do curso da perspectiva de quem já passou por todo seu processo de formação.

Dos 131 alunos egressos do curso, 35 responderam ao formulário, cerca de 26,71% dos egressos.

Considerando atualizar esta pesquisa, sugere-se para futuros trabalhos a realização de ações para angariar mais respondentes, realizar pesquisa com os desistentes do curso e estudos sobre quais cargos a região demanda, para assim poder direcionar melhor o curso, caso necessário.

O estudo sobre a atuação profissional dos alunos egressos do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal Catarinense, Câmpus Sombrio revelou que o curso possui um alto grau de satisfação por parte de seus alunos egressos. Uma visão geral sobre os resultados do formulário aponta que os egressos se encontram bem satisfeitos com suas trajetórias profissionais na área.

No entanto, o estudo também apontou alguns desafios para serem melhorados no curso com base nas sugestões dos

egressos. Possíveis melhorias na perspectiva dos egressos são: aulas práticas mais frequentes, dispositivos de redes de marcas variadas para estudo, ensino de uso de inteligências artificiais, parcerias com prestadores de serviços locais, filtrar quem está tendo primeiro contato e quem já está familiarizado com a área de Redes de Computadores.

6. Agradecimentos

Ao Comitê de Ética em Pesquisa em Seres Humanos do Instituto Federal Catarinense pela atenção prestada na solicitação de pesquisa, que foi aprovada, sob número de registro CAAE 80465924.4.0000.8049

7. Referências

- BAILER, C., TOMITCH, L. M. B., & D'ely, R. C. S. F. (2011). O planejamento como processo dinâmico: a importância do estudo piloto para uma pesquisa experimental em linguística aplicada. *Intercâmbio*, 24De Almeida Greff, Ponciano (2009). “Especificação de um Sistema para Monitoramento de Atividades de Natação usando RFId”.
https://wiki.sj.ifsc.edu.br/images/0/06/ProjetoFinal_Ponciano.pdf.
- BALDISSERA, O. (2024). Como fazer a revisão bibliográfica do TCC. Blog do EAD. <https://www.blogdoead.com.br/tag/vida-na-universidade/revisao-bibliografica>. [Online: acesso em 29-Janeiro-2024].
- BORGES, T. N., PARISI, C., & GIL, A. D. L. (2005). O Controller como gestor da Tecnologia da Informação: realidade ou ficção?. *Revista de Administração Contemporânea*, 9, 119-140.

- BRANSKI, R. M., FRANCO, R. A. C., & LIMA JUNIOR, O. F. (2010, January). Metodologia de estudo de casos aplicada à logística. In XXIV ANPET Congresso de Pesquisa e Ensino em Transporte (pp. 2023-10).
- COELHO, B. (2020). Mão na massa: como delimitar a metodologia científica do seu trabalho? Mettzer. <https://blog.mettzer.com/metodologia-cientifica>. [Online: acesso em 21-Maio-2024].
- Como usar o aplicativo Google Formulários. Google. <https://support.google.com/docs/answer/6281888?hl=pt-BR&co=GENIE.Platform%3DDesktop>. [Online: acesso em 02-Janeiro-2024].
- COSTA, J. R. F., & DINIZ, R. M. (2023). Um estudo sobre egressos do curso de Licenciatura em Computação da Universidade de Brasília.
- COSTA, R. M., ALBUQUERQUE, D. W., DANTAS FILHO, E., VALADARES, D. C., GOMES, A. B., & PERKUSICH, M. (2023, August). Atuação Profissional dos Egressos do Curso de Telemática. In Anais do XXXI Workshop sobre Educação em Computação (pp. 499-509). SBC.
- DE ASSIS, M. C. (2010). METODOLOGIA DO TRABALHO CIENTÍFICO.
- EISENHARDT, K. M. (1989). Building Theories from Case Study Research. *Academy of management review*, 14(4), 532-550.
- FERNANDES, S. R. S., OLIVEIRA, J. S. S. (2023). PROJETO PEDAGÓGICO DO CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES, p. 28-31.

- LEOPOLDO, J. F. (2016). PERFIL DE ATUAÇÃO DOS ALUNOS EGRESSOS DO CURSO DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO.
- MALHOTRA, N. K. (2019). Pesquisa de Marketing-: uma orientação aplicada. Bookman Editora.
- MARCONI, M. D. A., & Lakatos, E. M. (2003). Fundamentos de metodologia científica. Atlas.
- MARQUES, B. C., Beteli, L. B. (2018). Atuação Profissional dos Alunos Egressos do Curso Tecnologia em Redes de Computadores do Instituto Federal Catarinense, Câmpus Sombrio, Tecnologia e Redes - 4^a edição, p. 7-43.
- MENEZES, P. Estudo de Caso: o que é, exemplos e como fazer. Significados. <https://www.significados.com.br/estudo-de-caso>. [Online: acesso em 29-Janeiro-2024].
- Mercado de tecnologia em constante evolução: tendências e oportunidades de carreira. Insper. <https://www.insper.edu.br/pt/conteudos/tecnologia/mercado-de-tecnologia>. [Online: acesso em 04-Janeiro-2025].
- O que é rede de computadores? Saiba mais sobre a tecnologia que nos conecta. Controle Net. <https://www.controle.net/faq/rede-de-computadores>. [Online: acesso em 06-Janeiro-2024].
- Profissões de tecnologia: perspectivas e demanda atual do mercado de trabalho. Insper. <https://www.insper.edu.br/pt/conteudos/tecnologia/profissoes-de-tecnologia>. [Online: acesso em 04-Janeiro-2025].
- RAVAGNANI, A. (2024). Mercado de tecnologia cresce, mas encontrar profissionais qualificados ainda é um desafio. Carta Capital. <https://www.cartacapital.com.br/do-micro-ao-macro/mercado-de-tecnologia-cresce-mas-encontrar->

- profissionais-qualificados-ainda-e-um-desafio. [Online: acesso em 30-Outubro-2024].
- SANTOS, A. C. B. S. (2023). Estudo institucional e apreciativo do atual estágio de institucionalização da Secretaria da Controladoria-Geral do Estado de Pernambuco.
- SANTOS, A. C. N. N. (2023). A importância do gestor de tecnologia da informação para as organizações.
- SCHEREDER, B. N. (2021). Atuação dos Profissionais na área de TI: investigação das percepções e necessidades das competências dos profissionais de TI pelo meio produtivo na região de Goiânia e Anápolis.
- SOUSA, P. (2023). Egresso - O que é, conceito, importância e exemplos. Conceito.de. <https://conceito.de/egresso>. [Online: acesso em 06-Janeiro-2024].
- TANENBAUM, A. S., & WETHERALL, D. (2011). Redes de computadores. Tradução Daniel Vieira, revisão técnica Isaías Lima, São Paulo, Pearson Prentice Hall.
- YIN, R. K. (2009). Case study research: Design and methods (Vol. 5). sage.

