INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES
CAMPUS MACAPÁ

LEANDRO AFONSO LOPES CARDOSO
SILVIO NUNES DE SOUZA

DESENVOLVIMENTO DE UM GUIA COM CONFIGURAÇÕES E FATORES INFRAESTRUTURAIS EM REDES WIRELESS PARA AMBIENTES SOHO

MACAPÁ – AP
2023

LEANDRO AFONSO LOPES CARDOSO
SILVIO NUNES DE SOUZA

DESENVOLVIMENTO DE UM GUIA COM CONFIGURAÇÕES E FATORES INFRAESTRUTURAIS EM REDES WIRELESS PARA AMBIENTES SOHO

Trabalho de Conclusão de Curso apresentado ao curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Orientador: Me Olavo Nylander Brito Neto

MACAPÁ - AP
2023

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

C268d Cardoso, Leandro Afonso Lopes
Desenvolvimento de um guia com configurações e fatores infraestruturais em redes wireless para ambientes SOHO / Leandro Afonso Lopes Cardoso, Silvio Nunes de Souza. - Macapá, 2023.
67 f.: il.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2023.

Orientadora: Olavo Nylander Brito Neto.

1. Segurança cibernética. 2. Redes SOHO. 3. Tecnologia wireless.. I. Souza, Silvio Nunes de. I. Brito Neto, Olavo Nylander, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

LEANDRO AFONSO LOPES CARDOSO
SILVIO NUNES DE SOUZA

DESENVOLVIMENTO DE UM GUIA COM CONFIGURAÇÕES E FATORES INFRAESTRUTURAIS EM REDES WIRELESS PARA AMBIENTES SOHO

Trabalho de Conclusão de Curso apresentado ao curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Orientador: Me Olavo Nylander Brito Neto

BANCA EXAMINADORA

Me Olavo Nylander Brito Neto
Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP

Thiêgo Maciel Nunes
Me Thiego Maciel Nunes
Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP

gov.br Documento assinado digitalmente
LOURIVAL QUEIROZ ALCANTARA JUNIOR
Data: 06/10/2023 07:00:25-0300
Verifique em https://validar.iti.gov.br

Me Lourival Queiroz Alcantara Junior
Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP

Aprovados em: 04 / 10 / 2023

Nota: 9,0

A família que me apoiou incondicionalmente durante todo esse percurso, especialmente a minha mãe Maria das Graças Santos Lopes e ao meu pai Mario Afonso Nunes Cardoso.

(CARDOSO, 2023)

A família que me apoiou incondicionalmente durante todo esse percurso, especialmente a minha querida mãe Elizângela Ferreira Lobato.

(SOUZA, 2023)

AGRADECIMENTOS

A Deus, pelas nossas vidas, e por nos permitir ultrapassar todos os obstáculos encontrados ao longo da realização desta monografia. Aos amigos e familiares por todo o apoio e pela ajuda, que muito contribuíram para a realização deste trabalho.

Agradeço a minha querida mãe Elizângela Ferreira Lobato, ao meu querido pai Laércio Nunes de Oliveira, aos meus fortes irmãos Elessandro Lobato de Oliveira e Luiz Carlos Lobato de Oliveira e aos meus avós José Norvino e Maria Ferreira, (SOUZA, 2023). Agradeço a minha querida mãe Maria das Graças Santos Lopes, ao meu querido pai Mario Afonso Nunes Cardoso e a minha querida tia Maria Aparecida Santos Lopes, (CARDOSO, 2023).

Aos professores, pelas correções e ensinamentos que nos permitiram apresentar um melhor desempenho no nosso processo de formação profissional ao longo do curso. São eles: Aldina Tatiana Silva Pereira; André Luiz da Silva Freire; Andrew Hemerson Galeno Rodrigues; Célio do Nascimento Rodrigues; Clayton Jordan Espíndola do Nascimento; Dejildo Roque de Brito; Ederson Wilcker Figueiredo Leite; Emílio Balieiro de Souza; Hilton Prado de Castro Júnior; Jairo de Kassio Siqueira Barreto; Klenilmar Lopes Dias; Lourdes Terezinha Picanço Paes (que Jaz entre nós); Neilson Oliveira da Silva; Raimundo Alves Medeiros Neto; Thiego Maciel Nunes; Especialmente a nosso Professor Orientador Me Olavo Nylander Brito Neto, e nossa professor que iniciou o processo de orientação conosco: Érika da Costa Bezerra.

A todos aqueles que contribuíram de alguma forma para a realização deste trabalho. A todos que participaram, direta ou indiretamente em seu desenvolvimento, enriquecendo o nosso processo de aprendizado na área tecnológica. Às pessoas com quem convivemos ao longo desses anos de curso que nos incentivaram e certamente tiveram impacto na nossa formação acadêmica.

“A tecnologia *wireless* inovou as formas de comunicações entre as pessoas, gerando necessidade de mais níveis de segurança”

(CARDOSO; SOUZA, 2023)

RESUMO

Compreender a segurança cibernética em redes *wireless* de uma categoria de pessoas que trabalham com *Wi-Fi* para vendas *online* na área tecnológica de redes é relevante para melhorias na comunicação e eficiência dessas redes de computadores, melhorando processos e atendimentos desse público. O objetivo foi criar um guia científico com configurações e fatores infraestruturais em redes de computadores, especificamente da tecnologia WLAN. A justificativa reside nas significativas melhorias para trabalhadores autônomos em termos de segurança cibernética, redução de custos operacionais e oportunidades de negócios. A construção do guia contou com informações técnicas sobre configurações essenciais que os empresários devem implementar em suas redes, tais como senhas robustas, protocolos de segurança atualizados, configurações de firewall e gerenciamento adequado de login/senha do roteador e outros fatores. A metodologia utilizada nesta pesquisa é de natureza aplicada, fornecendo soluções práticas para melhorar a segurança em suas redes WLAN. Para atingir esse objetivo, adotou-se uma abordagem quantitativa, utilizando questionário como principal instrumento de coleta de dados junto aos empresários SOHO. A pesquisa de campo permitiu obter informações numéricas sobre as necessidades e conhecimentos desses empresários em relação à segurança da informação em redes sem fio. Foi desenvolvido um guia a partir dessa pesquisa divulgado para um site, configurado por meio do *software Google Sites* para facilitar o acesso e a navegabilidade. O conteúdo do guia foi estruturado de forma explicativa. Os principais resultados alcançados destacam a identificação das melhores práticas para a configuração *Wi-Fi*.

Palavras-chave: segurança cibernética; redes SOHO; tecnologia *Wireless*.

ABSTRACT

Understanding cybersecurity in *wireless* networks for a category of people who work with *Wi-Fi* for online sales in the network technology area is relevant for improvements in communication and efficiency of these computer networks, improving processes and services for this audience. The objective was to create a scientific guide with configurations and infrastructure factors in computer networks, specifically WLAN technology. The justification lies in improvements for self-employed workers in terms of cybersecurity, reduced operational costs and business opportunities. The guide's construction contains technical information on essential configurations that business owners should implement on their networks, such as strong passwords, updated security protocols, firewall configurations, proper router login/password management, and other factors. The methodology used in this research is applied in nature, providing practical solutions to improve security in your WLAN networks. To achieve this objective, we present a quantitative approach, using a questionnaire as the main data collection instrument from SOHO entrepreneurs. A field survey made it possible to obtain numerical information about the needs and knowledge of these entrepreneurs in relation to information security in *wireless* networks. A guide was developed based on this published research for a website, configured using *Google Sites software* to facilitate access and navigation. The content of the guide was structured in an explanatory manner. The main results obtained highlight the identification of best practices for *Wi-Fi* configuration.

Keywords: cyber security; SOHO networks; *Wireless* technology.

.

SUMÁRIO

1 INTRODUÇÃO

Atualmente, a segurança cibernética é uma necessidade imputada pelo desenvolvimento tecnológico. Para tornar nítido o entendimento dessa necessidade Grohmann (2023) representante da Empresa *Check Point Research* fornecedora de inteligência líder em ameaças cibernéticas, revela alguns dados do crescimento alarmante de ataques cibernéticos no Brasil em 2023. No segundo trimestre de 2023, 1.258 ataques cibernéticos por semana são enfrentados por organizações em média. Esse número representa um aumento significativo em comparação com o período correspondente em 2022. Essa estatística ressalta a persistência e a frequência das ameaças cibernéticas, destacando a necessidade crítica de medidas robustas de cibersegurança.

Outros setores que enfrentam a constante dessa problemática são: o Setor de Educação/Pesquisa com a maior média de ataques (2.179 por semana, queda de 6% em relação a 2022). Setor Governo/Militar como o segundo mais visado (1.772 ataques por semana, aumento de 9%). Setor de Saúde com aumento significativo de 30% (1.744 ataques por semana), (CHECK POINT RESEARCH, 2023).

Neste cenário Costa (2023) faz alguns apontamentos a respeito da importância da Segurança Cibernática. A interseção entre as transformações tecnológicas, a LGPD e os riscos cibernéticos em ambientes SOHO[1] (*Small Office and Home Office*) é um campo crítico de estudo e ação. Reconhecer a fragilidade de cada elo na corrente empresarial é essencial para fortalecer a resiliência cibernética. O treinamento em segurança cibernética e a conscientização dos colaboradores são medidas cruciais, enquanto a proteção de dados pessoais e profissionais assume uma relevância cada vez maior.

A motivação desta está relacionada à área tecnológica em redes de computadores, englobam fatores, como: impactar significativamente a maneira como as pessoas se conectam e interagem umas com as outras, levando a avanços em áreas como a comunicação no campo dos negócios potenciais do público pesquisado. Ainda, espera-se melhorar a eficiência das redes de computadores, permitindo uma comunicação mais rápida e eficiente entre os dispositivos. Podendo melhorar a utilização dos recursos de rede e reduzir custos operacionais.

No campo pessoal, a motivação é para compartilhar conhecimentos utilitário para as pessoal que trabalham de casa com vendas *online*. Com isso, compartilhar conhecimentos

[1] O termo 'SOHO' Refere-se a uma categoria de empresários que trabalham de escritórios em casa, autônomos, ainda qualquer pessoa que se utiliza de redes *Wi-Fi* para desenvolver atividades de vendas *online.*

científicos relacionados ao campo de redes de computadores é uma forma de empoderar pequenos empresários e ajudá-los a inovar em sua infraestrutura corporativa. Além disso, ao compartilhar conhecimentos sobre redes de computadores, contribui-se para o desenvolvimento de uma sociedade mais conectada e tecnologicamente avançada.

O problema de pesquisa é como contribuir com conhecimentos técnicos de configurações e fatores infraestruturais em redes de computadores relacionados a tecnologia *wireless* para segurança em ambientes SOHO?. Ainda, foi formulada a seguinte hipótese: O público não sabe como configurar sua rede *Wi-Fi* para aumentar a segurança contra ameaças virtuais.

O objetivo geral da pesquisa é criar um guia para divulgação em um site contendo configurações e fatores infraestruturais em redes de computadores relacionados a tecnologia *wireless* para pequenos escritórios. Com isso, se estipulou os seguintes objetivos específicos: (1) Desenvolver um site pelo *software Google Sites*; (2) Compreender as necessidades de segurança cibernética; (3) Disponibilizar um guia que auxilie pequenos empresários no entendimento de requisitos de segurança e proteção relacionado a tecnologia *wireless*. Portanto, a pesquisa foi desenvolvida tendo tais objetivos como delimitadores.

A justificativa compreende melhorias significativas para categoria de empresários autônomos em segurança cibernética, redução de custos operacionais, novas formas de comunicação para negócios potenciais de pessoal que trabalham de casa. Afinal de contas, vulnerabilidades na conexão de rede aumentam o risco da entrada de invasores. Com isso, a construção de um guia se direciona às configurações essenciais que a categoria de trabalhadores individuais devem estar atentos. São configurações relacionadas a senha de rede, os protocolos de segurança que prezam pela segurança da rede *Wi-Fi* que sejam atualizados, as configurações para um *firewall* é excelente barreira contra ações intrusivas, configurações relacionadas ao *login* e senha do roteador, atualização do *firmware* do roteador e a desativação do SSID. Assim, apenas pessoas autorizadas devem ter acesso para a realização de qualquer tipo de alteração nesse sentido, minimizando a ação de pessoas mal intencionadas, capaz de trazer prejuízos bastante significativos.

Portanto, suprir as necessidade das pessoas que fazem vendas de casa em relação a informações técnicas relacionadas a configurações da tecnologia *wireless* atendendo aos requisitos de segurança, pois trabalha com informações que devem ser protegidas no tráfego de informações contribui na proliferação de boas práticas em segurança da informação explorando os principais pilares para a consolidação de uma rede segura, sendo menos propensa a invasões cibernéticas como ataques *hackers*.

Além desta seção introdutória o presente trabalho está dividido da seguinte maneira:

Na seção 2, a literatura especializada em redes de computadores ressalta a significativa relevância da tecnologia *wireless* utilizada em escritórios residenciais. Na seção 2.1, são discutidos os ativos em sistemas de informações, incluindo *hardware*, *software*, dados, pessoas e procedimentos. Na seção 2.2, são apresentados os princípios fundamentais de segurança da informação aplicados infraestrutura de redes residenciais. Na seção 2.3, aborda-se a relevância dos equipamentos de redes sem-fio. Na seção 2.4, são discutidos os fatores infraestruturais em redes *Wi-Fi*, incluindo os padrões IEEE 802.11, tipos de enlace em redes WLAN, e a importância da infraestrutura bem elaborada para evitar interferências de sinal. Na última seção 2.5, trata-se das configurações e medidas de segurança de pequenas redes. Subsequentemente, a metodologia da pesquisa é detalhada na Seção 3, se atendo a sua classificação e delimitação. Após apresenta-se os resultados e discussões mais relevantes da pesquisa referente as configurações trabalhadas em laboratório. E, ao final estão as considerações finais a respeito dos principais aprendizados adquiridos no processo de pesquisa.

2 LITERATURA EM REDES DE COMPUTADORES

A literatura em redes de computadores destaca a importância da tecnologia *wireless*, mas também enfatiza a necessidade de medidas de segurança e configuração adequada para garantir um desempenho confiável dessa rede. Portando, tratar a segurança e proteção da informação é o ponto de partida no processo para melhorar as redes *wireless* e o fio condutor nessa discussão são os ativos de sistemas de informação.

2.1 Ativos em sistemas de informações

Silva e Pinto (2019), explicam como as micro e pequenas empresas enfrentam diversos problemas de gestão em seus ambientes organizacionais, entre eles a falta de especialização e a falta de informação sobre as boas práticas na gestão da tecnologia da informação, com isso, a gestão de ativos é suscitada na pauta de seu trabalho.

Concorda-se com Silva e Pinto (2019); Ghem (2019); ABNT NBR ISO/IEC 27001:2013; e Gil (2008) que a informação deve ser tratada como um ativo das empresas pela gestão, por ter esse nível de classificação, tem grande valor para as instituições. Seu gerenciamento é vital e muito importante para o sucesso e manutenção de qualquer organização, com isso, os ativos em sistemas de informação são os recursos e elementos que uma organização usa para criar, armazenar, processar, transmitir e proteger informações importantes para suas operações de negócios.

Kurose e Ross (2021) afirmam que o gerenciamento de rede contém a disponibilização, integração e a coordenação de elementos de *hardware*, *software* e humanos para monitorar, consultar, configurar e controlar os recursos da rede e seus elementos. Essa coordenação de recursos serve para manter e garantir as segurança e proteção de informações confidenciais nas empresas.

Castilho et al. (2014) destacam a importância da documentação dos ativos de rede para a manutenção das atividades e sucesso dos negócios. Manter registros desses ativos é fundamental para facilitar e conservar os processos que melhoraram ou não foram úteis na resolução de problemas envolvendo a segurança no ambiente ou infraestrutura da empresa, evitando e minimizando a ocorrência de falhas de segurança.

Sêmola (2014, p. 43-44) define um ativo como “todo elemento que compõe os processos que manipulam e processam a informação”. Segundo este autor, o ativo é um elemento de valor para um indivíduo ou organização e como tal deve ser protegido. Para Galvão (2015), ativo

pode ser entendido como “[...] qualquer parte que componha a estrutura de uma organização [...]”. Um ativo é, portanto, qualquer elemento que represente valor para a empresa.

Silva e Pinto (2019) e Amaral (2016) interpretam que no contexto de uma rede de computadores de uma empresa, os ativos de rede integram um conjunto de dispositivos e suas informações relacionadas que permitem a operacionalização dos negócios da organização. Esses ativos podem incluir o *hardware* que são dispositivos físicos, como computadores, servidores, roteadores, *switches*, dispositivos de armazenamento, impressoras, *scanners*, entre outros, usados para armazenar e processar informações. Amaral (2016) entende que os *software*s são programas de computador que ajudam a realizar tarefas específicas, como processamento de texto, planilhas, bancos de dados, sistemas de gestão de conteúdo, entre outros.

Ativos também podem ser identificados como sendo dados, incluindo informações que são armazenadas e processadas pelos sistemas de informação, como informações de clientes, registros financeiros, documentos de negócios, registros de vendas, entre outros. Amaral (2016) enfatiza que nas camadas de redes cada uma provê um nível de serviço e faz interface com duas camadas, trocando dados entre elas, nesse fluxo existe a rede que é uma infraestrutura que conecta dispositivos de *hardware* e *software* em uma organização, permitindo a comunicação e a transferência de informações entre eles.

As pessoas são ativos também, como funcionários, usuários e outros indivíduos que acessam, gerenciam ou usam sistemas de informação em uma organização. Menezes, Cardoso e Rocha (2015), explica que as informações devem ser concentradas em um grupo de pessoas capacitadas para garantir a proteção das informações. Consonante a essa ideia, os ativos apresentam-se como procedimentos, sendo as políticas e práticas que orientam o uso de sistemas de informação, incluindo políticas de segurança, procedimentos de *backup*, procedimentos de recuperação de desastres, entre outros.