APÊNDICE A - Formulário

Esse questionário é referente ao Trabalho de Conclusão de Curso (TCC) em redes de computadores intitulado "Atuação Profissional dos Alunos Egressos do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal Catarinense - Câmpus Sombrio" que está sendo produzido por Andrey Schwanck Machado sob orientação do professor Victor Martins de Sousa no Instituto Federal Catarinense (IFC).

Esse questionário foi desenvolvido para egressos do curso, portanto a participação destes é fundamental para o trabalho em desenvolvimento. Assim gostaria da vossa inestimável colaboração, se possível, respondendo esse questionário até o dia 08/09/2024.

Me coloco à disposição para qualquer tipo de esclarecimento através do e-mail (andreyismjvm@hotmail.com). O questionário é anônimo então, por favor, não hesite em responder sinceramente.

Desde já agradeço a sua colaboração.

No final deste questionário, ofereço uma pequena recompensa digital como agradecimento pelo seu tempo e esforço respondendo ao questionário.

Esta pesquisa foi aprovada pelo Comitê de Ética em Pesquisa em Seres Humanos do Instituto Federal Catarinense sob número de registro CAAE 80465924.4.0000.8049. Contato do professor orientador: victor.sousa@ifc.edu.br

1 - Termo de Consentimento Livre e Esclarecido (TCLE) disponível no link.

a) Realizei a leitura e estou de acordo

2 - Gênero

a) Feminino

b) Masculino

c) Outro

3 - Cidade que reside atualmente

Por favor, se a sua cidade **não** estiver listada abaixo, selecione a opção "**Outros**" e digite o nome de sua cidade **corretamente** e com as **iniciais maiúsculas**.

a) Araranguá

b) Arroio do Sal

c) Balneário Gaivota

d) Blumenau

e) Criciúma

f) Ermo

g) Florianópolis

h) Jacinto Machado

i) Passo de Torres

j) Porto Alegre

k) Santa Rosa do Sul

l) São João do Sul

m) Sombrio

n) Torres

o) Outros: _____

4 - Cidade de origem antes de concluir a graduação

Por favor, se a sua cidade **não** estiver listada abaixo, selecione a opção "**Outros**" e digite o nome de sua cidade **corretamente** e com as **iniciais maiúsculas**.

a) Araranguá

- b) Arroio do Sal
- c) Balneário Gaivota
- d) Blumenau
- e) Criciúma
- f) Ermo
- g) Florianópolis
- h) Jacinto Machado
- i) Passo de Torres
- j) Porto Alegre
- k) Santa Rosa do Sul
- l) São João do Sul
- m) Sombrio
- n) Torres
- o) Outros: _____

5 - Já possuía conhecimento na área de Tecnologia da Informação antes de ingressar na faculdade?

- a) Sim, me matriculei para melhorar currículo ou expandir conhecimento
- b) Sim, porém apenas conhecimentos básicos
- c) Não

6 - Você estava preparado para o mercado de trabalho quando se formou?

- a) Muito
- b) Razoavelmente
- c) Pouco

d) Não

7 - Atualmente você está exercendo atividade profissional?

- a) Sim, na área de minha formação acadêmica
- b) Sim, fora da área de minha formação acadêmica
- c) Não

Você atua na área.

Você respondeu na pergunta anterior que atua na área de Tecnologia da Informação.

8 - Você atua em qual sub-área/cargo?

- a) Administrador de Redes
- b) Analista de Redes
- c) Analista de Segurança da Informação
- d) Analista de Tecnologia da Informação
- e) Arquitetura de Redes
- f) Desenvolvedor de Software/Aplicativos
- g) Desenvolvedor Web
- h) Programação
- i) Segurança da Informação
- j) Suporte técnico
- k) Técnico em Informática
- l) Outros: _____

9 - Quanto tempo houve entre a formatura e o início de sua atividade profissional?

- a) Já trabalhava antes
- b) Menos de 1 ano

- c) Aproximadamente 1 ano
- d) Aproximadamente 2 anos
- e) Aproximadamente 3 anos
- f) Aproximadamente 4 anos
- g) Mais de 4 anos

10 - Em que tipo de organização você exerce sua atividade profissional?

- a) Autônoma
- b) Empresa própria
- c) Empresa privada
- d) Empresa pública

11 - Em sua visão, qual é a perspectiva profissional na sua área?

- a) Ótima
- b) Boa
- c) Razoável
- d) Desanimadora
- e) Não tenho condições de avaliar

12 - Teve dificuldades na contratação e/ou execução da profissão no mercado de trabalho?

- a) Falta de experiência
- b) Forte concorrência para obter emprego
- c) Falta de domínio de uma língua estrangeira
- d) Não houve dificuldade

13 - A Formação Acadêmica contribuiu para o seu desempenho profissional na área de Tecnologia da Informação?

- a) Muito
- b) Razoavelmente
- c) Pouco
- d) Não

Você não atua na área.

Você respondeu na pergunta anterior que não atua na área de Tecnologia da Informação.

14 - O principal motivo pelo qual você não exerce atividade profissional na sua área de formação é:

- a) Mercado de trabalho saturado
- b) Melhor oportunidade em outra área
- c) Motivos particulares

15 - A formação acadêmica contribuiu para o seu desempenho profissional na sua área?

- a) Muito
- b) Razoavelmente
- c) Pouco
- d) Não

Você não está exercendo atividade profissional atualmente.

Você respondeu na pergunta anterior que não atua profissionalmente no momento.

16 - Você gostaria de compartilhar com o IFC o porquê de não estar atuando profissionalmente no momento?

Favor descrever com breves palavras.

Final

Quase acabando...

17 - Você tem mantido algum contato com o IFC - Campus Sombrio?

- a) Participação de eventos
- b) Curso de atualização
- c) Informação em geral
- d) Procura dos serviços prestados pelo instituto
- e) Não tenho mantido contato

18 - Qual é o conceito que você atribui ao curso que concluiu?

- a) Ótimo
- b) Bom
- c) Regular
- d) Ruim
- e) Péssimo

19 - Você tem alguma sugestão para melhoria?

Sua resposta foi registrada. Muito obrigado pela colaboração.

Como recompensa eu preparei uma playlist no YouTube com algumas das músicas que mais gosto de artistas pequenos e grandes. A ideia é divulgar umas músicas "diferentonas" pelo meio também.

Na playlist, coloquei apenas 1 música por artista pra ficar mais curta, mas recomendo procurar as outras dos mesmos.

Playlist:

<https://www.youtube.com/playlist?list=PL4XFuLSVAI37JwNIQ1KzgbKvCLGC1H3CI>

Uma proposta de controle de acesso e fluxo de veículos e pessoas utilizando LoRa para propriedades de grande extensão

Jeferson da Silva dos Santos¹, Marco Antônio Silveira de Souza², Matheus Lorenzo Braga³

¹, Acadêmico do Instituto Federal Catarinense – Campus Sombrio – 88960000 – Sombrio – SC – Brasil

^{2,3}, Docentes do Instituto Federal Catarinense – Campus Sombrio – 88960000 – Sombrio – SC – Brasil

jefersondosantos89@hotmail.com, marco.souza@ifc.edu.br,
matheus.braga@ifc.edu.br

Abstract. *This article describes a study that aims to improve the access control and security of doors and gates in large residences and institutions. Using the Design and Science Research Methodology (DSRM), devices were developed with two ESP32s using LoRa technology, along with an HTTP server, to enable the connection and automation of gates. After the necessary tests were completed, the feasibility of the study was verified, opening up possibilities for future work, such as the use of cameras to monitor properties and connect other devices, bringing the concept of a smart city. These results can contribute to improving security and access control in residential and institutional environments.*

Resumo. *Este artigo descreve um estudo que visa melhorar o controle de acesso e segurança de portas e*

portões em residências e instituições de grande extensão. Utilizando a Design e Science Research Methodology (DSRM), foram desenvolvidos dispositivos com dois ESP32 com a tecnologia LoRa, juntamente com um servidor HTTP, para permitir a ligação e automação dos portões. Após a finalização dos testes, foi constatada a viabilidade da aplicação do estudo, o que abre possibilidades para trabalhos futuros, como o uso de câmeras para monitorar as propriedades e conectar outros dispositivos, trazendo o conceito de cidade inteligente. Esses resultados podem contribuir para aprimorar a segurança e o controle de acesso em ambientes residenciais e institucionais.

1. Introdução

A necessidade de segurança e controle do patrimônio é uma preocupação constante de proprietários, sejam eles de residências ou de corporações. Automatizar o acesso é uma das soluções para manter a organização e controle de uma propriedade. No entanto, em ambientes de grande extensão, a comunicação entre os equipamentos transmissor e receptor pode se tornar um obstáculo.

Para solucionar esse problema, conceitos de cidades inteligentes e IoT têm sido cada vez mais utilizados, uma vez que grandes extensões dependem de dispositivos compatíveis. A tecnologia LoRa (Long Range) é uma solução que proporciona comunicação de longa distância com baixo custo e consumo de energia. Em propriedades de grande extensão que precisam automatizar o controle de acesso, a tecnologia LoRa pode ser uma alternativa de bom custo/benefício.

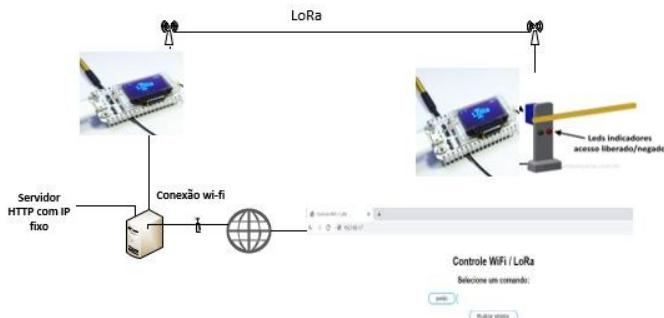
Nesse contexto, este artigo apresenta o desenvolvimento de dispositivos utilizando a tecnologia LoRa, um servidor HTTP e uma página web para a automação de portas e portões em

propriedades com média e grande extensão. O objetivo deste artigo é fornecer uma solução para melhorar a autonomia, controle e economia de tempo por meio da montagem de uma rede LoRa que utiliza o protocolo LoRaWAN para comunicação entre as placas ESP32. Uma das placas hospedará o servidor que fará a interligação com a página web, permitindo abrir e fechar as propriedades remotamente.

O artigo está dividido em cinco seções, sendo a segunda o referencial teórico, na qual serão descritas as tecnologias aplicadas. Na seção de métodos e materiais, serão apresentados todos os materiais utilizados, técnicas e métodos aplicados. Em seguida, na seção de resultados e discussão, será descrito o trabalho e como ele foi aplicado para a resolução da proposta sugerida, concretizando o artefato. As considerações finais retratarão possíveis melhorias e trabalhos a serem desenvolvidos futuramente.

Dessa forma, este artigo busca contribuir para a evolução tecnológica, apresentando uma solução eficiente e de baixo custo para a automação de portas e portões em propriedades de média e grande extensão, que poderão ser controlados de forma remota, aumentando a segurança e o controle sobre o patrimônio.

Figura 1 - Projeto



Fonte:O autor, 2022

2. Referencial teórico

Nesta seção são apresentados os referenciais teóricos utilizados para a pesquisa do presente trabalho.

2.1. LoRa

LoRa (Long Range) é uma tecnologia *Low Power Wide Area Network (LPWAN)* que utiliza modulação de radiofrequência baseada em *Chirp Spread Spectrum (CSS)*. De acordo com Samriddhi (2020), essa técnica é utilizada em comunicações militares e espaciais, permitindo cobrir longas distâncias de comunicação e obter resistência a interferências. Essa tecnologia pode ser utilizada em comunicação ponto a ponto ou em topologia em formato estrela através de gateways (Bertoleti, 2019, p. 18).

No Brasil, a ANATEL publicou a Lei nº 6.506 em agosto de 2018, que aprova os procedimentos para avaliação da conformidade de equipamentos de radiocomunicação com

emissões limitadas, permitindo a operação dos equipamentos no território do país.