Portanto, todos esses ativos são importantes para o bom funcionamento dos sistemas de informação de uma organização e devem ser gerenciados e protegidos adequadamente para garantir a segurança e integridade das informações, sem desconsiderar sua multiplicidade na organização que como foi verificado podem ser *hardware* e *software*, registros e documentações de processos, banco de dados, recursos humanos e as políticas de uma organização.

2.2 Princípios de segurança da informação

Os ambientes de negócios autônomos muitas vezes possuem limitações de recursos e orçamentos para segurança da informação. No entanto, é importante implementar alguns princípios básicos de segurança da informação para proteger dados e informações confidenciais.

Souza (2018) e Figueiredo (2015), entende que redes de pequenos escritórios também são alvos de ataques cibernéticos. A conscientização para investimentos de prevenção muitas vezes é difícil de ser aceita pelos gestores ou usuários, o que pode acarretar a perda de dados e consequentemente, perdas financeiras. Nakamura e Geus (2007), inferem que no âmbito de segurança, todos os agentes envolvidos estão em constante evolução. A ação de novos tipos de ataques tem como reação medidas de prevenção, que levam ao desenvolvimento de novas técnicas de ataques, formando um ciclo ininterrupto. Assim, no mundo da informação, a segurança deve ser contínua e prover aperfeiçoamento para novos tipos de ameaças. Ademais, os princípios de segurança da informação são um conjunto de diretrizes que orientam as boas práticas para proteger a informação e garantir sua integridade, confidencialidade e disponibilidade. A Confidencialidade visa garantir que apenas pessoas autorizadas tenham acesso à informação. Para isso, é necessário implementar medidas de segurança, como criptografia, controles de acesso e autenticação de usuários, (GONÇALVES, 2015).

A integridade refere-se à proteção da informação contra alterações não autorizadas. Para garantir a integridade dos dados, é necessário implementar controles de versão, *backups* regulares e procedimentos de monitoramento, (GONÇALVES, 2015). A violação da integridade pode levar a consequências graves, como perda de dados, informações imprecisas ou danificadas e problemas legais. Além disso, é importante educar os usuários sobre práticas de segurança adequadas, como evitar o *download* de *software* suspeito e manter seus dispositivos atualizados com as últimas correções de segurança. A garantia da integridade dos dados é fundamental para proteger as redes contra perda de dados, roubo de informações e danos à reputação. Portanto, a implementação de medidas de segurança para garantir a integridade dos dados deve ser uma das principais prioridades para proprietários de redes WLAN.

A disponibilidade refere-se à garantia de que a informação estará disponível quando necessário. Para isso, é indispensável implementar medidas de redundância e *backup* para garantir que os sistemas estejam sempre disponíveis, (BRANCO; CARVALHO; BARRERO et al., 2023), (GONÇALVES, 2015). Ainda, implementar controles de segurança que permitam verificar a autenticidade dos dados, como assinaturas digitais, (VIANA; DATTEN; SILVA et al., 2022).

O princípio da disponibilidade é importante já que redes sem-fio geralmente têm poucos recursos e uma infraestrutura mais simples em comparação com redes corporativas maiores. Em uma rede utilizada para vendas digitais, a disponibilidade dos recursos de informação, como arquivos e aplicativos, pode ser crítica para a operação do negócio ou para a produtividade do usuário. Por exemplo, se um arquivo importante não estiver disponível quando necessário, isso pode atrasar a conclusão de uma tarefa importante ou até mesmo prejudicar um negócio.

O não-repúdio é o princípio que se refere à garantia de que uma pessoa ou organização não possa negar a autoria de uma ação ou transação. Para isso, é necessário implementar medidas de autenticação forte e rastreamento de atividades, (VIANA, et al., 2022). O não-repúdio é particularmente importante para transações financeiras e contratos digitais, que são comuns em muitas empresas de empreendedor individual. Por exemplo, se um usuário desse enviar um e-mail com um contrato digital anexado, é importante garantir que o usuário não possa negar ter enviado o e-mail ou assinado o contrato posteriormente. Para garantir a não-repúdio nessas redes, é necessário utilizar tecnologias que permitam o registro e a autenticação de todas as transações, como assinaturas digitais e sistemas de registro de auditoria. Isso pode ajudar a garantir que todas as transações sejam registradas e autenticadas, de modo que as partes envolvidas não possam negar ter realizado a ação posteriormente. O princípio do mínimo privilégio estabelece que os usuários devem ter apenas o acesso mínimo necessário para realizar suas atividades. Isso reduz o risco de acesso indevido a informações confidenciais e minimiza o impacto de uma violação de segurança, (SIX, 2012).

Assim, esses princípios são fundamentais para garantir a segurança da informação e devem ser aplicados em todas as fases do ciclo de vida da informação, desde a coleta até a exclusão, para assim garantir a confidencialidade, disponibilidade, não-repúdio, integridade e o mínimo privilégio nas redes WLAN. É importante lembrar que a segurança da rede é um processo contínuo e que deve ser revisado e atualizado regularmente para proteger a rede contra as ameaças em constante evolução independentemente do porte empresarial.

2.3 Segurança dos equipamentos em redes sem-fio

A relevância dos equipamentos de redes sem-fio é um tema de estudo abordado por diversos autores, pois proporciona conexão sem fio para diversos dispositivo, facilitando a criação de redes locais eficientes.

Pinheiro (2011) e Tanenbaum, Feamster e Wetherall (2003), enfatizam que os equipamentos de redes wireless têm uma grande relevância, isso é válido para contexto de

vendas digitais, pois permitem a conexão sem fio de diversos dispositivos, como laptops, smartphones, tablets, smart TVs e outros dispositivos inteligentes, em uma rede local. Isso permite que esses dispositivos possam compartilhar recursos e se comunicar entre si, bem como acessar a internet. No trabalho com vendas pela internet, muitas vezes não há a necessidade de uma infraestrutura de rede cabeados complexa, pois isso pode ser caro e difícil de implementar.

Mayer e Neto (2014), abordam sobre a importância dos equipamentos de redes, sendo fundamental para garantir a eficiência, disponibilidade e segurança dos serviços oferecidos pelas empresas. Os equipamentos de rede são responsáveis por conectar dispositivos, compartilhar recursos, transmitir dados e permitir a comunicação entre usuários em uma rede. Porém, a ocorrência de falhas pode causar impactos significativos, levando à interrupção do serviço e à perda de dados críticos.

Kurose e Ross (2021), ressaltam a importância da segurança nas redes de computadores, protegendo o tráfego de informações e garantindo confiança nos sistemas computacionais. A redundância é apontada como uma técnica para aumentar a disponibilidade e a confiabilidade da rede, seja através de dispositivos redundantes, redundância de links ou redundância de serviços.

A segurança do fornecimento de energia também é abordada, com a utilização de fontes de alimentação ininterrupta (UPS) e geradores para garantir a continuidade do fornecimento de energia. O monitoramento de energia é mencionado como uma medida importante para identificar o consumo de energia, detectar problemas e tomar medidas preventivas. No geral, a atenção à segurança e ao monitoramento dos equipamentos é essencial para garantir o bom funcionamento da redes residenciais.

Portanto, a capacidade de oferecer conexões sem fio para uma variedade de dispositivos, possibilitando a criação de redes locais eficientes é crucial para a interconectividade e compartilhamento de recursos nesse contexto. A flexibilidade proporcionada pelos equipamentos de redes sem fio elimina a necessidade de complexas infraestruturas cabeadas, tornando a implementação mais acessível.

2.4 Fatores infraestruturais em redes *wireless*

Destaca-se percepções importante referente aos fatores infraestruturais em redes *wireless*, apresentadas nas principais ideias de alguns autores. Para Gast (2005), o padrão IEEE 802.11 pode ser referenciado por vários nomes como: Ethernet sem fio, justificando a ligação direta com o padrão de rede com fio IEEE 802.3. O nome *Wi-Fi* é definido pela organização

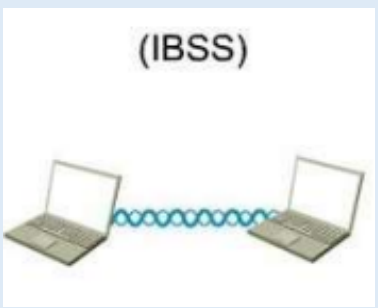
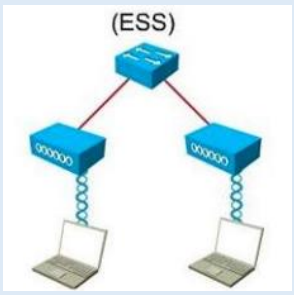
Wi-Fi Alliance a partir do programa de certificação de interoperabilidade de produtos que utilizam as referências desse padrão. É também é referenciado como WLAN.

Pinheiro (2011) e Paz, Daniel, Maran et. al. (2015) e Zampar (2022), expandem a compreensão das redes sem fio, destacando os diferentes padrões, como 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, *Wi-Fi* 6 e *Wi-Fi* 6E, cada um com suas características e velocidades de transmissão. Além disso, aborda as formas de enlace em redes *Wi-Fi* como IBSS (*Ad-Hoc*), BSS (*Basic Service Set*) e ESS (*Extended Service Set*), e discute a importância do ponto de acesso (AP) para estabelecer conexões sem fio. No que se refere à interferência na infraestrutura de fotorreceptores, Freitas (2020) destaca a importância de infraestruturas bem elaboradas para evitar problemas de interferência no sinal *Wi-Fi*, citando interferências eletromagnéticas e outras redes sem fio como possíveis problemas.

Para garantir a qualidade do sinal de redes de pequenos escritórios, são apresentadas medidas como escolher frequências menos congestionadas, posicionar o roteador centralmente e livre de obstáculos, configurar corretamente a rede e manter os dispositivos atualizados. Assim, uma infraestrutura adequada é crucial para garantir um desempenho confiável e consistente das redes sem fio, bem como, a implementação de medidas adequadas pode minimizar interferências e garantir uma conexão estável e rápida para os usuários.

Cada geração de tecnologia *Wi-Fi* representa um avanço em relação à anterior, oferecendo maior velocidade, alcance e eficiência em ambientes com muitos dispositivos conectados. Nessa discursiva não podemos deixar de assimilar a arquitetura das WLAN, as formas dos elementos se comunicarem e trocarem informações em uma infraestrutura sem-fio podem variar em diferentes arquiteturas. As 3 principais formas para um enlace são: IBSS (*Independent Basic Service Set*), também referenciada com Ad-Hoc. BSS (*Basic Service Set*). e ESS (*Extended Service Set*), (PINHEIRO, 2011).

Quadro 1 - Principais formas de enlace em redes WLAN

Para o enlace BSS, existe a necessidade de um equipamento concentrador, um ponto de acesso ou AP (Access Point). Também chamada de rede infraestruturada, os elementos móveis participantes dessa rede devem se conectara ao elemento AP que está em seu raio de alcance. Atuando como um elemento de camada 1 (Física) do modelo OSI, o AP é semelhante ao Hub em uma rede cabeada, recebe o sinal de um dispositivo e propaga o para todos os elementos de sua área de cobertura em busca do receptor. Essa característica já demonstra uma vulnerabilidade dos ambientes Wi-Fi. Onde todos os dispositivos participantes daquela rede pode receber a comunicação uns dos outros mesmo não sendo o nó receptor da transmissão.	Para a arquitetura BSS, o AP pode atuar como uma ponte (bridge) entre a rede LAN e a WLAN. Dessa forma os equipamentos móveis (Wi-Fi) e fixo (Ethernet) pode se comunicar, formando uma mesma rede lógica. Mas um ponto de vulnerabilidade pode observado nessa ligação do mundo com e sem fio. Essa característica permite promover acesso de um dispositivo móvel sem fio a uma rede física.	As redes BSS são limitadas a um único elemento concentrador. Para resolver essa limitação, o enlace ESS estende o crescimento de uma WLAN através da ligação de várias BSS`s, possibilitando maior abrangência e área cobertura. Nesse cenário de múltiplas BSS, o protocolo WDS (Wireless Distribution System) compartilha as informações entre os AP`s, dando possibilidade de os dispositivos trocarem de BSS sem desconectar-se e possibilitado a criação de várias células para atendimento de grandes áreas geográficas como: universidades, fábricas, parques, praças, shoppings e até pequenas cidades.

Fonte: Pinheiro (2011).

Em consonância com os conceitos de Freitas (2020), é nítido o motivo de se ter uma infraestrutura elaborada estrategicamente para evitar problemas de interferência no sinal *Wi-Fi* é extremamente relevante para garantir um desempenho confiável e consistente da rede sem fio. A interferência pode causar quedas na conexão, diminuição da velocidade da Internet e até mesmo desconexões frequentes. Vieira et al. (2020) chama atenção a respeito da comunicação sem fio, bem como, a questão de se tratar da qualidade evitando falhas e ruídos.

Assim, com essas medidas é possível minimizar as interferências na infraestrutura de fotorreceptores e garantir a qualidade do sinal *wireless*. Portanto, uma infraestrutura elaborada estrategicamente para evitar problemas de interferência no sinal *Wi-Fi* é crucial para garantir um desempenho confiável e consistente da rede sem fio. A implementação de medidas adequadas pode ajudar a minimizar a interferência e garantir uma conexão estável e rápida para os usuários.

2.5 Configurações *wireless* para pequenos escritórios

Adiante, busca-se simplificar as configurações e medidas de segurança para redes sem-fio. Os autores López, Monroy e Murcia (2018), Moreno, palacios e Trujillo (2015), enfatizam a importância da criptografia de dados, especialmente com protocolos WPA2 ou superiores, para garantir a segurança da rede. Através do Quadro 2, é explicado um procedimento para configurar a criptografia WPA2 em um roteador genérico.

Quadro 2 - Configurações de criptografia / senhas fortes

1. Acesse o painel de administração do seu roteador sem fio: abra um navegador da web e digite o endereço IP do seu roteador sem fio na barra de endereços. O endereço IP padrão para a maioria dos roteadores é 192.168.1.1, mas pode ser diferente para o seu modelo específico. Consulte o manual do usuário do roteador para obter o endereço IP correto.
2. Faça login no painel de administração: insira seu nome de usuário e senha para acessar o painel de administração. Se você ainda não alterou as informações de login padrão, elas podem ser encontradas no manual do usuário do roteador.
3. Encontre a seção de configuração de segurança: procure por uma seção no painel de administração que permita configurar as opções de segurança da rede sem fio. Dependendo do modelo do roteador, essa seção pode ser chamada de "Configurações sem fio", "Segurança", "Opções de segurança sem fio", entre outros.
4. Selecione WPA2 como método de criptografia: dentro da seção de configuração de segurança, selecione "WPA2" como método de criptografia. Algumas opções de roteadores podem incluir WPA2-PSK (Pre-Shared Key), WPA2-Enterprise, ou uma combinação de ambas.
5. Configure a chave de criptografia: insira uma chave de criptografia segura na seção correspondente. A chave de criptografia é a senha que os usuários precisarão digitar para se conectar à rede sem fio. Use uma senha forte com pelo menos oito caracteres que inclua uma combinação de letras, números e símbolos.
6. Salve as alterações: após configurar a criptografia WPA2 e a chave de criptografia, clique em "Salvar" ou "Aplicar" para salvar as alterações e sair do painel de administração.

Fonte: Cardoso e Souza, 2023.

Além disso, é ressalta-se o uso do aplicativo "Password Generator" para gerar senhas fortes e seguras, o que ajuda a proteger a rede contra invasões e ataques cibernéticos (Quadro 3).

Quadro 3 - Aplicativo gerador de senhas fortes

1. Baixe e instale o aplicativo "Password Generator" em seu dispositivo móvel ou computador. O aplicativo está disponível para iOS, Android, Windows e Mac.
2. Abra o aplicativo e selecione "Gerador de Senhas" na página inicial.
3. Escolha a força da senha que deseja gerar: escolha entre "Fácil", "Médio" ou "Difícil". A opção "Difícil" é a mais recomendada para redes wireless.
4. Personalize as opções de senha: você pode escolher o comprimento da senha, incluir ou excluir caracteres especiais, números e letras maiúsculas e minúsculas.
5. Clique em "Gerar senha" e uma senha forte será gerada automaticamente.
6. Copie a senha gerada e cole-a na seção de configuração de segurança do painel de administração do seu roteador sem fio.
7. Salve as alterações e teste a nova senha para garantir que ela esteja funcionando corretamente.

Fonte: Souza, 2023.

Os autores Moreno, Palacios e Trujillo (2015) defendem a configuração das redes WLAN com base nos procedimentos dos Quadros 1 e 2, destacando a eficiência dessas medidas. E, apresenta-se a importância da atualização de *firmware* para corrigir vulnerabilidades de segurança conhecidas nos roteadores *wireless* (Quadro 4).

Quadro 4 - Atualização do *firmware* do roteador

1. Preparação:

- Verifique o modelo do roteador e a versão atual do firmware. Isso geralmente pode ser encontrado no painel de administração do roteador ou no manual do usuário.
- Certifique-se de ter uma conexão estável à internet e, de preferência, conecte-se ao roteador via cabo Ethernet.
- Faça backup das configurações do roteador, caso seja necessário reconfigurá-lo após a atualização.

2. Download:

- Acesse o site do fabricante do roteador e navegue até a página de suporte e downloads.
- Localize a seção de firmware e procure a versão mais recente disponível para o seu modelo de roteador.
- Faça o download do arquivo do firmware em seu computador.

3. **Instalação:**

- Acesse o painel de administração do roteador digitando o endereço IP do roteador na barra de endereço do navegador. O endereço IP padrão varia de acordo com o fabricante do roteador, mas geralmente é 192.168.0.1 ou 192.168.1.1.
- Faça login no painel de administração do roteador com o nome de usuário e senha padrão ou os detalhes de login personalizados.
- Navegue até a seção de firmware ou atualização de software e faça o upload do arquivo do firmware que você baixou anteriormente.
- Aguarde o processo de atualização ser concluído. O roteador pode reiniciar automaticamente durante o processo.
- Após a atualização ser concluída, faça login novamente no painel de administração do roteador e verifique se todas as configurações foram mantidas e se o firmware foi atualizado com sucesso.