O padrão adotado foi o australiano, que usa a faixa de 915 MHz e inclui a faixa de 902 MHz a 907,5 MHz e 915 MHz a 928 MHz. O padrão australiano possui 72 canais para uplink e 8 para downlink. Os canais de uplink de 0 a 63 usam largura de banda de 125 kHz com uma taxa de codificação 4/5 começando em 915,2 MHz e aumentando linearmente de 200 kHz até 927,8 MHz, enquanto os canais de 64 a 71 têm largura de banda de 500 kHz de 915,9 MHz (Bertoleti, 2019, p. 18).

2.2. *LoRaWAN*

LoRaWAN é um dos diversos protocolos para definir como altas das redes. É também uma regulamentação para a camada de controle de acesso à mídia (*MAC*) baseada em nuvem, mas usada sobretudo como uma norma para camada de rede e também para gerenciar a comunicação entre gateways *LPWAN* e dispositivos de nó final. Também, como um protocolo de roteamento mantido pela *LoRa* Alliance. Segundo Osório (2020), sua transmissão de dados não será maior que 5,5 kb/s, tornando assim viável para aplicações em *IoT* (*Internet of Things*).

2.3. *ESP32*

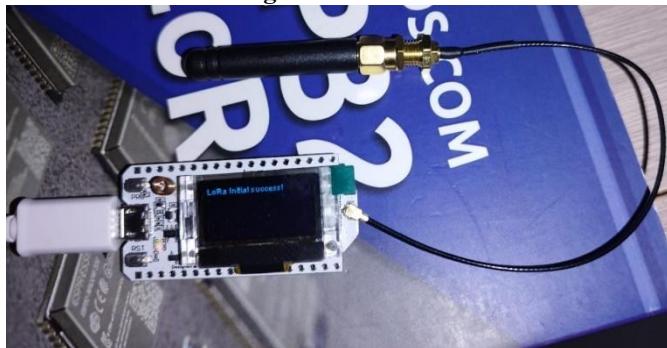
O *ESP32* é um microcontrolador com tecnologia dual core, que inclui o chip *LoRa V2* da fabricante Heltec Automation. Ele é um módulo altamente versátil, já que inclui tecnologia WiFi e Bluetooth, além de um display *OLED*. O *ESP32* é amplamente utilizado para a criação de soluções de *IoT*, devido à sua capacidade de comunicação sem fio e baixo consumo de energia.

Em diversas pesquisas na área de *IoT*, o *ESP32* tem sido amplamente adotado como uma das plataformas preferidas para o desenvolvimento de soluções nessa área, devido às suas

características de conectividade e ao baixo custo de aquisição. Segundo Leston et al. (2021), o *ESP32* é um microcontrolador muito utilizado em projetos de automação residencial, monitoramento ambiental e agrícola, controle de energia e muitas outras aplicações *IoT*.

No contexto deste trabalho, o *ESP32* com o chip *LoRa* V2 da *Heltec Automation* é utilizado como o dispositivo de nó final, responsável pela coleta de dados e comunicação com a rede *LoRaWAN*. O módulo *ESP32* foi escolhido por sua capacidade de comunicação sem fio e por suportar as tecnologias *WiFi*, *Bluetooth* e *LoRa*, tornando-se uma solução ideal para a construção de dispositivos *IoT* com recursos avançados de conectividade.

Figura 2 - *ESP32*



Fonte: O autor, 2022

2.4 Servidor HTTP

O *HTTP* (*Hypertext Transfer Protocol*) é um dos protocolos mais importantes da internet, responsável por permitir a comunicação entre clientes e servidores web. Ele é utilizado para transferir informações como imagens, vídeos, textos e outros arquivos entre esses dispositivos. O *HTTP* é fundamental para o funcionamento das aplicações web modernas, que dependem

dele para permitir que os usuários acessem e interajam com conteúdo na internet.

Segundo Nadeem et al. (2019), o protocolo *HTTP* foi desenvolvido em 1991 pelo físico britânico Tim Berners-Lee, considerado o criador da *World Wide Web (WWW)*. Inicialmente, o *HTTP* era utilizado apenas para transferir documentos em hipertexto, como páginas HTML, mas com o passar do tempo, passou a ser utilizado para a transferência de diversos tipos de arquivos e dados.

No contexto deste trabalho, o protocolo *HTTP* é utilizado para realizar a comunicação entre a aplicação web e o servidor web. A aplicação web é hospedada no servidor e acessada pelos usuários através de seus navegadores web. Quando o usuário interage com a aplicação, os dados são transmitidos via *HTTP* para o servidor, que processa as informações e retorna a resposta adequada para o navegador.

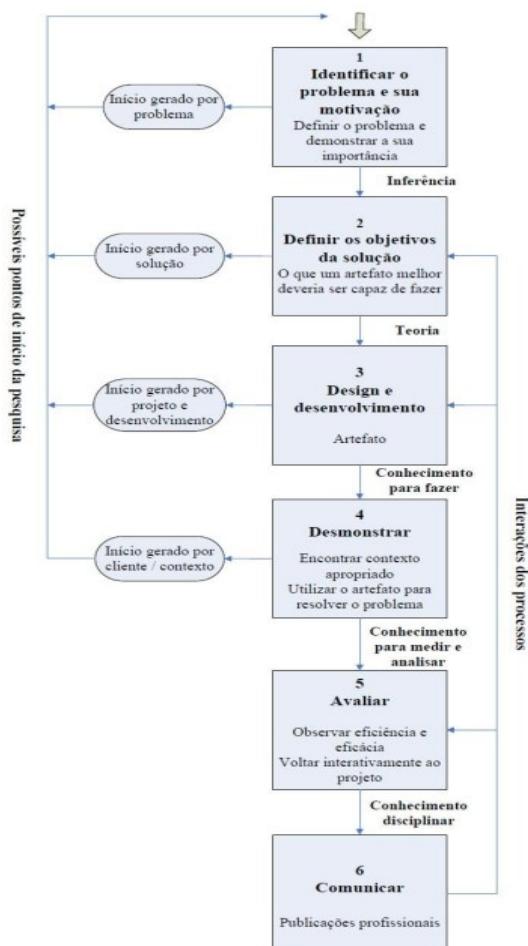
De acordo com Maruyama et al. (2019), o *HTTP* é um protocolo de camada de aplicação, baseado em texto, que utiliza o método de requisição-resposta. Na requisição, o cliente solicita uma ação ao servidor, enquanto na resposta, o servidor envia ao cliente uma mensagem com o resultado da ação solicitada. O *HTTP* utiliza o conceito de *URL (Uniform Resource Locator)* para identificar os recursos a serem transferidos entre os dispositivos.

O uso do protocolo *HTTP* é essencial para o funcionamento das aplicações web modernas, permitindo a criação de interfaces de usuário dinâmicas e responsivas, bem como a integração de diversas tecnologias e serviços web. Segundo Li et al. (2021), o *HTTP* é amplamente utilizado em diversas outras aplicações na internet, como serviços de streaming de vídeo, download de arquivos e comunicação entre sistemas distribuídos.

3. Materiais e Métodos

O presente artigo foi desenvolvido seguindo o método de pesquisa tecnológica através da técnica DSRM (Design Science Research Methodology), conforme proposto por Freitas Junior (2018).

Figura 3 - DSRM



Fonte: Freitas Junior (2018)

Para tanto, foram realizadas pesquisas bibliográficas, além de consultas aos sites dos fabricantes de dispositivos com tecnologia LoRa. Dentre os materiais utilizados, destacam-se:

- a) Notebook Acer Aspire E 15, equipado com processador Intel® Core™ i5-5200U e sistema operacional Windows 11, utilizado para configuração das placas e desenvolvimento das linguagens de programação;
- b) Arduino IDE 1.8, essencial para importação de bibliotecas e programação das placas, utilizando a linguagem C;
- c) Duas placas *ESP32* com *LoRa* V2 Heltec, utilizadas para implementação do trabalho como transmissor e receptor, comunicando-se por tecnologia *LoRa* através do protocolo *LoRaWAN*;
- d) Módulo Relé Songle de 10A, de extrema importância para o acionamento do dispositivo final;
- e) Visual Studio Code, utilizado para programação da página web utilizando as linguagens HTML (HyperText Markup Language) e CSS (Cascading Style Sheets), onde serão acionados os dispositivos. Além disso, foram consultados outros fabricantes de chips com tecnologia LoRa, como Semtech e Murata, a fim de avaliar outras opções disponíveis no mercado e enriquecer a pesquisa.

Segundo Semtech (2022), uma das principais fabricantes de chips com tecnologia LoRa, a comunicação LoRaWAN é capaz de atingir longas distâncias e oferecer alta capacidade de penetração em obstáculos, tornando-a ideal para aplicações em IoT. De acordo com Murata (2021), outro importante empresa do ramo, a tecnologia LoRa é altamente eficiente em termos de

consumo de energia, o que permite a operação de dispositivos alimentados por bateria por longos períodos.

Conforme ressaltado por Glaropoulos et al. (2020), a tecnologia LoRa é especialmente adequada para aplicações de automação residencial, devido à sua capacidade de transmitir dados de sensores e dispositivos de forma confiável e econômica. Em um estudo realizado por Cho et al. (2021), foi demonstrado que a utilização de placas ESP32 com tecnologia LoRa em conjunto com um servidor LoRaWAN pode proporcionar uma solução eficiente e escalável para monitoramento de energia em residências.

Seguindo a abordagem da DSRM, a pesquisa tecnológica realizada neste trabalho objetivou não apenas desenvolver um protótipo funcional, mas também contribuir para o avanço do conhecimento na área de automação residencial, como defendido por Hevner et al. (2004).

4. Resultados e Discussão

Para fins de montagem dos dispositivos e implementação dos mesmos, realizou-se aplicação de um passo a passo, junto a figuras que implicará em uma melhor resolução dos resultados obtidos, assim ficará subentendido melhor compreensão do trabalho realizado.

A escolha dos dispositivos *ESP32* se dá pelo baixo custo e facilidade de reposição de peças, também com um consumo energético menor aos convencionais, podendo assim ser alimentado até por pequenas baterias.

A Arduino IDE foi utilizada como ferramenta de programação, sendo uma opção de fácil compreensão mesmo para aqueles que não estão familiarizados com IDEs de desenvolvimento. Segundo Calvo et al. (2018), a Arduino IDE é uma plataforma de desenvolvimento de software livre que oferece suporte para várias placas e linguagens de programação,

incluindo a linguagem C, que foi utilizada neste trabalho para as aplicações principais.

Dessa forma, a escolha da Arduino IDE foi uma decisão estratégica para o desenvolvimento do projeto, uma vez que ofereceu facilidade e flexibilidade para a programação dos dispositivos.

4.1. Compilação de códigos

A implementação do sistema que permitiu a integração de duas máquinas e a troca de informações entre elas com melhor desempenho foi realizada utilizando a linguagem C. Para isso, foi montado um código estruturado de maneira limpa e de fácil compreensão, dividido em seções, utilizando a plataforma Arduino *IDE*.

No código do emissor (sender), primeiramente foram inseridas as bibliotecas responsáveis por definir os parâmetros do sistema. Em seguida, foram definidas informações como o estado do display, a tecnologia que seria utilizada para a comunicação dos dispositivos e a identificação do serial do aparelho, se ele estaria ou não ativo para a conexão. Além disso, foi definido se o amplificador de potência estaria atuante ou não.

Para a comunicação dos dispositivos *LoRa*, foi utilizada a faixa de frequência de 915MHz, que é o padrão australiano para a transmissão de dados. Essa escolha se deu em função da alta eficiência dessa frequência na transmissão de dados a longa distância, o que possibilitou uma comunicação mais eficaz entre as duas máquinas.

Figura 4 – Código sender



```

1 //COM 6
2 #include "Arduino.h" //inclui a biblioteca padrão Arduino.h
3 #include "Heltec.h" //inclui a biblioteca da Heltec
4 #include "WiFi.h" //inclui a biblioteca WiFi
5 // Definições do rádio LoRa
6 #define DisplayEstado true //define se o display estará ou não ativo
7 #define LoRAEstado true //define se o rádio LoRa estará ou não ativo
8 #define SerialEstado true //define se a Serial do módulo estará ou não disponível (Baud Rate padrão 115200)
9 #define AmplificadorDePotencia true // define se o amplificador de potência PABOOST estará ou não ativo
10 #define BandaDeTransmissao 915E6 //define a frequência média de transmissão: 868E6, 915E6
11 // Definições do WiFi
12 #define SSId "Jef e Jaque" //Identificador do serviço de rede WiFi
13 #define Senha "892004helena" //Senha de acesso ao serviço WiFi
14 //Variáveis de estado dos controlados
15 bool Estadoportao = 0;
16 bool Estadocamera = 0;
17 bool Estadodolofote = 0;
18 bool Atuar = false;
19 //Inicia o servidor na porta 80
20 WiFiServer servidor(80);
21 void setup()
...