Fonte: Cardoso e Souza, 2023.

A filtragem de endereços MAC é discutida como uma camada adicional de segurança (Quadro 5), mas alerta-se que não é uma solução infalível.

Quadro 5 - Configurações de restrições de acesso por filtragem MAC

1. Acesse o painel de administração do seu roteador sem fio: abra um navegador da web e digite o endereço IP do seu roteador sem fio na barra de endereços. O endereço IP padrão para a maioria dos roteadores é 192.168.1.1, mas pode ser diferente para o seu modelo específico. Consulte o manual do usuário do roteador para obter o endereço IP correto.
2. Faça login no painel de administração: insira seu nome de usuário e senha para acessar o painel de administração. Se você ainda não alterou as informações de login padrão, elas podem ser encontradas no manual do usuário do roteador.
3. Encontre a seção de configuração de segurança: procure por uma seção no painel de administração que permita configurar as opções de segurança da rede sem fio. Dependendo do modelo do roteador, essa seção pode ser chamada de "Configurações sem fio", "Segurança", "Opções de segurança sem fio", entre outros.
4. Ative a filtragem de endereços MAC: encontre a opção de filtragem de endereços MAC na seção de configuração de segurança e ative-a. A filtragem de endereços MAC permite que você restrinja o acesso à sua rede sem fio para dispositivos específicos.
5. Encontre o endereço MAC do dispositivo que deseja permitir ou bloquear: em cada dispositivo que deseja permitir ou bloquear, localize o endereço MAC. O endereço MAC é um código exclusivo atribuído a cada dispositivo de rede sem fio. O endereço MAC pode ser encontrado nas configurações de rede do dispositivo.
6. Adicione o endereço MAC à lista de acesso: volte para o painel de administração do roteador sem fio e adicione o endereço MAC do dispositivo à lista de acesso. Se você deseja permitir o acesso, adicione o endereço MAC à lista de permissões. Se você deseja bloquear o acesso, adicione o endereço MAC à lista de proibições.
7. Salve as alterações: após adicionar o endereço MAC à lista de acesso, clique em "Salvar" ou "Aplicar" para salvar as alterações e sair do painel de administração.
8. Teste a nova configuração: certifique-se de que a nova configuração esteja funcionando corretamente, tentando conectar um dispositivo à rede sem fio que foi adicionado à lista de permissões ou proibições.

Fonte: Cardoso e Souza, 2023.

A ocultação do SSID Broadcast é apresentada como uma medida adicional de segurança para tornar a rede menos visível para hackers (Quadro 6).

Quadro 6 - Configurações para ocultar a rede

1. Acesse o painel de administração do seu roteador sem fio: abra um navegador da web e digite o endereço IP do seu roteador sem fio na barra de endereços. O endereço IP padrão para a maioria dos roteadores é 192.168.1.1, mas pode ser diferente para o seu modelo específico. Consulte o manual do usuário do roteador para obter o endereço IP correto.
2. Faça login no painel de administração: insira seu nome de usuário e senha para acessar o painel de administração. Se você ainda não alterou as informações de login padrão, elas podem ser encontradas no manual do usuário do roteador.
3. Encontre a seção de configuração de segurança: procure por uma seção no painel de administração que permita configurar as opções de segurança da rede sem fio. Dependendo do modelo do roteador, essa seção pode ser chamada de "Configurações sem fio", "Segurança", "Opções de segurança sem fio", entre outros.

4. Desative o SSID Broadcast: encontre a opção "SSID Broadcast" e desative-a. Essa opção pode ser encontrada em diferentes lugares, dependendo do modelo do roteador. Em alguns modelos, ela pode estar localizada na seção de configurações sem fio, enquanto em outros pode estar na seção de rede sem fio avançada.
5. Salve as alterações: após desativar o SSID Broadcast, clique em "Salvar" ou "Aplicar" para salvar as alterações e sair do painel de administração.
6. Reconecte seus dispositivos à rede: após desativar o SSID Broadcast, você precisará reconectar seus dispositivos à rede sem fio manualmente. Eles não aparecerão na lista de redes disponíveis, portanto, você precisará adicionar manualmente o nome da rede (SSID) e a senha para se conectar à rede sem fio.

Fonte: Cardoso e Souza, 2023.

A configuração de firewall para bloquear determinados sites com base nas políticas da organização é descrita no (Quadro 7).

Quadro 7 - Configurações de filtragem URL

1. O processo para ativar a filtragem de URL na interface do roteador pode variar um pouco dependendo do modelo do seu roteador, mas geralmente segue os seguintes passos:
2. Conecte-se à interface do seu roteador. Para isso, abra um navegador e digite o endereço IP do roteador na barra de endereços. O endereço IP padrão pode ser encontrado no manual do usuário do roteador ou na parte inferior do dispositivo.
3. Faça login na interface do roteador com suas credenciais de administrador. Se você nunca alterou o nome de usuário e senha padrão, eles devem estar impressos no manual do usuário.
4. Procure pela seção de configurações de segurança ou controle dos pais. As opções podem variar dependendo do modelo do roteador.
5. Ative a filtragem de URL. Normalmente, isso envolve marcar uma caixa de seleção para habilitar a filtragem de URL e, em seguida, inserir uma lista de URLs que deseja bloquear.
6. Salve as configurações do roteador. Depois de fazer as alterações necessárias, clique no botão "Salvar" ou "Aplicar" na interface do roteador para salvar as novas configurações.
7. Reinicie o roteador. Algumas alterações de configuração podem exigir que o roteador seja reiniciado antes de entrar em vigor. Verifique se as instruções específicas são fornecidas no manual do usuário.

Fonte: Cardoso e Souza, 2023.

Por fim, a configuração do controle de potência do sinal *Wi-Fi* como uma forma de limitar o alcance do sinal e evitar acesso não autorizado está no (Quadro 7). O controle de potência pode afetar o desempenho da rede e a vida útil do dispositivo, portanto, é importante ajustar a potência de transmissão de forma adequada. Além disso, com uma rede bem configurada e níveis diferentes de segurança evita acesso não autorizado. Assim, a segurança da rede é um processo contínuo, devendo ser revisado e atualizado regularmente para proteção adequada dos dados e informações transmitidos pela rede.

Quadro 8 - Configurações de controle do potência do sinal *Wi-Fi*

1. Acesse as configurações do roteador: Conecte-se ao roteador usando um cabo de rede ou um dispositivo conectado à rede. Abra um navegador da web e insira o endereço IP do roteador na barra de endereço. Insira o nome de usuário e a senha para acessar as configurações do roteador.
2. Localize as configurações sem fio: As configurações sem fio geralmente estão localizadas em um menu de configurações separado. Procure por um menu de "Wireless" ou "Wi-Fi".
3. Ative o controle de potência: Procure por uma opção de "Potência de Transmissão" ou "Transmit Power". Ative essa opção para permitir o controle de potência. Em alguns roteadores, você pode ajustar a potência de transmissão em um intervalo de 1-100%, enquanto outros podem ter configurações mais específicas.
4. Ajuste a potência de transmissão: Ajuste a potência de transmissão de acordo com as necessidades da sua rede. Se a rede cobre uma área pequena, reduzir a potência de transmissão pode economizar energia e reduzir interferências. Se a rede cobre uma área grande ou tem muitos obstáculos, aumentar a potência de transmissão pode melhorar o alcance e a qualidade do sinal.

5. Salve as alterações: Depois de fazer as alterações, clique em "Salvar" ou "Aplicar" para salvar as alterações e sair do menu de configurações sem fio.

Fonte: Souza, 2023.

Verifica-se assim, a importância da configuração de redes *wireless* para garantir a segurança dessas redes sem-fio. Diversas medidas são apresentadas para fortalecer a segurança, incluindo a criptografia de dados, especificamente a importância do protocolo WPA2 ou superior para proteger as informações transmitidas e a necessidade de usar senhas fortes. Também são discutidos procedimentos detalhados para configurar criptografia, restrição de acesso, ocultação de SSID, atualização de *firmware* e controle de potência do sinal *Wi-Fi*. A filtragem URL é introduzida como uma forma de aplicar políticas de acesso à internet. Enfatiza-se que essas medidas devem ser adotadas em conjunto para garantir a segurança efetiva da rede, visto que nenhuma medida isolada é infalível. A ideia central é que uma configuração adequada e múltiplas camadas de segurança são essenciais para proteger dispositivos e dados, contribuindo para a integridade e privacidade das redes de pequenos escritórios.

3 METODOLOGIA

A pesquisa está classificada da seguinte forma: a natureza é aplicada, a abordagem do problema é quantitativa, os objetivos têm enforque explicativo, e seus procedimentos técnicos compreendem a pesquisa de campo em laboratório com aplicação de questionário e a partir dos dados compilou-se os requisitos para divulgação do guia em site desenvolvido pelo Google Sites. A pesquisa aplicada tem por foco a busca por soluções práticas para problemas específicos, (FLEURY, 2016). A pesquisa teve seu projeto cadastrado na Plataforma Brasil intitulado 'A Tecnologia *Wireless* para Ambiente SOHO. E parte que envolve seres humanos não apresentou riscos a integridade física dos participantes conforme legislação vigente.

O objetivo foi aplicar os conhecimentos teóricos na área de segurança cibernética em redes sem-fio para desenvolver um guia funcional e útil, com orientações claras para aprimorar a segurança das redes *wireless*. Optou-se por uma abordagem quantitativa para a coleta e análise de dados em nossa pesquisa. Utilizando questionário estruturado como instrumento de coleta de dados, aplicados a um grupo representativo (21 vinte e um) de empresários SOHO do estado do Amapá e do estado do Pará.

Para alcançar todos os objetivos, a pesquisa de campo foi necessária, com a coleta direta de dados junto ao público-alvo. Utilizando o laboratório de redes de IFAP e um roteador, aplicou-se as configurações específicas e relevantes para o desenvolvimento do guia. O guia resultante desta pesquisa foi divulgado em um site configurado por meio do *software Google Sites* para garantir fácil acesso e navegabilidade.

O Guia SOHO apresenta informações técnicas aprofundadas com linguagem acessível ao público específico, bem como, configurações e medidas essenciais para proteger a rede sem-fio. O conteúdo tem forma clara e didática, visando facilitar o entendimento dos empresários sobre a importância da segurança de suas redes e como implementar as práticas recomendadas. Os dados da pesquisa foram tratados de maneira cuidadosa e sistemática. As respostas do questionário quantitativo foram registradas em uma planilha do Excel, permitindo uma organização eficiente dos dados.

Foram realizadas verificações para identificar e corrigir erros, valores atípicos e respostas incompletas. Em seguida, foram calculadas estatísticas descritivas para cada pergunta, proporcionando uma visão geral dos dados coletados. Gráficos foram utilizados para visualizar padrões e correlações nos resultados. Os dados foram apresentados em um relatório claro e conciso, destacando as principais conclusões e suas implicações para a segurança em redes de pequenos escritórios. No processo de desenvolvimento do site pensou-se em elementos da

interface para o usuário, sendo esses elementos: as guias, compostas por 4 (quatro) abas básicas: Home; Sobre os autores; Contato e Download. E, incorporou-se a licença Creative Commons.

Quadro 9 - Principais especificações do roteador utilizado no laboratório de redes

D-Link DIR-809 roteador sem fio Fast Ethernet Dual-band (2,4 GHz / 5 GHz) 4G Preto	
Conexão WAN	**Networking**
Ethernet WAN	Tipo de interface Ethernet LAN: Fast Ethernet
Recursos LAN wireless	Taxas de dados Ethernet LAN: 10, 100 Mbit/s
Banda Wi-Fi: Dual band (2,4 GHz / 5 GHz)	Tecnologia de cabeamento: 10/100Base-T(X)
Padrão Wi-Fi: 802.11ad	Padrões de rede: IEEE 802.11a, IEEE 802.11ac, IEEE
Padrões de Wi-Fi: Wi-Fi 5 (802.11ac), 802.11ad,	802.11ad, IEEE 802.11az, IEEE 802.11b, IEEE
802.11b, 802.11g, Wi-Fi 4 (802.11n)	802.11g, IEEE 802.11n
Networking	**Segurança**
Ethernet LAN	Algoritmos de segurança: WPA, WPA2, WPS

Fonte: Google, 2023.

Após a aplicação das configurações sobre a tecnologia *wireless* no roteador do laboratório do Instituto Federal do Amapá – IFAP, as quais foram selecionadas e organizadas em forma de roteiro, se obteve as evidências registradas por print, assim foi possível materializar o esboço pensado inicialmente. Na sequência o guia foi organizado e criado pelo Power Point 2019 e disponibilizado em PDF para o público pesquisado no site (https://sites.google.com/view/projetoifap/home).

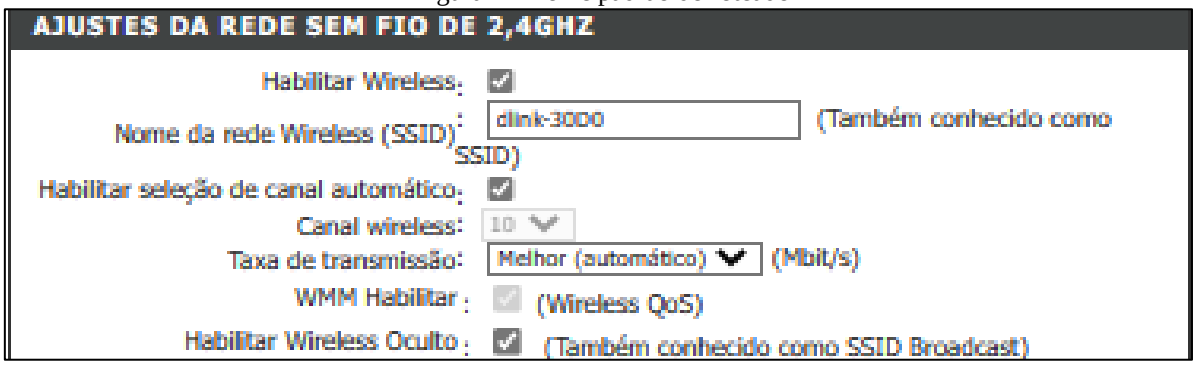
O Guia SOHO foi desenvolvido exclusivamente para dispositivos da marca D-Link devido à disponibilidade limitada de equipamentos para avaliação. Optou-se por focar nos produtos da D-Link como uma base representativa que pode ser útil como referência para outros dispositivos no mercado. Com base na pesquisa realizada sobre configurações e fatores infraestruturais em redes de computadores relacionados à tecnologia sem-fio, estudos futuros podem envolver a necessidade de desenvolver ferramentas de gerenciamento de segurança específicas de trabalhos autônomos, visando simplificar a implementação de medidas de segurança, e a importância de realizar estudos de caso em empresas reais para avaliar empiricamente o impacto das configurações de segurança propostas.

4 RESULTADOS E DISCUSSÃO

4.1 Resultados obtidos na pesquisa em laboratório

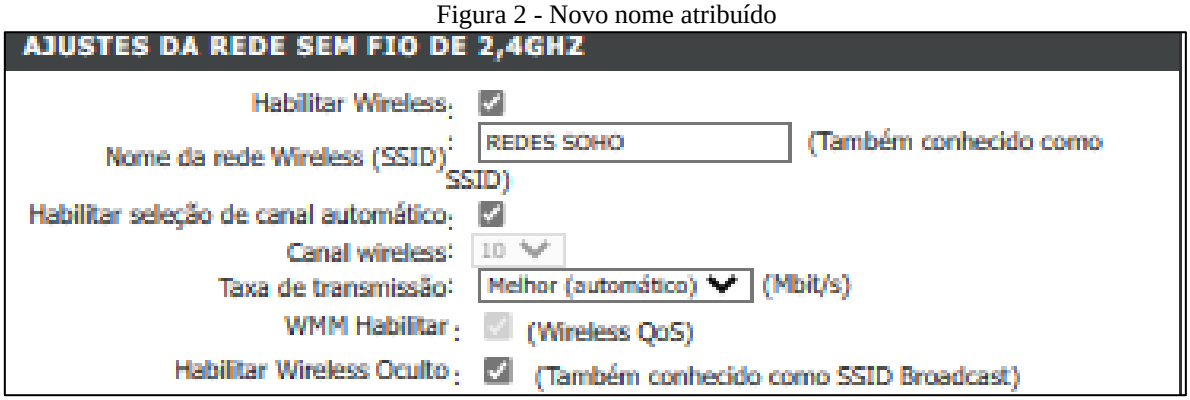
A criptografia de dados é importante para configurar a rede *wireless* de preferência com protocolos WPA2 ou superior, para garantir que as informações transmitidas pela rede estejam protegidas contra interceptação e acesso não autorizado. Depois de acessar o painel de administração mudou-se o nome padrão do SSID da rede:

Figura 1 - Nome padrão do roteador



Fonte: Souza; Cardoso, 2023.