```

Fonte: O autor, 2022

Esse, por definição, será também usado mais abaixo como servidor HTTP, identificando uma rede wi-fi para o serviço.

Contou também como a utilização de uma rede de IP fixo para a ancoragem do servidor.

Figura 5 – IP fixo

```
  //inicio dos ajustes do conexão WiFi
  WiFi.disconnect(true); //Desconecta de uma possível conexão prévia
  delay(100);
  IPAddress ip(192,168,1,12); // Definição de um IP fixo
  IPAddress gateway(192,168,1,1); //Gateway da rede
  IPAddress subnet(255,255,255,0); //Máscara de rede
  WiFi.mode(WIFI_STA); //Ajusta para o modo STATION
  WiFi.setAutoConnect(true); //Ativa a auto reconexão
  WiFi.config(ip, gateway, subnet); //Configura os endereços fixos
  WiFi.begin(SSid, Senha); //Informa o id do Serviço WiFi e a senha
  delay(100);
  byte count = 0; // Contador das tentativas de conexão

  while (WiFi.status() != WL_CONNECTED && count < 10)
```

Fonte: o autor, 2022

Para o acesso às informações, criou-se uma página web para ser acessada remotamente, que fará o papel de ligação dos serviços no receptor.

Entretanto, na parte do receiver, ou em português receptor, o código é muito mais simples. Foram usadas só as entradas de informação ditadas quais pinos do módulo ESP32 farão as funções de ligação e a frequência que o sinal transmitirá. Define quais pinos de saída, recebe o sinal e imprime no display o RSSI (Received Signal Strength Indicator).

Figura 6 – Código receiver

```

receiver_correto
1 // COM 6
2 #include "heltec.h" //inclui a biblioteca da Heltec
3 #define DisplayEstado true //define se o display estará ou não ativo
4 #define LoRaEstado true //define se o rádio LoRa estará ou não ativo
5 #define SerialEstado true //define se a Serial do módulo estará ou não disponível
6 // (Baud Rate padrão 115200)
7 #define AmplificadorDePotencia true // define se o amplificador de potência PABOOST estará ou não ativo
8 #define BandaDeTransmissao 915E6 //define a frequência média de transmissão: 868E6, 915E6
9 #define pinPortao 22 //pino usado para acionar o motor do portão
10 #define pinCamera 23 //pino usado para acionar a câmera
11 #define pinHolofote 17 //pino usado para acionar o holofote
12 void setup()
13 {
14     //define os pino como saída
15     pinMode(pinPortao, OUTPUT);
16     pinMode(pinCamera, OUTPUT);
17     pinMode(pinHolofote, OUTPUT);
18     //os pinos são ajustados para nível alto logo no inicio
19     //porque o módulo de relés tem lógica invertida
20     digitalWrite(pinPortao, HIGH);
21     digitalWrite(pinCamera, HIGH);
22     digitalWrite(pinHolofote, HIGH);
23 //inicia o ESP Wifi LoRa 32 da Heltec
24 Heltec.begin(DisplayEstado, LoRaEstado, SerialEstado, AmplificadorDePotencia, BandaDeTransmissao);
25 SetupLoRa(); //faz os ajustes do rádio LoRa
26 delay(100);

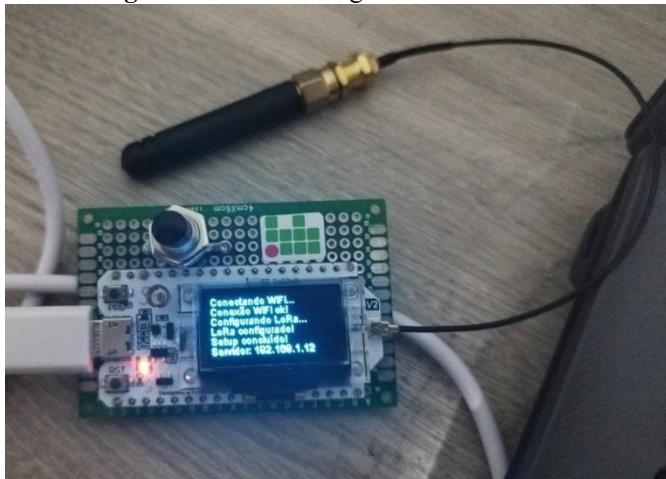
```

Fonte: o autor, 2022

4.2. Montagem dos dispositivos

Usou-se duas placas ESP32 com tecnologia LoRa, com base nas pesquisas feitas, usando uma máquina como transmissor que fará a interligação com a rede através de um servidor HTTP e enviará os dados via protocolo LoRaWan.

Figura 7 – Terminal aguardando conexão

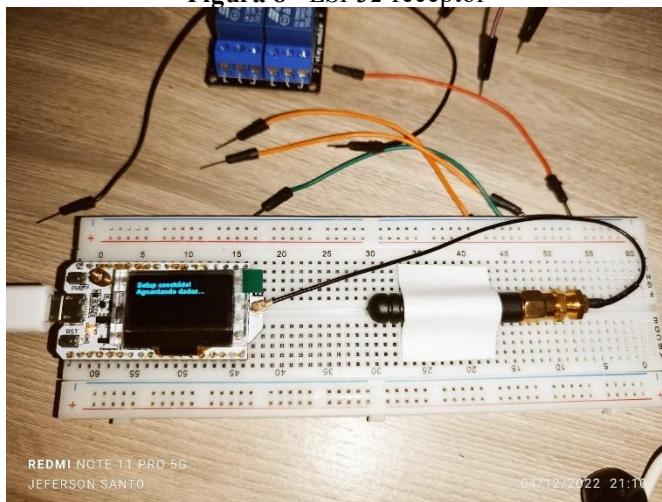


Fonte: O autor, 2022

A placa *sender*, aguardando ligação com o receptor, pois aparece no display como *wi-fi* configurado e IP do servidor fixo.

Já na parte do receptor, o dispositivo fica inativo até haver interação.

Figura 8 - ESP32 receptor



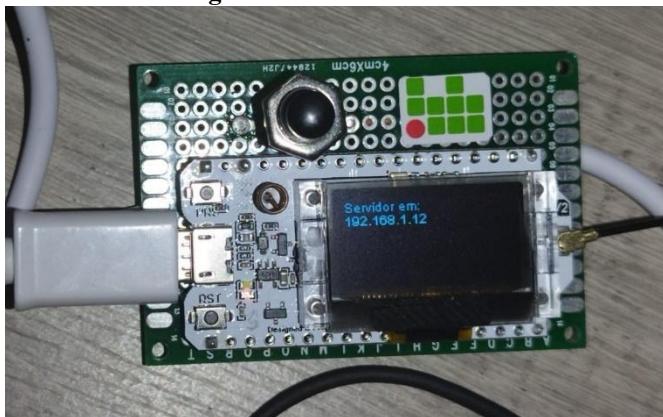
Fonte: O autor, 2022

Ao fazer o acesso do IP fixo para a função de chamar a página web, temos acesso ao painel de controle de automação dos dispositivos.

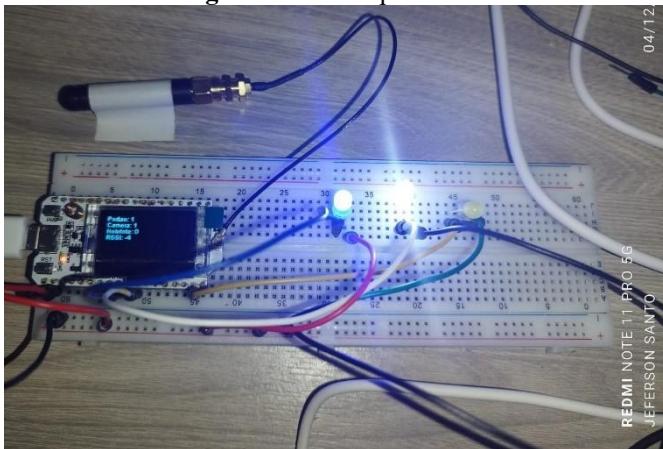
Figura 9 – página de controle

Fonte: O autor, 2022

Com os acionamentos dos dispositivos a placa *sender* (transmissor) fica em estado servidor e printa no display o número do IP.

Figura 10 – Servidor ativo**Fonte: O autor, 2022**

Automaticamente, o receptor recebe os comandos, acionará os dispositivos ligados a ele e printará na tela qual dispositivo está ligado, qual estará desligado e também o RSSI que se trata do alcance do sinal da antena.

Figura 11 – Receptor ativo**Fonte: o autor, 2022**

4.3. Teste de sinal

Nesse estudo também foram realizados medição de alcance e qualidade de sinal do disposto LoRa. A medição baseou-se na potência do sinal, medida através do RSSI e seu alcance em metros. Foi utilizado as antenas originais, visto que o fabricante indica a distância máxima de 3600 metros, levando em consideração propriedades rurais, e de 1400 metros em propriedades urbanas

Entretanto, os testes revelaram que as antenas têm um alcance muito menor. Mediou-se em linha reta a distância de 450 metros.

Tabela 1 sinal x metros

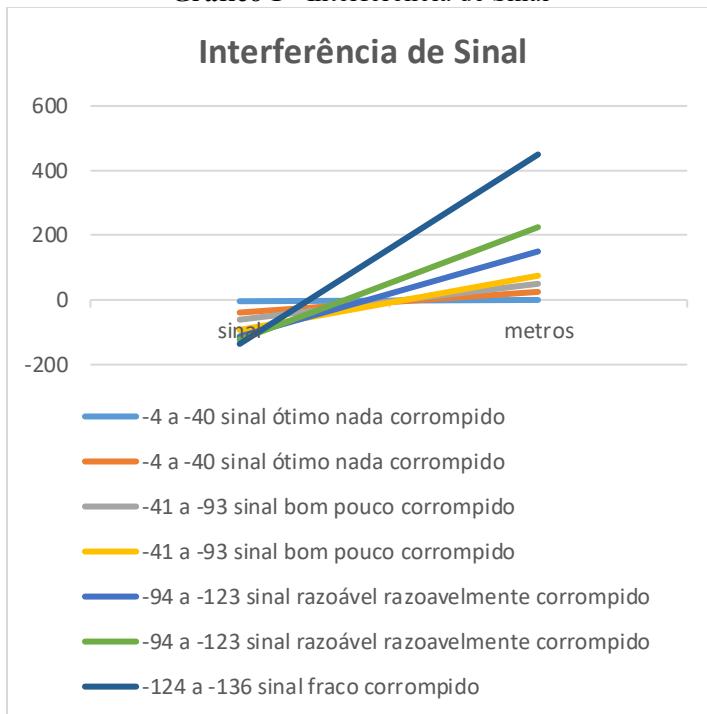
medida de comparação	variação de sinal	pacotes	sinal	metros
-4 a -40	sinal ótimo	nada corrompido	-4	0
-4 a -40	sinal ótimo	nada corrompido	-39	25
-41 a -93	sinal bom	pouco corrompido	-61	50
-41 a -93	sinal bom	pouco corrompido	-93	75
-94 a -123	sinal razoável	razoavelmente corrompido	-113	150
-94 a -123	sinal razoável	razoavelmente corrompido	-123	225

-124 a -136	sinal fraco	corrompido	-136	450
-------------	-------------	------------	------	-----

Fonte: o autor, 2022

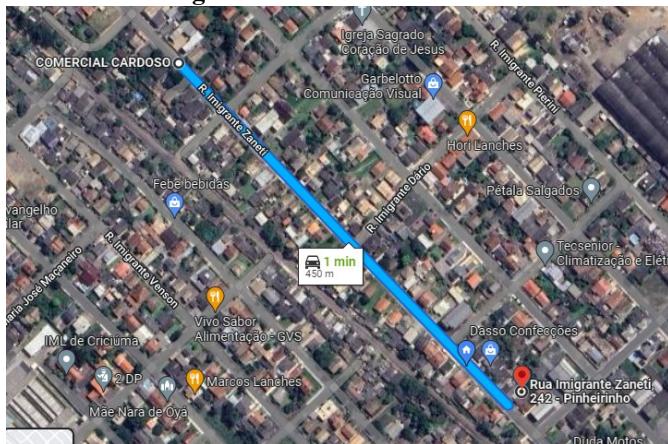
O estudo apresentou variação de sinal e erro a partir de 75 metros, muito suscetível a interferência.

Gráfico 1 - Interferência de Sinal



Fonte: o autor, 2022

Figura 12 – Percurso de Teste



Fonte: O autor, 2022

A medição foi realizada em linha reta em uma rua de Criciúma.

5. Considerações Finais

Apesar das dificuldades e imprevistos que surgiram ao longo do projeto, foi possível concluir a montagem dos dispositivos com determinação e foco.