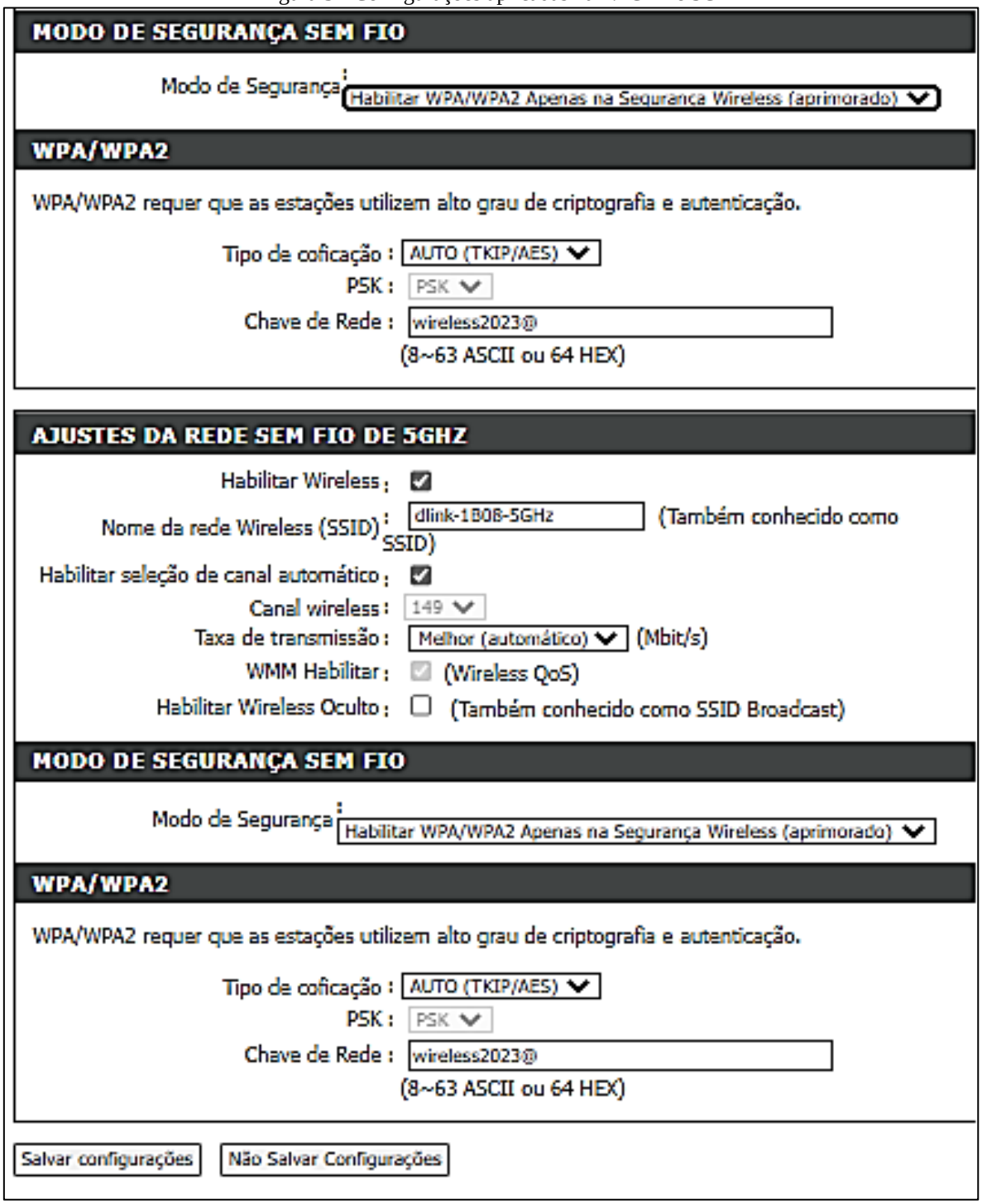
Figura 2 - Novo nome atribuído



Fonte: Souza; Cardoso, 2023.

A chave de criptografia é a senha que os usuários precisarão digitar para se conectar à rede sem fio. A senha forte deve ter pelo menos oito caracteres que inclua uma combinação de letras, números e símbolos. Após configurar a criptografia WPA2 e a chave de criptografia, clicou-se em "Salvar Configurações" para salvar as alterações e sair do painel de administração, (Figura 3).

Figura 3 - Configurações aplicadas na 2.4GHz e 5GHz

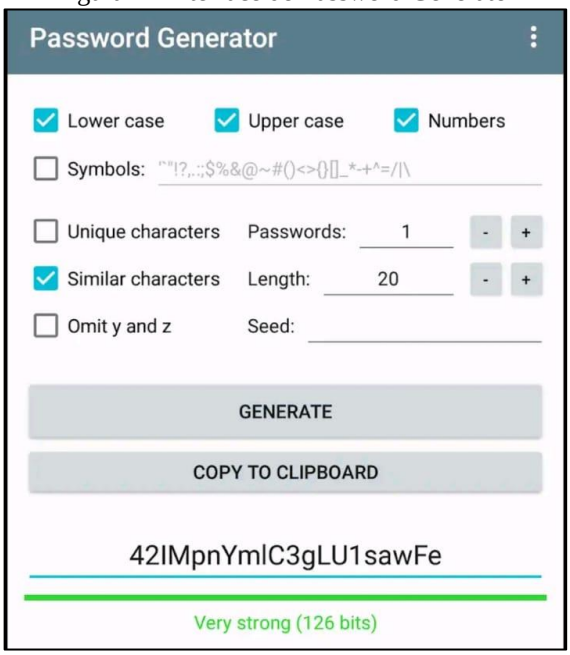


Fonte: Souza; Cardoso, 2023.

4.1.2 Senhas fortes

O aplicativo ‘Password Generator’ é disponibilizado na Play Store, como ele pode-se escolher o comprimento da senha, incluir ou excluir caracteres especiais, números e letras maiúsculas e minúsculas.

Figura 4 - Interface do Password Generator

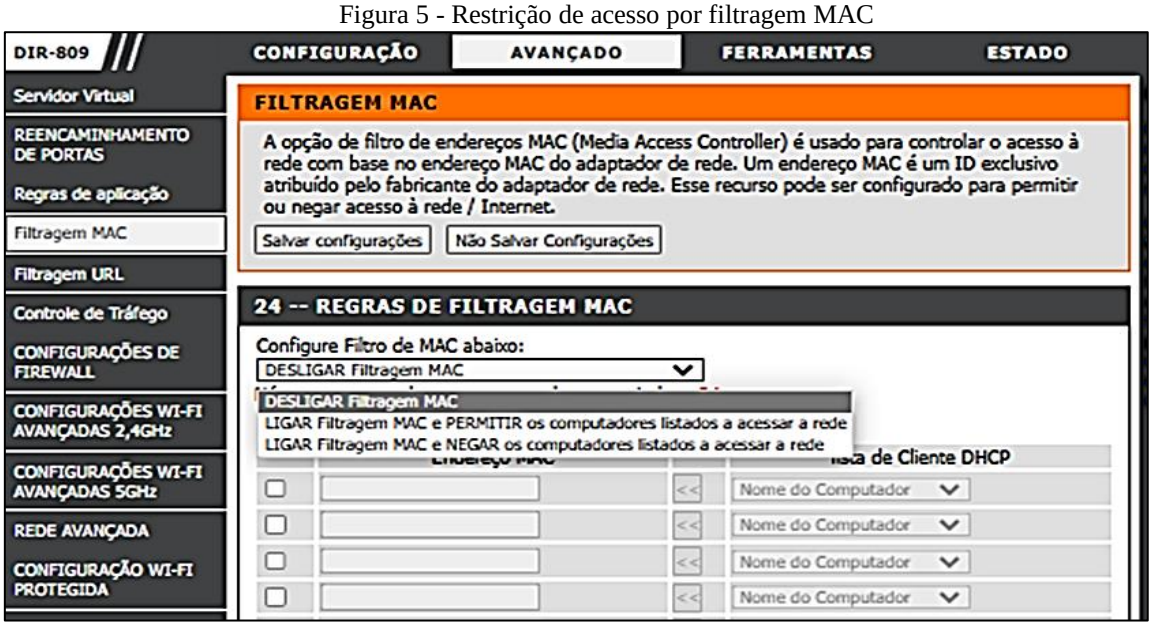


Fonte: Souza; Cardoso, 2023.

4.1.3 Restrições de acesso

Uma configuração interessante é a restrição do acesso à rede *wireless* apenas aos dispositivos autorizados e conhecidos. É possível fazer isso utilizando filtragem de endereços MAC, que permite configurar a rede para permitir apenas dispositivos com endereços MAC específicos.

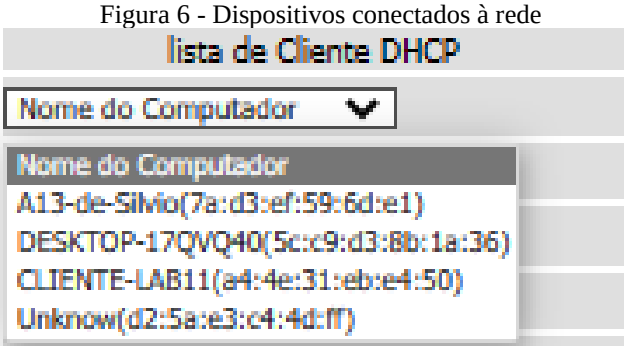
Figura 5 - Restrição de acesso por filtragem MAC



Fonte: Souza; Cardoso, 2023.

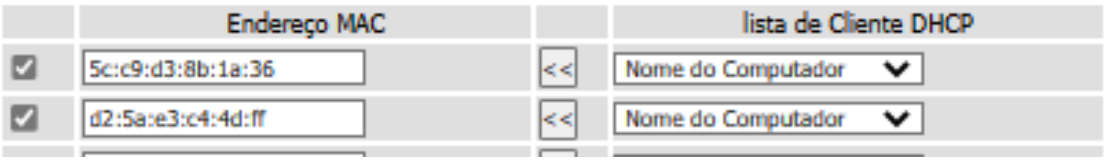
Ao habilitar a ‘Filtragem MAC’ pode-se fazer esta configuração de duas maneiras. Inserir o MAC manualmente (Figura 7), no campo em branco de endereço MAC ou colocar os aparelhos que estão conectados na rede pela lista de Cliente DHCP (Figura 6), basta ir à opção ‘Nome do Computador’ onde irá aparecer a lista de dispositivos conectados, após isso clique em sobre o aparelho deseja bloquear ou conceder permissão.

Figura 6 - Dispositivos conectados à rede



Fonte: Souza; Cardoso, 2023.

Figura 7 - Dispositivos selecionados



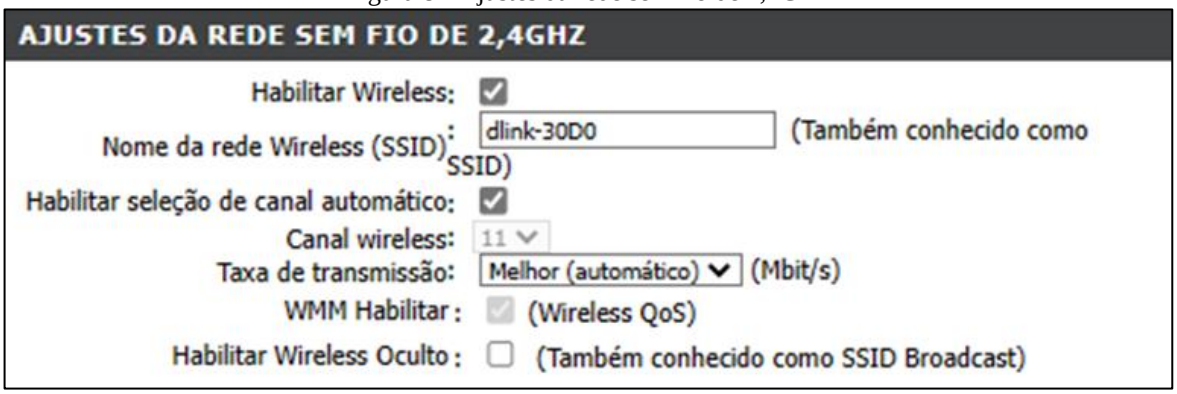
Fonte: Souza; Cardoso, 2023.

Após salvar as configurações os dispositivos que foram selecionados só poderão acessar a rede, e outros não selecionados ficaram sem acesso a rede, ou caso contrário, se negados os dispositivos que foram selecionados automaticamente perdem o acesso à rede.

4.1.4 Desativar o SSID Broadcast / SSID Oculto

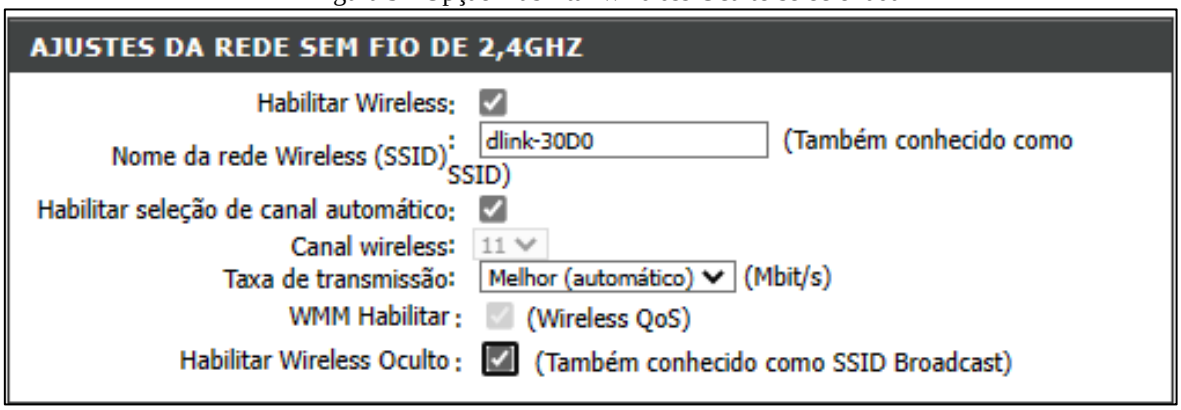
Quando o roteador transmite o nome da rede (SSID) publicamente, ele pode ser facilmente encontrado por pessoas mal-intencionadas. Desativar o SSID Broadcast torna a rede menos visível para hackers. No roteador, na aba de configuração em ‘Ajustes da rede sem fio de 2,5GHz e na 5GHz’ seleciona-se a opção ‘Habilitar Wireless Oculto’ e salva-se tal configuração, (Figura 8 e 9). Após a rede ser reiniciada a nome da rede torna-se oculto. Após aplicadas as configurações os dados da rede devem ser informados manualmente, sendo ‘SSID’ e ‘Senha’, (Figura 10).

Figura 8 - Ajustes da rede sem fio de 2,4GHz



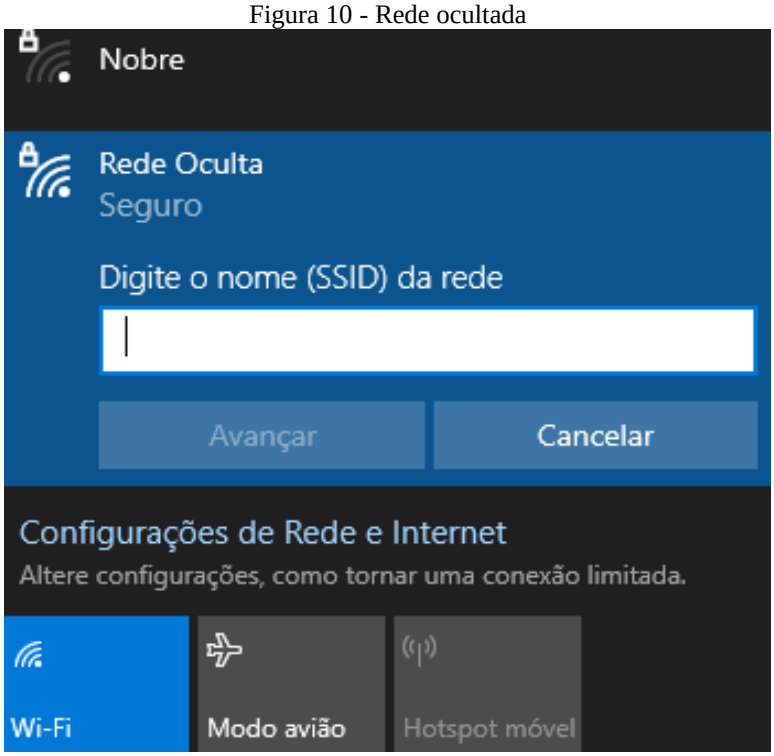
Fonte: Souza; Cardoso, 2023.

Figura 9 - Opção Habilitar *Wireless* Oculto selecionada



Fonte: Souza; Cardoso, 2023.

Figura 10 - Rede ocultada

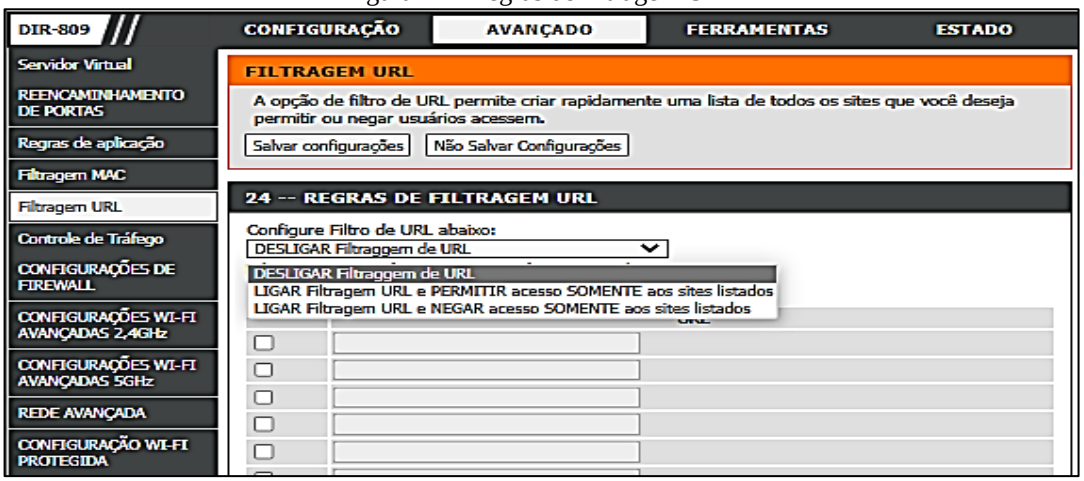


Fonte: Souza; Cardoso, 2023.

4.1.5 Filtragem URL

A filtragem de URL em um roteador é uma função que permite controlar o acesso a determinados sites ou categorias de sites na rede. Essa função é útil para restringir o acesso a conteúdo inadequado ou indesejado, como sites de jogos, redes sociais ou pornografia. É importante ressaltar que a filtragem URL não é uma solução perfeita e pode ter algumas limitações, mas é uma camada de segurança para bloquear sites indesejados. Alguns sites legítimos podem ser erroneamente bloqueados e alguns sites maliciosos podem não ser detectados. Além disso, é possível contornar a filtragem URL usando técnicas como a utilização de VPNs ou proxies. Na aba ‘Avançado’ em Filtragem URL são realizadas as configurações, nesse caso, colocando os sites que desejasse bloquear nos espaços em brancos e seleciona a opção ‘LIGAR Filtragem URL e NEGAR acesso SOMENTE aos sites listados’ (Figura 11 e 12) e basta salvar e reiniciar a interface.

Figura 11 - Regras de filtragem URL



Fonte: Souza; Cardoso, 2023.

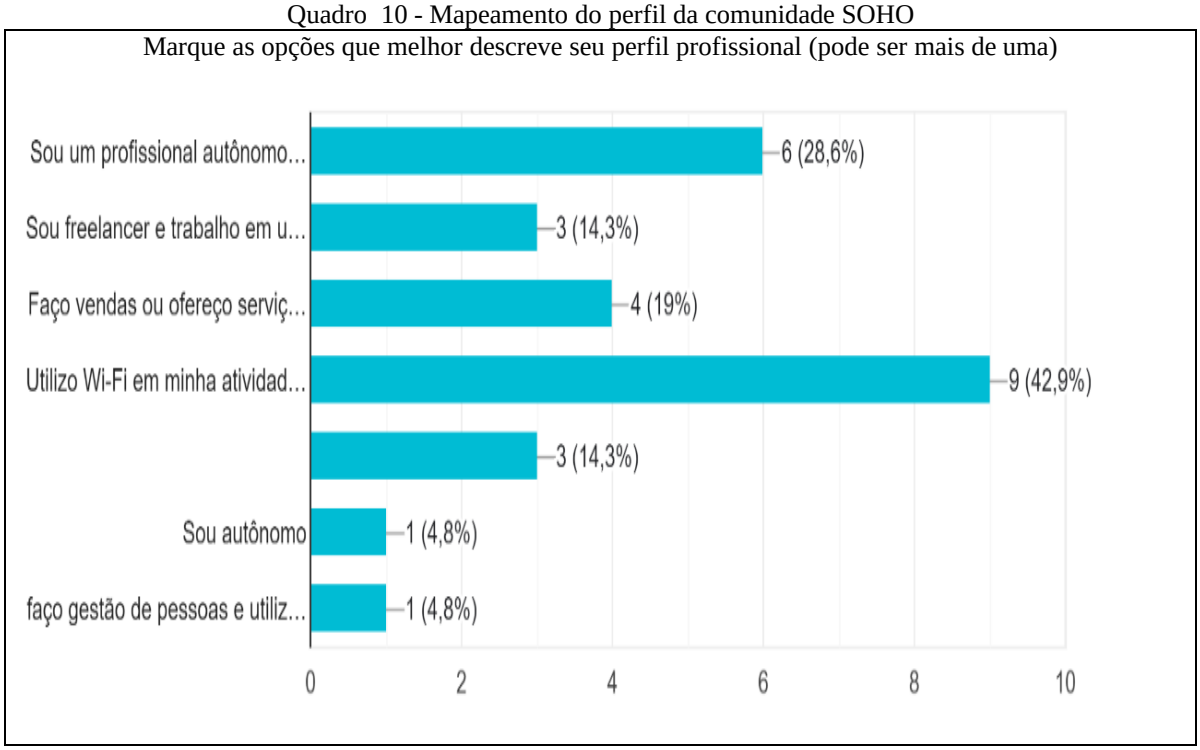
Figura 12 - Regras criadas

Fonte: Souza; Cardoso, 2023.

4.4 Pesquisa de campo – questionário

Nesta parte, apresenta-se um mapeamento do perfil do público pesquisado (Quadro 10). Após se apresenta uma síntese dos dados dos resultados estatísticos obtidos da nossa pesquisa com a aplicação do questionário.

Quadro 10 - Mapeamento do perfil da comunidade SOHO



Fonte: Cardoso e Souza, 2023.

O Quadro 10 mostra que a pesquisa de campo foi realizada com um total de 21 participantes que responderam a um questionário sobre a tecnologia *wireless*. As respostas revelaram uma variedade de perfis profissionais e uso do *Wi-Fi* em suas atividades. Profissionais autônomos com empresa MEI: 28,6% (6 respostas).

Esses participantes são profissionais autônomos que possuem uma empresa como Microempreendedor Individual (MEI). Eles utilizam a tecnologia *wireless* em suas atividades profissionais. Freelancers que trabalham em escritório em suas residências: 14,3% (3 respostas). Esses participantes são freelancers que realizam seu trabalho em um escritório localizado em suas residências.

Eles também utilizam a tecnologia *wireless* em suas atividades profissionais. Vendas ou serviços online: 19% (4 respostas). Esses participantes estão envolvidos em atividades de vendas ou prestação de serviços ao público de forma online. Eles dependem do *Wi-Fi* para realizar suas transações comerciais.

Utilização do *Wi-Fi* em atividades profissionais: 42,9% (9 respostas). Esses participantes utilizam o *Wi-Fi* em suas atividades profissionais, embora não tenha sido especificado o tipo de atividade em que estão envolvidos. Além desses perfis principais, houve algumas respostas adicionais que representaram uma parcela menor do público: Profissionais autônomos: 4,8% (1 resposta).

Essa resposta indica que o participante é um profissional autônomo, mas não foram fornecidos detalhes adicionais sobre sua atividade específica. Gestão de pessoas e comunicação por *Wi-Fi*: 4,8% (1 resposta). Essa resposta indica que o participante está envolvido na gestão de pessoas e utiliza o *Wi-Fi* para se comunicar com elas. Outro: 14,3% (3 respostas). Essas respostas não se enquadram em nenhuma das categorias anteriores, mas fornecem uma perspectiva adicional sobre o uso da tecnologia *wireless*.

Quadro 11 - Campo de atuação da comunidade SOHO

Qual o Ramo que você atua e a quanto tempo?
21 Respostas
R1 = Vendas de plantas há cinco anos; R2 = Uma lojinha de variedades, trabalho já tem 3 anos; R3 = Construção civil , 10 anos; R4 = Educacional / 4 anos; R5 = sou líder de negócio natura, já trabalho a quase a 1 ano; R6 = Restaurante, faz 6 anos; R7 = Cosméticos perfumaria e lingerie a mais de 3 anos; R8 = Entregador de delivery; R9 = Vendas de comida, 2 anos; R10 = Restaurante, 9 anos; R11 = Cestas de café 8 anos; R12 = Sou empreendedor; R13 = Pesquisa científica, 4 anos; R14 = IT - 10 anos; R15 = Educadora; R16 = Educadora; R17 = Assessoria e serviços de informática; R18 = Vendas de presentes / 8 anos; R19 = Vendas 2 anos e meio; R20 = IT 10 anos; R21 = Coordenação de polo há 3 anos.

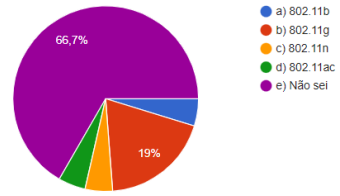
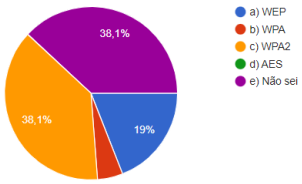
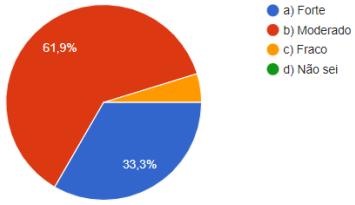
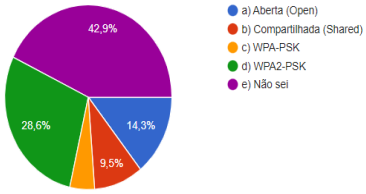
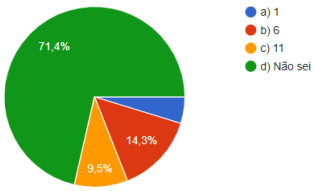
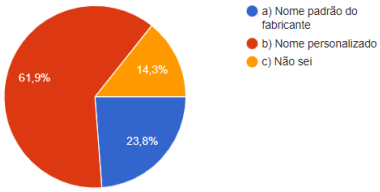
Fonte: Souza, 2023.

O Quadro 11 traz a análise dos dados mostra uma comunidade pesquisada em termos de setores econômicos representados. Essa diversidade reflete uma tendência crescente de empreendedorismo e atividades econômicas realizadas por indivíduos que trabalham em pequenos escritórios domésticos ou em suas próprias residências.

Observa-se que a maioria dos participantes possui experiência considerável em suas áreas de atuação, com um bom número de anos de trabalho acumulados. Isso indica um cenário em que muitos empreendedores e profissionais independentes estão estabelecidos e têm experiência no mercado. Com o aumento do número de dispositivos conectados e a dependência crescente da internet para operações comerciais, a segurança das redes sem fio torna-se uma preocupação crítica.

Adiante, apresenta-se a análise explicativa dos dados obtidos dos resultados do questionário aplicado:

Quadro 12 – 1° conjunto de dados para identificação de lacunas sobre necessidades de segurança Wi-Fi

1) Qual é o padrão de rede sem fio que sua rede utiliza? 	2) Qual é o tipo de criptografia que sua rede sem fio utiliza? 
3) Qual é a força do sinal sem fio na sua rede? 	4) Qual é o tipo de autenticação que sua rede sem fio utiliza? 
5) Qual é o canal sem fio que sua rede utiliza? 	6) Qual é o nome de rede (SSID) da sua rede sem fio? 

Fonte: Cardoso e Souza, 2023.

Quadro 13 – Detalhamento do 1° conjunto de gráficos e primeira conclusão sobre as configurações *Wi-Fi.*

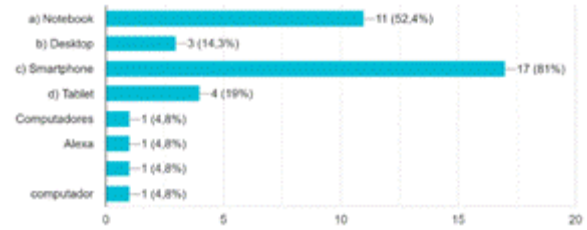
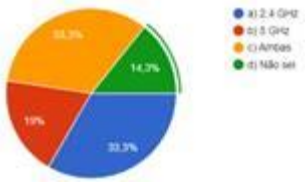
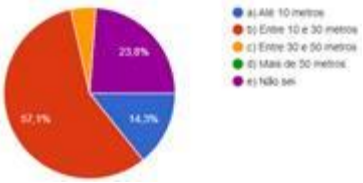
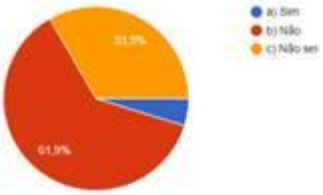
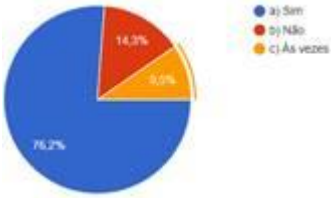
Análise dos dados	
Analisando as respostas obtidas na pesquisa sobre o padrão de rede sem fio utilizado, podemos observar o seguinte:	
> Padrão de Rede sem Fio: 802.11b: Utilizado por 4,8%, é antigo e oferece 11 Mbps. 802.11g: Usado por 19%, oferece 54 Mbps e é compatível com o 802.11b. 802.11n: Utilizado por 4,8%, está sendo substituído por padrões mais recentes. 802.11ac: Usado por 4,8%, oferece altas velocidades, opera em 5 GHz. Não sabe: 66,7% não conhecem o padrão, indicando falta de conhecimento.	**> Tipo de Criptografia:** WEP: 19% utilizam, é considerado inseguro. WPA: 4,8% utilizam, menos seguro que opções recentes. WPA2: 38,1% utilizam, mais seguro que WEP e WPA. AES: Nenhum respondente indicou uso exclusivo. Não sabe: 38,1% não sabem, sugerindo falta de conhecimento.
> Força do Sinal Sem Fio: Forte: 33,3% têm sinal forte. Moderado: 61,9% têm sinal moderado. Fraco: 4,8% têm sinal fraco. Não sabe: Nenhum respondeu "não sabe", indicando conhecimento.	**>Tipo de Autenticação:** Aberta: 14,3% usam autenticação aberta. Compartilhada: 9,5% usam autenticação compartilhada. WPA-PSK: 4,8% usam WPA-PSK. WPA2-PSK: 28,6% usam WPA2-PSK, considerado seguro. Não sabe: 42,9% não sabem, sugerindo falta de conhecimento.
>Canal Sem Fio: Canal 1: 4,8% usam o canal 1. Canal 6: 14,3% usam o canal 6. Canal 11: 9,5% usam o canal 11. Não sabe: 71,4% não sabem, indicando falta de conhecimento.	**>Nome da Rede sem Fio (SSID):** Nome padrão do fabricante: 23,8% usam o padrão do fabricante, menos seguro. Nome personalizado: 61,9% usam um nome personalizado, mais seguro. Não sabe: 14,3% não sabem o SSID, indicando falta de conhecimento.

Fonte: Cardoso e Souza, 2023.

Nos Quadros 12 e 13 a pesquisa revela uma falta de conhecimento e adoção de práticas de segurança em várias áreas relacionadas às redes sem fio, como padrões, criptografia,

autenticação e configuração de canais e SSID. Se faz necessário a conscientização e implementação de medidas de segurança adequadas.

Quadro 14 – 2° conjunto de dados para identificação de lacunas sobre necessidades de segurança *Wi-Fi*

<table>
<tr><td colspan="2">7) Qual é o tipo de dispositivo que você usa para acessar sua rede sem fio?
 
</td></tr>
<tr><td>8) Qual é a largura de banda (banda de frequência) que sua rede sem fio utiliza?
 
</td><td>9) Qual é a distância máxima que você alcança com sua rede sem fio?
 
</td></tr>
<tr><td>10) Você utiliza algum tipo de filtragem de MAC na sua rede sem fio?
 
</td><td>11) Você permite a conexão de convidados em sua rede sem fio?
 
</td></tr>
</table>

Fonte: Cardoso e Souza, 2023.

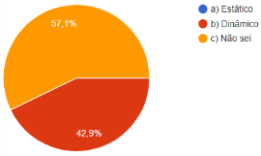
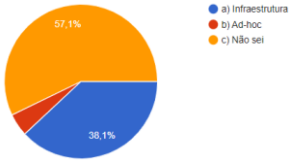
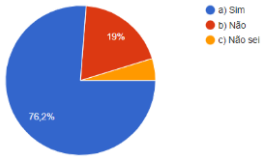
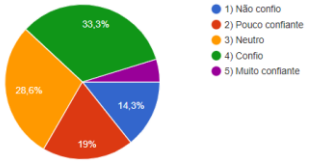
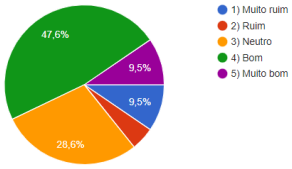
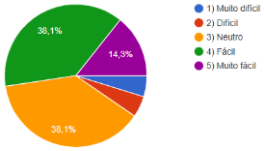
Quadro 15 – Detalhamento do 2° conjunto de gráficos e segunda conclusão sobre as configurações *Wi-Fi.*

> Tipo de Dispositivo Utilizado: - Notebook: Utilizado por 52,4%, comum em ambientes SOHO. - Desktop: Utilizado por 14,3%, menos comum em ambientes móveis. - Smartphone: Utilizado por 81%, dispositivo móvel amplamente adotado. - Tablet: Utilizado por 19%, dispositivo portátil com tela sensível ao toque. - Outro: 14,4% mencionaram dispositivos como a Alexa e o computador.	**> Largura de Banda (Banda de Frequência):** - 2,4 GHz: Utilizada por 33,3%, comum e amplamente suportada. - 5 GHz: Utilizada por 19%, oferece velocidades mais rápidas. - Ambas: 33,3% utilizam ambas as bandas para otimização. - Não sabe: 14,3% não sabem a banda de frequência usada.
> Distância Máxima Alcançada: - Até 10 metros: 14,3% têm alcance limitado. - Entre 10 e 30 metros: 57,1% têm alcance padrão. - Entre 30 e 50 metros: 4,8% têm alcance estendido. - Mais de 50 metros: Nenhum indicou alcance superior a 50 metros. - Não sabe: 23,8% não sabem a distância máxima.	**> Filtragem de MAC:** - Sim: 1% utiliza filtragem de MAC para maior segurança. - Não: 61,9% não utilizam essa medida de segurança. - Não sabe: 61,9% não sabem se utilizam filtragem de MAC.
> Permissão de Conexão de Convidados: - Sim: 76,2% permitem conexão de convidados, visando conveniência. - Não: 14,3% não permitem, priorizando a segurança da rede. - Às vezes: 9,5% permitem em ocasiões específicas, equilibrando conveniência e segurança	

Fonte: Cardoso e Souza, 2023.

A partir dos Quadros 14 e 15 a análise dos dados revela que a maioria dos usuários utiliza dispositivos móveis, como smartphones, para acessar redes sem fio. Além disso, a banda de 2,4 GHz é comum, enquanto a filtragem de MAC não é amplamente adotada. A permissão de conexão de convidados é uma prática comum, apesar dos riscos de segurança associados. Há uma necessidade de conscientização sobre medidas de segurança e configurações de rede para proteger os dados e dispositivos.

Quadro 16 – 3° conjunto de dados e detalhamento de gráficos para identificação de experiência da rede do usuário

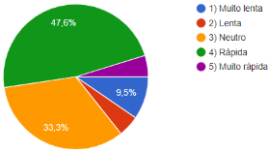
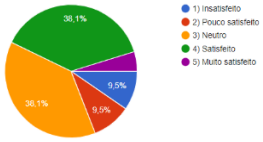
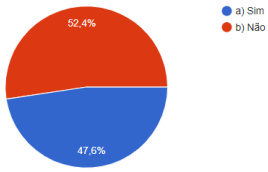
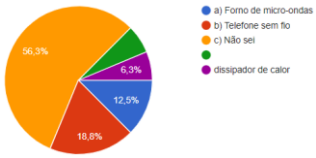
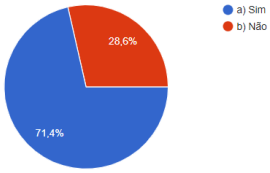
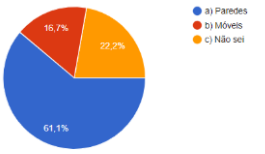
<table>
<tr><td>12) Qual é o tipo de endereço IP que sua rede sem fio utiliza?
 