Inicialmente, o projeto tinha a intenção de utilizar inteligência artificial e câmera para leitura de placas de veículos e automatizar a comunicação com um banco de dados. Contudo, devido ao tempo restrito e à complexidade da pesquisa, optou-se por uma abordagem mais simples, porém igualmente valiosa para o estudo em questão.

Este trabalho permitiu a realização de um estudo que possibilitará a implementação de melhorias em propriedades de grande extensão, utilizando a tecnologia LoRa. Com base em uma estrutura de baixo custo e consumo energético reduzido. Espera-se que essas melhorias sejam acessíveis a um público

mais amplo e possam contribuir para o desenvolvimento sustentável.

Para trabalhos futuros, sugere-se a ampliação da rede utilizando gateway, permitindo a automação de vários dispositivos simultaneamente e abrindo novas possibilidades de aplicação da tecnologia *LoRa*.

Gostaria de agradecer à minha família, em especial à minha esposa Jaqueline Inês Agnes e à minha filha Helena Agnes dos Santos, que me apoiaram durante finais de semana e momentos de ausência. Ser o primeiro filho a concluir um curso superior em uma universidade renomada é um marco importante na minha vida, e não seria possível sem o amor e suporte incondicionais deles.

Também gostaria de agradecer aos professores que não só foram excelentes orientadores, mas se tornaram amigos ao longo desses anos de curso. Sem a ajuda e incentivo deles, esse sonho não teria se tornado realidade.

Referências

- DE OLIVEIRA JÚNIOR, Javan; OYAMADA, Marcio. Avaliando o impacto da compressão de dados no desempenho e energia em redes LoRa. In: ARTIGOS COMPLETOS - SIMPÓSIO BRASILEIRO DE ENGENHARIA DE SISTEMAS COMPUTACIONAIS (SBESC), 10. , 2020, Evento Online. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 81-88. ISSN 2763-9002. DOI: https://doi.org/10.5753/sbesc_estendido.2020.13094.
- OSORIO M. CALLE, J. D. Soto and J. E. Candeló-Becerra, "Routing in LoRaWan: Overview and Challenges," in IEEE Communications Magazine, vol. 58, no. 6, pp. 72-76, June 2020, doi:: 10.1109/MCOM.001.2000053.
- F. ADELANTADO, X. VILAJOSANA, P. TUSET-PEIRO, B. MARTINEZ, J. MELIA-SEGÜI AND T. WATTEYNÉ, "Understanding the Limits of LoRaWAN," in IEEE Communications Magazine, vol. 55, no. 9, pp. 34-40, Sept. 2017, doi: 10.1109/MCOM.2017.1600613.
- LORA ALLISANCE. What is LaRaWan? 2015. URL: <https://lora-alliance.org/wpcontent/uploads/2020/11/what-is-lorawan.pdf>. Acesso: 27/11/2022.
- FREITAS JUNIOR, Vanderlei Guia para escrita de artigos científicos: uma perspectiva da pesquisa tecnológica / Vanderlei Freitas Junior; Victor Martins de Sousa. - Sombrio: Instituto Federal 2018.
- INGALE, P.; ASWALE, P.; AKSAPURE, P.; CHAUDHURI, K. Sistema de Posicionamento Distressed baseado em Long Range Module (LoRa).
- SAMRIDDHI: Um Jornal de Ciências Físicas, Engenharia e Tecnologia, v. 12, n. SUP 2, pág. 01-05, 30 nov. 2020.

SV, ASWIN KUMMER et al. Monitoramento de Parâmetros Industriais com Tecnologia Lora em Comunicações Sem Fio de Próxima Geração. Turco. J. Fisioterapeuta. Rehabil, v. 32, n. 2, 2021.

BERTOLRTI, Pedro Projetos com ESP 32 e Lora/ Instituto NCB 2019.

LI, M., Zeng, X., & Jiang, S. (2021). A Novel HTTP-based Caching Scheme for Video Streaming Services. *IEEE Transactions on Circuits and Systems for Video Technology*, 31(3), 1173-1183.

MARUYAMA, K., Watanabe, H., & Higashino, T. (2019). A Study of HTTP Request-Response Processing Over TCP and QUIC. *IEEE Communications Magazine*, 57(12), 70-76.

NADEEM, M., Iqbal, W., Arif, S., & Saeed, S. (2019). A Comprehensive Review of Internet Protocols and Standardization Organizations. *Journal of King Saud University-Computer and Information Sciences*, 31(4), 393-404.

ESPRESSIF SYSTEMS. (2021). ESP32. Recuperado em 27 de janeiro de 2023, de <https://www.espressif.com/en/products/socs/esp32/overview>

HELTEC AUTOMATION. (2021). ESP32 LoRa Development Board. Recuperado em 27 de janeiro de 2023, de <https://heltec.org/project/wifi-lora-32/>

LESTON, J., Rodrigues, E., Braga, R., & Zuffo, M. (2021). Development of an IoT System for Air Quality Monitoring Based on LoRaWAN. In *Proceedings of the 34th Conference on Graphics, Patterns and Images* (pp. 1-8). IEEE. <https://doi.org/10.1109/SIBGRAPI51730.2021.00008>

OLIVEIRA, R., Nunes, G., & Carvalho, H. (2020). ESP32 as a Platform for IoT Applications: A Survey. In *Proceedings of*

the 33rd Conference on Graphics, Patterns and Images (pp. 1-8). IEEE.

<https://doi.org/10.1109/SIBGRAPI51864.2020.00029>

SEMTECH. (2022). LoRaWAN® for IoT. Recuperado em 27 de janeiro de 2023, de <https://lora-developers.semtech.com/resources/white-paper/lorawan-iot>

MURATA. (2021). LoRaWAN. Recuperado em 27 de janeiro de 2023, de <https://www.murata.com/en-eu/products/wireless-communication-module/lpwa/lora>

GLAROPOULOS, I., Papadopoulos, G. A., Groumas, P., & Kameas, A. (2020). Comparative study of wireless technologies for home automation applications. International Journal of Interactive Mobile Technologies, 14(6), 1-22.

CHO, S., Park, H., Kim, S., & Oh, J. (2021). Energy monitoring and management system using LoRaWAN network. Electronics, 10(2), 144.

HEVNER, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.

CALVO, J. M., García, J. C., Valenzuela, S., & Arriagada, C. (2018). Platform for open-source embedded development in Internet of Things (IoT) based on Arduino. In 2018 International Conference on Electronics, Communications and Computers (CONIELECOMP) (pp. 140-145). IEEE.