</td><td>13) Qual é o tipo de rede (infraestrutura ou ad-hoc) que sua rede sem fio utiliza?
 
</td></tr>
<tr><td>14) Você já teve problemas com interferência em sua rede sem fio?
 
</td><td>15) Em uma escala de 1 a 5, qual é a sua confiança na segurança da sua rede sem fio?
 
</td></tr>
<tr><td>16) Em uma escala de 1 a 5, qual é a qualidade do sinal sem fio em sua rede?
 
</td><td>17) Em uma escala de 1 a 5, qual é a facilidade de uso da configuração da sua rede sem fio?
 
</td></tr>
<tr><td>¡>Tipo de Endereço IP:
- A maioria (42,9%) utiliza endereços IP dinâmicos.
- 57,1% não sabem qual tipo de endereço IP sua rede utiliza.
- A escolha entre dinâmico e estático deve considerar as necessidades da rede.</td><td>> Tipo de Rede sem Fio:
- A maioria (38,1%) utiliza o modo infraestrutura.
- Apenas 4,8% utilizam o modo ad-hoc, menos comum em SOHO.
- 57,1% dos participantes não sabem o tipo de rede utilizada.</td></tr>
<tr><td>> Problemas de Interferência:
- 76,2% relataram problemas de interferência em suas redes.
- 19% não tiveram problemas de interferência.
- 4,8% não tinham certeza sobre interferência.</td><td>> Confiança na Segurança:
- 33,3% se sentem confiantes na segurança de suas redes.
- 19% têm pouca confiança, enquanto 14,3% não confiam.
- 28,6% se consideram neutros em relação à segurança.</td></tr>
<tr><td>>Qualidade do Sinal Sem Fio:
- 47,6%, classifica a qualidade do sinal como boa.
- 28,6% a consideraram neutra.
- 9,5% acham que é muito boa, e 9,5% a veem como muito ruim.
- 4,8% a consideram ruim.</td><td>>Facilidade de Configuração:
- 38,1% a consideraram neutra, e 38,1% a acharam fácil.
- 14,3% indicaram que é muito fácil configurar a rede sem fio.
- 4,8% a consideraram muito difícil ou difícil.</td></tr>
</table>

Fonte: Cardoso e Souza, 2023.

O Quadro 16 apresenta resultados que refletem uma variedade de percepções e experiências dos participantes em relação à segurança, qualidade do sinal e facilidade de configuração em redes sem fio. A falta de conhecimento sobre alguns aspectos técnicos destaca

a necessidade de educação e conscientização sobre configurações de rede e práticas de segurança.

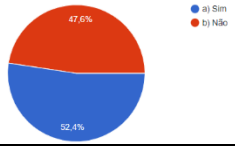
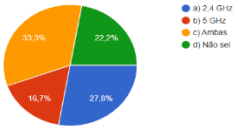
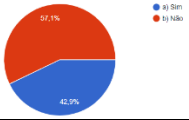
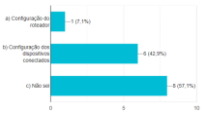
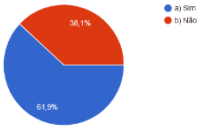
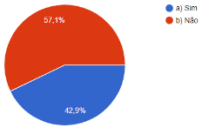
Quadro 17 – 4° conjunto de dados e detalhamento de gráficos para identificação de experiência da rede do usuário

<table>
<tr>
<td>18) Em uma escala de 1 a 5, qual é a velocidade da sua rede sem fio?
 
</td>
<td>19) Em uma escala de 1 a 5, qual é a sua satisfação geral com sua rede sem fio?
 
</td>
</tr>
<tr>
<td>20) Você já teve problemas de interferência eletromagnética em sua rede wireless?
 
</td>
<td>Caso tenha respondido "sim" na pergunta anterior, qual foi a fonte da interferência eletromagnética?
 
</td>
</tr>
<tr>
<td>21) Existem obstáculos físicos que possam afetar a qualidade do sinal da sua rede wireless?
 
</td>
<td>Caso tenha respondido "sim" na pergunta anterior, quais são os obstáculos físicos presentes no ambiente da sua rede wireless?
 
</td>
</tr>
<tr>
<td>> Velocidade da Rede Sem Fio:
- A maioria (47,6%) classificou a velocidade como rápida.
- 33,3% a consideraram neutra.
- 9,5% a acharam muito lenta.
- 4,8% a classificaram como lenta ou muito rápida.
- Destaque para a importância de compreender fatores que afetam a velocidade</td>
<td>> Satisfação Geral com a Rede Sem Fio:
- 38,1% dos participantes estão satisfeitos com suas redes sem fio.
- Outros 38,1% se consideram neutros em relação à satisfação.
- 9,5% expressaram insatisfação ou pouca satisfação.
- Apenas 4,8% estão muito satisfeitos.</td>
</tr>
<tr>
<td>> Interferência Eletromagnética:
- 52,4% relataram problemas de interferência em suas redes.
- Principais fontes de interferência incluem forno de micro-ondas e telefone sem fio.
- 56,3% não sabem a fonte específica de interferência.
- Destaque para a importância de educar sobre identificação e mitigação de interferência.</td>
<td>> Obstáculos Físicos:
- 71,4% mencionaram obstáculos físicos em seus ambientes que afetam o sinal.
- Paredes (61,1%) são o obstáculo mais comum.
- 22,2% não sabem se existem obstáculos físicos.
- Enfatiza a necessidade de conscientização sobre como obstáculos afetam a qualidade do sinal.</td>
</tr>
</table>

Fonte: Cardoso e Souza, 2023.

A análise do Quadro 17 ressalta a complexidade das redes sem fio e a importância de compreender os fatores que influenciam a velocidade, satisfação do usuário, interferência e obstáculos físicos. Fornecer conhecimentos técnicos sobre esses aspectos é fundamental para melhorar a eficácia e a qualidade das redes residenciais.

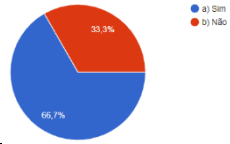
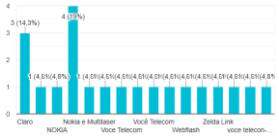
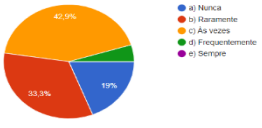
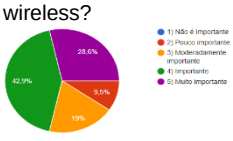
Quadro 18 – 5° conjunto de dados e detalhamento de gráficos sobre fatores da infraestrutura da redes *Wi-Fi*

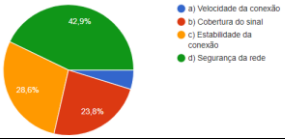
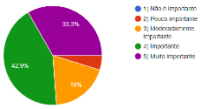
<table>
<tr><td>22) Existem outras redes wireless próximas que possam interferir na sua rede?
  </td><td>Caso tenha respondido "sim" na pergunta anterior, qual é a frequência utilizada por essas outras redes wireless?/
  </td></tr>
<tr><td>23) Você já teve problemas de configuração em sua rede wireless?
  </td><td>Caso tenha respondido "sim" na pergunta anterior, quais foram os problemas de configuração enfrentados?
  </td></tr>
<tr><td>24) Você utiliza um roteador de alta qualidade em sua rede wireless?
  </td><td>25) Você já configurou opções avançadas no seu roteador?
  </td></tr>
<tr><td>> Interferência de Redes Próximas:
- Maioria (52,4%) relatou a presença de outras redes wireless próximas.
- 27,8% operam na frequência de 2,4 GHz.
- 16,7% operam na frequência de 5 GHz.
- 33,3% operam em ambas as frequências.
- 22,2% não sabem a frequência.
- Destaca a necessidade de educar sobre frequências e interferência.</td><td>> Problemas de Configuração:
- 42,9% enfrentaram problemas de configuração em suas redes.
- Problemas de dispositivos conectados foram mencionados por 42,9%.
- Apenas 7,1% tiveram problemas com a configuração do roteador.
- 57,1% não sabem a causa específica dos problemas.
- Reforça a importância de fornecer orientações sobre configuração.</td></tr>
<tr><td>> Utilização de Roteador de Alta Qualidade:
- 61,9% utilizam roteador de alta qualidade.
- 38,1% não utilizam.
- Indica que muitos reconhecem a importância do investimento em roteadores de alta qualidade.</td><td>> Configuração de Opções Avançadas:
- 42,9% configuraram opções avançadas em seus roteadores.
- 57,1% não o fizeram.
- Mostra que uma parcela significativa dos usuários ainda não explorou os recursos avançados de seus roteadores.</td></tr>
</table>

Fonte: Cardoso e Souza, 2023.

Essa análise ao Quadro18, destaca-se a necessidade de educação e orientação técnica para os usuários, especialmente em relação a frequências, configuração de dispositivos e aproveitamento de recursos avançados de roteadores. Isso pode melhorar a eficácia, desempenho e segurança de suas redes *wireless*.

Quadro 19 – 6° conjunto de dados e detalhamento de gráficos sobre fatores da infraestrutura da redes Wi-Fi

<table>
<tr><td>26) Você mantém seus dispositivos atualizados com as últimas atualizações de software e firmware?
  </td><td>27) Qual é a marca e modelo do seu roteador?
  </td></tr>
<tr><td>28) Em sua empresa, a perda de vendas já foi causada por problemas na rede wireless?
  </td><td>29) Em uma escala de 1 a 5, qual é o nível de importância que sua empresa dá para a infraestrutura da rede wireless?
  </td></tr>
</table>

30) Em sua opinião, qual é o fator mais importante para garantir uma boa infraestrutura em uma rede wireless?	31) Em uma escala de 1 a 5, qual é o nível de importância que sua empresa dá para a segurança dos equipamentos de rede?
	
> Atualização de Dispositivos: - Maioria (66,7%) mantém dispositivos atualizados. - 33,3% não realizam atualizações. - Destaca a importância da conscientização sobre a segurança por meio de atualizações.	**> Marcas de Roteadores:** - Nokia e Multilaser mencionadas por 38,2% dos participantes. - Você Telecom mencionada por 24%. - Outras marcas incluem Claro, Q-Link, Webflash, Wi-fi ultra duo e Ótimo. - 4,8% não sabem a marca/modelo do roteador. - Mostra as marcas populares em uso nas redes SOHO.
> Impacto de Problemas na Rede Wireless nas Empresas: - 42,9% relataram que problemas podem causar perda de vendas "Às vezes". - 33,3% disseram "Raramente". - 19% afirmaram "Nunca". - Apenas 4,8% mencionaram "Frequentemente". - Indica a variabilidade na frequência de problemas de rede nas empresas SOHO.	**> Valorização da Infraestrutura de Rede Wireless:** - 42,9% consideram a infraestrutura "Importante". - 28% a veem como "Muito importante". - 19% acham "Moderadamente importante". - 9,5% consideram "Pouco importante". - Nenhum participante disse que não é importante. - Destaca a relevância da infraestrutura de rede nas empresas SOHO.
> Fatores de Importância na Infraestrutura de Rede Wireless: - 42,9% consideram a "Segurança da rede" como o fator mais importante. - 28,6% valorizam a "Estabilidade da conexão". - 23,8% mencionaram "Cobertura do sinal". - Apenas 4,8% consideram "Velocidade da conexão" como o fator mais importante. - Mostra que a segurança é prioridade em ambientes SOHO.	**> Importância da Segurança dos Equipamentos de Rede:** - 42,9% a veem como "Importante". - 33,3% consideram-na "Muito importante". - Reforça a necessidade de educação sobre segurança em equipamentos de rede.

Fonte: Cardoso e Souza, 2023.

O Quadro 19 ressalta a necessidade de conscientização sobre segurança, atualizações de dispositivos, escolha de marcas de qualidade e a importância atribuída à infraestrutura e à segurança em vendas digitais. Educação técnica sobre esses tópicos pode melhorar a eficácia e a segurança das redes sem fio nesses ambientes.

Portanto, ao investir na segurança de suas redes *Wi-Fi*, a comunidade estudada pode colher diversos benefícios econômicos, como:

Ao garantir a segurança das redes *Wi-Fi*, esses empreendedores e profissionais protegem seus próprios dados, bem como os dados de seus clientes. Isso ajuda a evitar violações de segurança, roubo de informações confidenciais e prejuízos financeiros associados.

Uma rede *Wi-Fi* segura e estável é essencial para manter as operações comerciais em funcionamento. Ao evitar interrupções causadas por ataques cibernéticos ou falhas de segurança, podendo-se garantir a continuidade de suas atividades e minimizar perdas financeiras.

Os clientes valorizam a segurança e a privacidade de suas informações. Ao demonstrar um compromisso com a segurança das redes *Wi-Fi*, os empreendedores individuais estabelecem uma reputação de confiança e atraem mais clientes.

A segurança das redes *Wi-Fi* pode ser um diferencial competitivo para os pequenos empresários. Ao destacar-se como um negócio seguro e confiável, eles podem ganhar vantagem em relação à concorrência e conquistar uma fatia maior do mercado. Redes *Wi-Fi* seguras permitem um fluxo de trabalho mais eficiente e ágil.

Enfatiza-se a importância de fornecer informações técnicas sobre as configurações e fatores infraestruturais em redes *wireless* para garantir a segurança. Destaca-se a necessidade de escolher padrões mais recentes e seguros, como o 802.11ac ou o 802.11ax (*Wi-Fi* 6), e adotar protocolos de segurança avançados, como o WPA2 ou o WPA3 em conjunto com criptografia AES.

Também ressalta a influência da força do sinal sem fio e a importância de minimizar obstáculos físicos e interferências para um desempenho adequado da rede. E necessário abordar uma escolha adequada do canal sem fio para evitar interferências e destaca-se a importância de personalizar o nome da rede sem fio (SSID) para aumentar a segurança.

Somente assim será alcançado o objetivo de configurar redes sem fio eficientes e seguras, com orientações claras sobre os protocolos de segurança e práticas de autenticação seguras. A conscientização sobre esses fatores é crucial para evitar vulnerabilidades.

A pesquisa aponta a falta de conhecimento técnico dos usuários SOHO em relação à configuração de suas redes *Wi-Fi* para aumentar a segurança contra ataques cibernéticos. Com isso, a hipótese inicial, de que o público SOHO não sabe configurar suas redes com segurança, foi confirmada pelos resultados que revelaram a falta de conhecimento sobre configurações e medidas de segurança em redes sem fio.

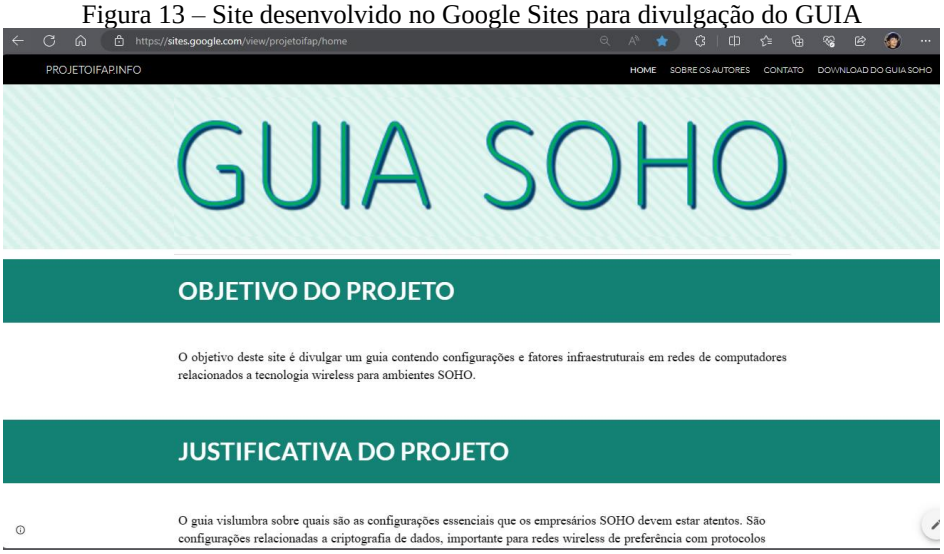
Para refutar a hipótese, seria necessário apresentar resultados que mostrassem que o público pesquisado possui amplo conhecimento e habilidades na configuração de redes *Wi-Fi* para garantir a segurança contra ataques cibernéticos. No entanto, os dados da pesquisa apontam para a necessidade de fornecer informações claras e orientações técnicas sobre configurações de segurança, escolha de protocolos adequados, senhas fortes, criptografia e filtros de MAC para preencher a lacuna de conhecimento identificada.

Portanto, com base nos resultados o Guia SOHO foi construído, mostrando oportunidades para as empresas melhorarem os serviços e aumentarem a satisfação dos clientes em relação às configurações de *Wi-Fi*. Isso inclui informações essenciais sobre a importância das atualizações de *firmware* e *software*, suporte técnico especializado para configurar roteadores e solucionar problemas de segurança e estabilidade, e orientações para melhorar a cobertura do sinal.

4.5 Desenvolvimento do site para divulgação do GUIA

A criação do site "Projetoifap.info" é um exemplo de aplicação da ciência da computação, design web e comunicação digital para alcançar objetivos específicos, como a divulgação e distribuição de informações sobre o projeto chamado "Projeto IFAP."

Figura 13 – Site desenvolvido no Google Sites para divulgação do GUIA



Fonte: Cardoso e Souza, 2023.

A página inicial do site serve como ponto de entrada e apresentação do projeto. Do ponto de vista científico, a *home page* é projetada para atrair a atenção dos visitantes e transmitir informações importantes de maneira eficaz. Os princípios de usabilidade e design são aplicados para garantir que a interface seja amigável e atraente.

A seção ‘sobre os autores’ do projeto na perspectiva científica contribui para estabelecer a credibilidade do projeto ao fornecer informações sobre as pessoas envolvidas. Os princípios de design de perfil, redação e gerenciamento de conteúdo são aplicados para criar perfis informativos e atraentes. A aba de ‘contato’ oferece uma maneira de os visitantes se comunicarem com os responsáveis pelo projeto. Na seção de ‘*download’* os visitantes têm a opção de fazer o download do "GUIA SOHO" gratuitamente. Do ponto de vista científico, isso envolve a implementação de tecnologias de gerenciamento de arquivos, como servidores de arquivos, para disponibilizar o guia para download, portando, utilizou-se o Google Drive.

Assim, a criação do site "Projetoifap.info" envolve a aplicação de princípios científicos em áreas como design de interface, usabilidade, segurança da informação e otimização web. O objetivo é facilitar a disseminação de informações sobre o projeto e permitir a interação eficaz com os visitantes, contribuindo para o sucesso e o impacto do Projeto IFAP.

5 CONSIDERAÇÕES FINAIS

Os clientes estão cada vez mais conscientes da importância da segurança de seus dados pessoais e empresariais, e escolherão empresas que demonstrem um cuidado adequado com a proteção desses dados. Além disso, a reputação de uma empresa em relação à segurança dos dados pode se tornar um diferencial competitivo no mercado. Empresas que investem na segurança de suas redes sem fio e que fornecem orientações e suporte aos seus clientes nessa área podem se destacar como parceiros confiáveis e responsáveis.

Portanto, ao oferecer conhecimentos técnicos de configurações e fatores infraestruturais em redes de computadores relacionados à tecnologia sem fio para segurança cibernética, os pequenos empresários tem a oportunidade de construir uma sólida proteção de dados sensíveis, o que pode resultar em prestígio, confiança e uma vantagem competitiva no mercado. Aprender conhecimentos técnicos de configurações e fatores infraestruturais em redes de computadores relacionados à tecnologia WLAN e sua proteção no meio digital, incluem recursos como configurações de segurança (como criptografia, filtragem de MAC), configurações de qualidade de serviço (QoS) para priorização de tráfego, configurações de rede de convidados, controle parental, redirecionamento de portas, entre outros.

Ao fornecer conhecimentos técnicos sobre essas opções avançadas, os usuários ajuda otimizar o desempenho de sua rede, melhorar a segurança e personalizar as configurações de acordo com suas necessidades individuais. É importante destacar a importância de equilibrar a segurança e o desempenho ao configurar opções avançadas, para evitar configurações incorretas que possam comprometer a estabilidade ou a segurança da rede residencial.

Oferecer um guia e suporte técnico para auxiliar os usuários na configuração das opções avançadas do roteador foi uma estratégia eficaz para promover o conhecimento e a adoção dessas configurações, a pesquisa destacou a importância de conscientizar os usuários sobre a necessidade de manter seus dispositivos atualizados com as últimas atualizações de *software* e *firmware*. Fornecer conhecimentos técnicos sobre como realizar as atualizações e os benefícios associados a elas contribuem significativamente para a proteção das redes de escritórios contra ameaças e vulnerabilidades.

REFERÊNCIAS

AMARAL, A. F. F. **Redes de computadores.** Colatina: Instituto Federal do Espírito Santo, 2012. ISBN: 978-85-62934-35-3.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001.** 20013. Tecnologia da Informação. Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos . Rio de Janeiro, 2013.

BRANCO, L. Y. I.; CARVALHO, P. M.; BARRETO, M. S. **Sistema de monitoramento de fontes redundantes de alimentação para ambientes de missão crítica.** 2022. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/31484. Acesso em: 7 jan. 2023.

CASTILHO, S. D.; MORAES, D. A. S.; VELLOSO, F. L.; OLIVEIRA, W. Sistemas para Documentação de Ativos de Tecnologias da Informação. **Caderno de Estudos Tecnológicos,** v. 01, n. 1, p. 226-237, jul. 2014.

CHECK POINT RESEARCH. **Quem Somo.** 2023. Disponível em: https://research.checkpoint.com/about-us/. Acesso em: 4 set. 2023.

COSTA. T. **Treinamento em segurança cibernética:** por que investir nessa capacitação? 2023. Disponível em: https://niduu.com/blog/treinamento-em-seguran%C3%A7a-cibern%C3%A9tica. Acesso em: 4 set. 2023.

FIGUEIREDO, D. A. **Análise da segurança de redes wi-fi através de teste de penetração em instituições de ensino superior de belo horizonte.** 2015.

FLEURY, M. T. L.; WERLANG, S. R. Pesquisa aplicada: conceitos e abordagens. **Anuário de Pesquisa GVPesquisa,** 2016.

GALVÃO, M. C. **Fundamentos em Segurança da Informação.** São Paulo: Pearson Education do Brasil, 2015.

GAST. M. **Redes sem fio 802.11:** o guia definitivo. 2. ed. O'Reilly, 2005.

GHEM, M. B. Implantação de processo para garantir a recuperação dos principais dados e sistemas de uma PME brasileira após um desastre, minimizando downtime e perda de dados. **Gestão da Segurança da Informação-Unisul Virtual**, 2019. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/3701. Acesso em: 6 jan. 2023.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas, 2008.

GONÇALVES, L. R. O. **Segurança da Informação.** 2015. Disponível em: https://lrodrigo.sgs.lncc.br/wp/wp-content/uploads/2015/10/UCP-Pos-SEG-Legistacao-Aula01-Parte04-NBR-e-Politica-de-Seguranca-2015.10.17-v2-tres-por-folha.pdf. Acesso em: 4 jan. 2023.

GROHMANN, G. **Brasil teve aumento de 7% em ataques cibernéticos no segundo trimestre de 2023. 2023.** Disponível em:

https://mercadoeconsumo.com.br/20/07/2023/tecnologia/brasil-teve-aumento-de-7-em-ataques-ciberneticos-no-segundo-trimestre-de-2023/?cn-reloaded=1. Acesso em: 4 set. 2023.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet:** uma abordagem topdown. 8. ed. São Paulo: Pearson Education do Brasil, 2021.

LÓPEZ, A. A.; MONROY, E. Y. M.; MURCIA, P. A. L. Avaliação de segurança em protocolo de rede sem fio WPA2-PSK usando as ferramentas Linset e Aircrack-ng. **Rev. Fac. ing.** v. 27, n. 47, Jan./Apr. 2018.

MAYER, R.; NETO, M. C. O. P. Uma Revisão de Propostas de Sobrevivência para Redes Multicasting P2P. **CAP Accounting and Management-B4**, v. 7, n. 7, 2014. Disponível em: http://revistas.utfpr.edu.br/pb/index.php/CAP/article/view/1603/1168. Acesso em: 6 jan. 2023.

MENEZES, P. M.; CARDOSO, L. M.; ROCHA, F. G. Segurança em redes de computadores uma visão sobre o processo de Pentest. **Interfaces Científicas-Exatas e Tecnológicas,** v. 1, n. 2, p. 85-96, 2015. Disponível em: https://periodicos.set.edu.br/exatas/article/view/2258/1296. Acesso em: 4 jan. 2023.

MORENO, W. A. M.; PALACIOS, D. J. M.; TRUJILLO, E. R. Vulnerabilidade do protocolo de criptografia WEP, WPA e WPA2 em redes sem fio de plataforma Linux**. Tecnura** v.19, dez, 2015. Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500007&lang=pt. . Acesso em: 30 mar. 2023.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em ambientes cooperativos.** São Paulo: Novatec, 2007.

PAZ, L. F.; DANIEL, R. P.; MARAN, V.; ELLWANGER, C. Um Método para Minimbizar Falhas de Segurança em Redes WLAN 802.11 b/g: controlando acessos provenientes de dispositivos móveis. Frederico Westphalen-RS: **Anais do EATI Ano,** v. 5, p. 39-46, 2015.

PINHEIRO, J. M. S. **Conceitos de redundância e contingência.** 2011.

SÊMOLA, M. **Gestão da Segurança da Informação:** uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SILVA, S. F.; PINTO, J. S. Análise da importância da gestão de ativos de ti no ambiente de micro e pequenas empresas. **Revista científica e-locução,** v. 1, n. 15, p. 18-18, 2019. Disponível em: https://periodicos.faex.edu.br/index.php/e-Locucao/article/view/181. Acesso em: 1 jan. 2023.

SIX, J. **Segurança de aplicativos android.** São Paulo: Novatec, 2012.

SOUZA, G. M. **Implantação de ferramenta livre para controle e segurança de rede local.** 2018. Disponível em: http://repositorio.utfpr.edu.br/jspui/handle/1/25804. Acesso em: 2 jan. 2023.

TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. **Redes de computadores**. 6 ed. Porto Alegre: Bookman, 2022.

VIANA, C. J.; DATTEIN, G. M.; SILVA, J. V. B. G.; CAMPOS, P. K. Criptografia e segurança. **Revista científica e-locução,** v. 1, n. 22, p. 30-30, 2022.

VIEIRA, A. G.; VIEIRA, L. F. M.; VIEIRA, M. A. M. Tamanho Ótimo do Pacote em Comunicação por Luz Visível Sem Fio. In: **Anais do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. SBC,** 2020.

ZAMPAR, D. M. **Wi-fi 6:** estudo do padrão e análise de desempenho. 2022. Disponível em: https://sites.uel.br/dc/wp-content/uploads/2022/09/TCC_DIOGO_MACHADO_ZAMPAR.pdf. Acesso em: 05 out. 2023.

ANEXOS

ANEXO A – Questionário da pesquisa de campo quantitativa

QUESTIONÁRIO – A TECNOLOGIA WIRELESS

1) Qual é o padrão de rede sem fio que sua rede utiliza?
a) 802.11b
b) 802.11g
c) 802.11n
d) 802.11ac
e) Não sei

2) Qual é o tipo de criptografia que sua rede sem fio utiliza?
a) WEP
b) WPA
c) WPA2
d) AES
e) Não sei

3) Qual é a força do sinal sem fio na sua rede?
a) Forte
b) Moderado
c) Fraco
d) Não sei

4) Qual é o tipo de autenticação que sua rede sem fio utiliza?
a) Aberta (Open)
b) Compartilhada (Shared)
c) WPA-PSK
d) WPA2-PSK
e) Não sei

5) Qual é o canal sem fio que sua rede utiliza?
a) 1
b) 6
c) 11
d) Não sei

6) Qual é o nome de rede (SSID) da sua rede sem fio?
a) Nome padrão do fabricante
b) Nome personalizado
c) Não sei

7) Qual é o tipo de dispositivo que você usa para acessar sua rede sem fio?
a) Notebook
b) Desktop
c) Smartphone
d) Tablet
e) Outro

8) Qual é a largura de banda (banda de frequência) que sua rede sem fio utiliza?
a) 2,4 GHz
b) 5 GHz
c) Ambas
d) Não sei

18) Em uma escala de 1 a 5, qual é a velocidade da sua rede sem fio?
1) Muito lenta
2) Lenta
3) Neutro
4) Rápida
5) Muito rápida

19) Em uma escala de 1 a 5, qual é a sua satisfação geral com sua rede sem fio?
1) Insatisfeito
2) Pouco satisfeito
3) Neutro
4) Satisfeito
5) Muito satisfeito

20) Você já teve problemas de interferência eletromagnética em sua rede wireless?
a) Sim
b) Não

Caso tenha respondido "sim" na pergunta anterior, qual foi a fonte da interferência eletromagnética?
a) Forno de micro-ondas
b) Telefone sem fio
c) Outros (especificar)
d) Não sei

21) Existem obstáculos físicos que possam afetar a qualidade do sinal da sua rede wireless?
a) Sim
b) Não

Caso tenha respondido "sim" na pergunta anterior, quais são os obstáculos físicos presentes no ambiente da sua rede wireless?
a) Paredes
b) Móveis
c) Outros (especificar)_____
d) Não sei

22) Existem outras redes wireless próximas que possam interferir na sua rede?
a) Sim
b) Não

Caso tenha respondido "sim" na pergunta anterior, qual é a frequência utilizada por essas outras redes wireless?
a) 2,4 GHz
b) 5 GHz
c) Ambas
d) Não sei

23) Você já teve problemas de configuração em sua rede wireless?
a) Sim
b) Não

9) Qual é a distância máxima que você alcança com sua rede sem fio?
a) Até 10 metros
b) Entre 10 e 30 metros
c) Entre 30 e 50 metros
d) Mais de 50 metros
e) Não sei

10) Você utiliza algum tipo de filtragem de MAC na sua rede sem fio?
a) Sim
b) Não
c) Não sei

11) Você permite a conexão de convidados em sua rede sem fio?
a) Sim
b) Não
c) Às vezes

12) Qual é o tipo de endereço IP que sua rede sem fio utiliza?
a) Estático
b) Dinâmico
c) Não sei

13) Qual é o tipo de rede (infraestrutura ou ad-hoc) que sua rede sem fio utiliza?
a) Infraestrutura
b) Ad-hoc
c) Não sei

14) Você já teve problemas com interferência em sua rede sem fio?
a) Sim
b) Não
c) Não sei

15) Em uma escala de 1 a 5, qual é a sua confiança na segurança da sua rede sem fio?
1) Não confio
2) Pouco confiante
3) Neutro
4) Confio
5) Muito confiante

16) Em uma escala de 1 a 5, qual é a qualidade do sinal sem fio em sua rede?
1) Muito ruim
2) Ruim
3) Neutro
4) Bom
5) Muito bom

17) Em uma escala de 1 a 5, qual é a facilidade de uso da configuração da sua rede sem fio?
1) Muito difícil
2) Difícil
3) Neutro
4) Fácil
5) Muito fácil

Caso tenha respondido "sim" na pergunta anterior, quais foram os problemas de configuração enfrentados?
a) Configuração do roteador
b) Configuração dos dispositivos conectados
c) Outros (especificar)_____
d) Não sei

24) Você utiliza um roteador de alta qualidade em sua rede wireless?
a) Sim
b) Não

25) Você já configurou opções avançadas no seu roteador?
a) Sim
b) Não

26) Você mantém seus dispositivos atualizados com as últimas atualizações de software e firmware?
a) Sim
b) Não

27) Qual é a marca e modelo do seu roteador?
a) _____

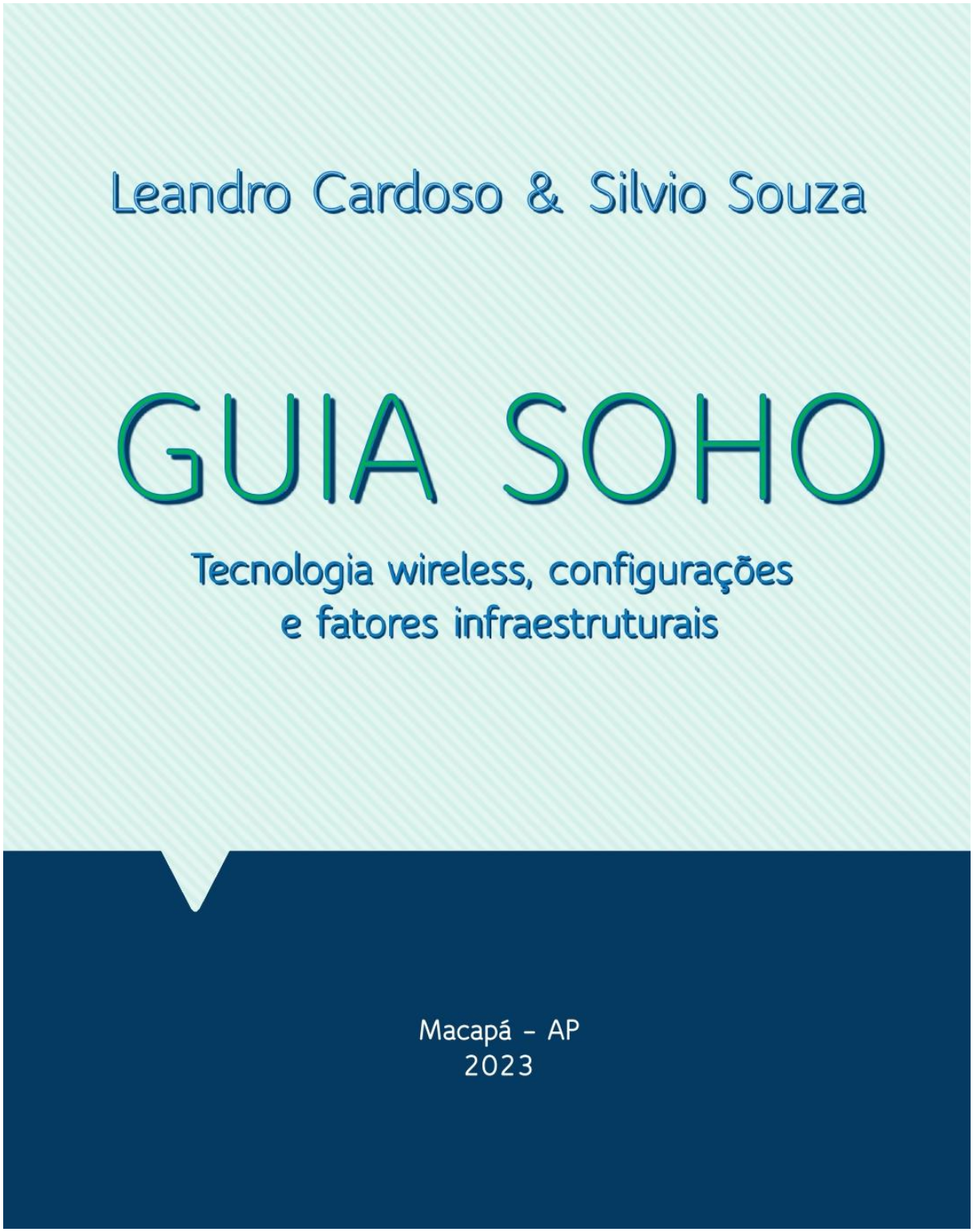
28) Em sua empresa, a perda de vendas já foi causada por problemas na rede wireless?
a) Nunca
b) Raramente
c) Às vezes
d) Frequentemente
e) Sempre

29) Em uma escala de 1 a 5, qual é o nível de importância que sua empresa dá para a infraestrutura da rede wireless?
1) Não é importante
2) Pouco importante
3) Moderadamente importante
4) Importante
5) Muito importante

30) Em sua opinião, qual é o fator mais importante para garantir uma boa infraestrutura em uma rede wireless?
a) Velocidade da conexão
b) Cobertura do sinal
c) Estabilidade da conexão
d) Segurança da rede
e) Outros (especificar)_____

31) Em uma escala de 1 a 5, qual é o nível de importância que sua empresa dá para a segurança dos equipamentos de rede?
1) Não é importante
2) Pouco importante
3) Moderadamente importante
4) Importante
5) Muito importante

ANEXO B– GUIA SOHO CRIA DO (PRODUTO DA PESQUISA)



Introdução

Neste guia técnico, você encontrará informações sobre como configurar a rede sem fio de sua pequena empresa ou escritório em casa (SOHO) para aumentar o nível de segurança. Além disso, destacaremos a importância dos fatores infraestruturais para a proteção das informações que trafegam na rede. Este guia foi elaborado com base em um roteiro aplicado em laboratório no Instituto Federal do Amapá (IFAP).

No capítulo 1, apresentamos alguns conceitos básicos sobre redes sem fio e segurança da informação. Abordaremos os tipos de criptografia, a importância de alterar as senhas padrão dos dispositivos, o uso de firewalls e a segmentação da rede.

No capítulo 2, fornecemos um guia passo a passo para configurar a rede sem fio de sua empresa ou escritório em casa. Abordaremos tópicos como a escolha do SSID, a configuração do tipo de segurança e a escolha da senha.

Neste capítulo 3, destacaremos a importância dos fatores infraestruturais para a proteção da informação. Abordaremos tópicos como a atualização do firmware do roteador, a instalação de patches de segurança e a escolha de dispositivos de qualidade.

Neste capítulo 4, forneceremos algumas dicas de solução de problemas para a rede sem fio. Abordaremos tópicos como a análise de interferências, a verificação de conflitos de endereços IP e a atualização dos drivers dos dispositivos.

Ao final são sintetizadas as informações sobre como configurar a rede sem fio de sua pequena empresa ou escritório em casa para aumentar o nível de segurança. Além disso, destacamos a importância dos fatores infraestruturais para a proteção das informações que trafegam na rede. Esperamos que este guia seja útil e que você possa implementar essas medidas em sua rede. Lembre-se sempre de manter seus dispositivos atualizados e de escolher dispositivos de qualidade para garantir a segurança de sua rede.

Conceitos básicos

Especificações do roteador utilizado no laboratório de redes de computadores

Figura 1: Roteador DIR-809

Fonte: Google, 2023.

D-Link DIR-809 roteador sem fio Fast Ethernet Dual-band (2,4 GHz / 5 GHz) 4G Preto	
Conexão WAN **Ethernet WAN** **Recursos LAN wireless** ***Banda Wi-Fi:* Dual band (2,4 GHz / 5 GHz)** **Padrão Wi-Fi: 802.11ad** ***Padrões de Wi-Fi:* Wi-Fi 5 (802.11ac), 802.11ad, 802.11b, 802.11g, Wi-Fi 4 (802.11n)** **Networking** **Ethernet LAN**	Networking *Tipo de interface Ethernet LAN:* Fast Ethernet *Taxas de dados Ethernet LAN:* 10, 100 Mbit/s Tecnologia de cabeamento: 10/100Base-T(X) Padrões de rede: IEEE 802.11a, IEEE 802.11ac, IEEE 802.11ad, IEEE 802.11az, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n Segurança Algoritmos de segurança: WPA, WPA2, WPS

> CRIPTOGRAFIA DE DADOS:

A criptografia de dados é importante configurar a rede wireless de preferência com protocolos WPA2 ou superior, para garantir que as informações transmitidas pela rede estejam protegidas contra interceptação e acesso não autorizado.

> CHAVE DE CRIPTOGRAFIA:

A chave de criptografia é a senha que os usuários precisarão digitar para se conectar à rede sem fio. A senha forte deve ter pelo menos oito caracteres que inclua uma combinação de letras, números e símbolos.

Conceitos básicos

> APLICATIVO PARRA CRIAR SENHAS FORTES:

O aplicativo 'Password Generator' é disponibilizado na Play Store, como ele pode-se escolher o comprimento da senha, incluir ou excluir caracteres especiais, números e letras maiúsculas e minúsculas.

> RESTRIÇÕES DE ACESSO:

Uma configuração interessante é a restrição do acesso à rede wireless apenas a dispositivos autorizados e conhecidos. É possível fazer isso utilizando filtragem de endereços MAC, que permite configurar a rede para permitir apenas dispositivos com endereços MAC específicos.

> DESATIVAR O SSID BROADCAST / SSID OCULTO:

Quando o roteador transmite o nome da rede (SSID) publicamente, ele pode ser facilmente encontrado por pessoas mal-intencionadas. Desativar o SSID Broadcast torna a rede menos visível para hackers.

> FILTRAGEM URL:

A filtragem de URL em um roteador é uma função que permite controlar o acesso a determinados sites ou categorias de sites na rede. Essa função é útil para restringir o acesso a conteúdo inadequado ou indesejado, como sites de jogos, redes sociais ou pornografia.

Conceitos básicos

> ATUALIZAÇÃO DO FIRMWARE DO ROTEADOR:

A atualização do firmware do roteador é um processo importante para garantir que seu roteador tenha as últimas correções de segurança, melhorias de desempenho e recursos adicionais fornecidos pelo fabricante.

> CONTROLE DE POTÊNCIA DO ROTEADOR:

Controlar a potência de transmissão da rede serve para limitar o alcance do sinal e evitar que pessoas de fora da rede tenham acesso. O controle de potência em redes wireless é uma função importante que pode ajudar a otimizar o desempenho da rede, economizar energia e reduzir interferências.

> SENHA DO ADMINISTRADOR

A senha do administrador do roteador pode variar de acordo com o modelo e o fabricante do dispositivo. No entanto, existem algumas senhas padrão comuns que são amplamente utilizadas pelos fabricantes. Ao alterar a senha de administrador é importante guardar a nova senha em um local seguro, para evitar que seja esquecida ou perdida. Também é uma boa prática alterar a senha de administrador regularmente para manter a segurança da rede.

> FIREWALL NA INTERFACE DO ROTEADOR:

Um firewall em um roteador é uma funcionalidade de segurança que controla o tráfego de rede entre a rede interna e a Internet, ajudando a proteger os dispositivos conectados à rede contra ameaças externas. O firewall do roteador pode ser configurado para filtrar pacotes de dados com base em regras de segurança pré-definidas.

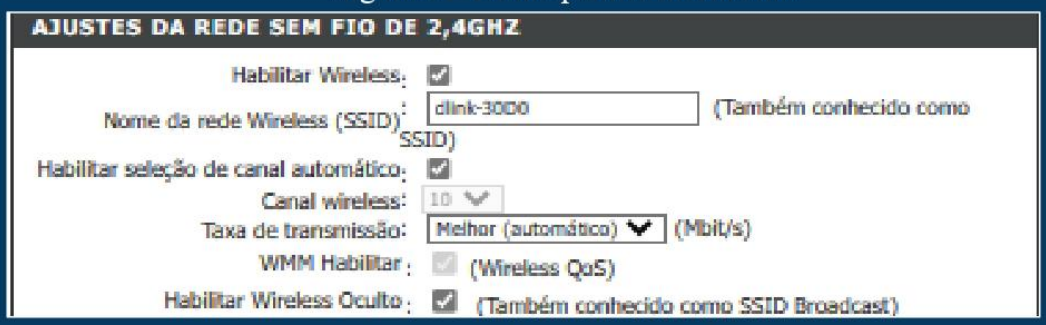
Configuração da rede sem fio 2

As configurações em laboratório foram as seguintes: (1) Criptografia de dados; (2) Senhas fortes com aplicativo Password Generator; (3); Restrição de acesso por filtragem MAC; (4) Desativar o SSID Broadcast / SSID Oculto; (5) Filtragem URL. Outras são generalizações para configurações em roteadores que sejam mais avançados, não foram realizados testes no laboratório devido à limitações na interface do roteador utilizado. São elas: (6) Atualização do firmware; (7) Controle de potência do sinal Wi-Fi; (8) Configuração do firewall da interface do roteador.

Início do processo de configuração do roteador:

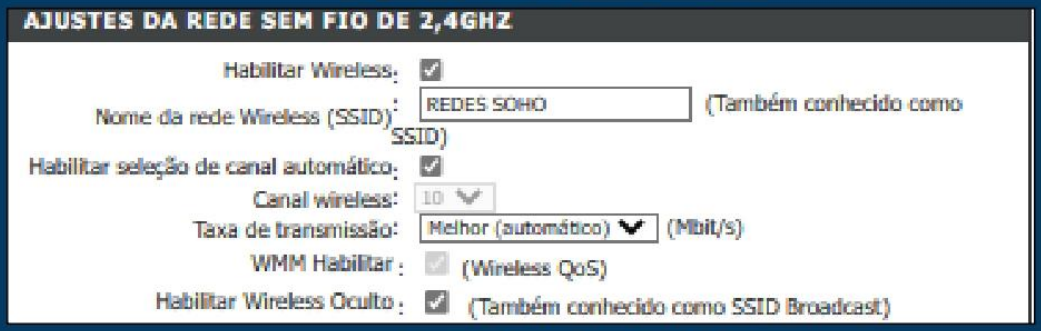
1) Acesse o painel de administração do seu roteador sem fio, abra um navegador da web e digite o endereço IP do seu roteador sem fio na barra de endereços. O endereço IP padrão para a maioria dos roteadores é 192.168.1.1, mas pode ser diferente para o seu modelo específico. Consulte o manual do usuário do roteador para obter o endereço IP correto. Depois de acessar o panel de administração mudou-se o nome padrão do SSID da rede:

Figura 2 – Nome padrão do roteado



Fonte: Cardoso; Souza, 2023.

Figura 2 – Novo nome atribuído



Fonte: Cardoso; Souza, 2023.

2) A chave de criptografia é a senha que os usuários precisarão digitar para se conectar à rede sem fio. A senha forte deve ter pelo menos oito caracteres que inclua uma combinação de letras, números e símbolos. Após configurar a criptografia WPA2 e a chave de criptografia, clicou-se em "Salvar Configurações" para salvar as alterações e sair do painel de administração:

Figura 3 – Configurações aplicadas na 2.4GHz e 5GHz

MODO DE SEGURANÇA SEM FIO

Modo de Segurança: Habilitar WPA/WPA2 Apenas na Segurança Wireless (aprimorado)

WPA/WPA2

WPA/WPA2 requer que as estações utilizem alto grau de criptografia e autenticação.

Tipo de codificação : AUTO (TKIP/AES)
PSK : PSK
Chave de Rede : wireless2023@
(8~63 ASCII ou 64 HEX)

AJUSTES DA REDE SEM FIO DE 5GHZ

Habilitar Wireless :
Nome da rede Wireless (SSID) : dlink-1B0B-5GHz (Também conhecido como SSID)
Habilitar seleção de canal automático :
Canal wireless : 149
Taxa de transmissão : Melhor (automático) (Mbit/s)
WMM Habilitar : (Wireless QoS)
Habilitar Wireless Oculto : (Também conhecido como SSID Broadcast)

MODO DE SEGURANÇA SEM FIO

Modo de Segurança: Habilitar WPA/WPA2 Apenas na Segurança Wireless (aprimorado)

WPA/WPA2

WPA/WPA2 requer que as estações utilizem alto grau de criptografia e autenticação.

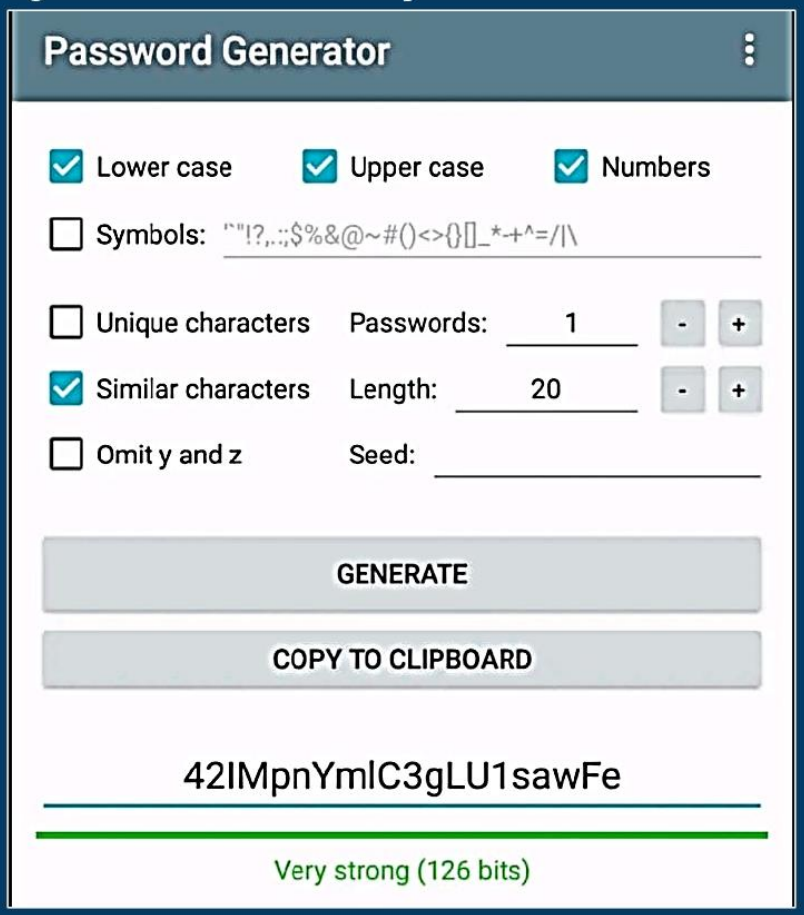
Tipo de codificação : AUTO (TKIP/AES)
PSK : PSK
Chave de Rede : wireless2023@
(8~63 ASCII ou 64 HEX)

Salvar configurações | Não Salvar Configurações

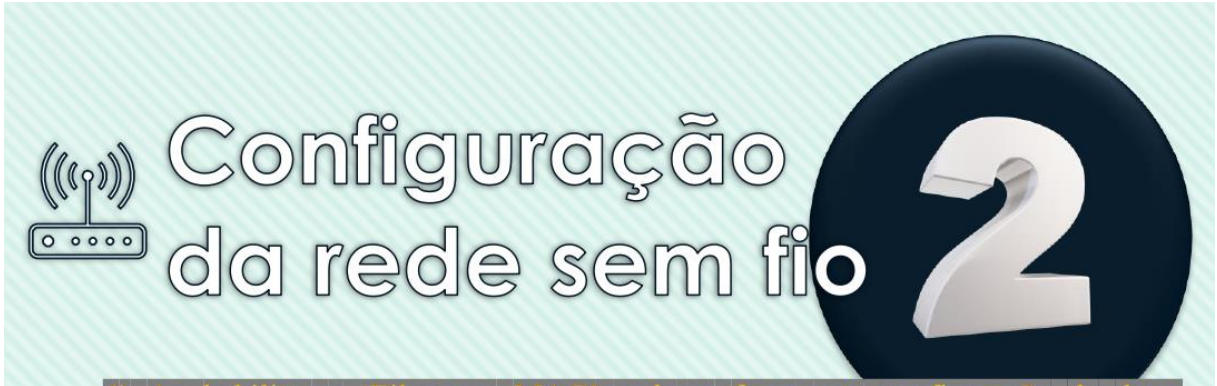
Fonte: Cardoso; Souza, 2023.

3) O aplicativo ‘Password Generator’ é disponibilizado na Play Store, como ele pode-se escolher o comprimento da senha, incluir ou excluir caracteres especiais, números e letras maiúsculas e minúsculas.

Figura 4 – Senhas fortes com aplicativo Password Generator



Fonte: Cardoso; Souza, 2023.

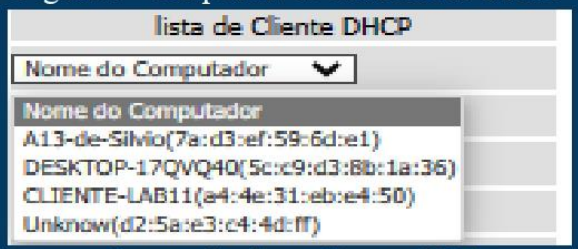


4) Ao habilitar a 'Filtragem MAC' pode-se fazer esta configuração de duas maneiras. Inserir o MAC manualmente, no campo em branco de endereço MAC ou colocar os aparelhos que estão conectados na rede pela lista de Cliente DHCP, basta ir à opção 'Nome do Computador' onde irá aparecer a lista de dispositivos conectados, após isso clique em sobre o aparelho deseja bloquear ou conceder permissão.

Figura 6 – Restrição de acesso por filtragem MAC

Fonte: Cardoso; Souza, 2023.

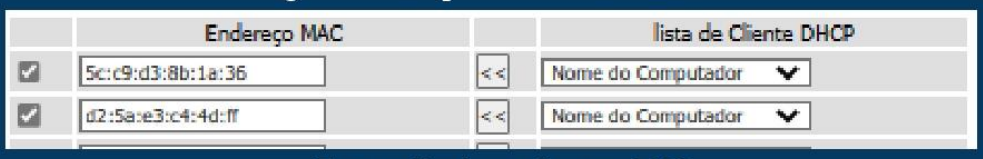
Figura 7 – Dispositivos conectados à rede



Fonte: Cardoso; Souza, 2023.

5) Após salvar as configurações os dispositivos que foram selecionados só poderão acessar a rede e outros não selecionados ficaram sem acesso a rede, ou caso contrário se negados os dispositivos que foram selecionados automaticamente perdem o acesso à rede.

Figura 8 – Dispositivos selecionados



Fonte: Cardoso; Souza, 2023.

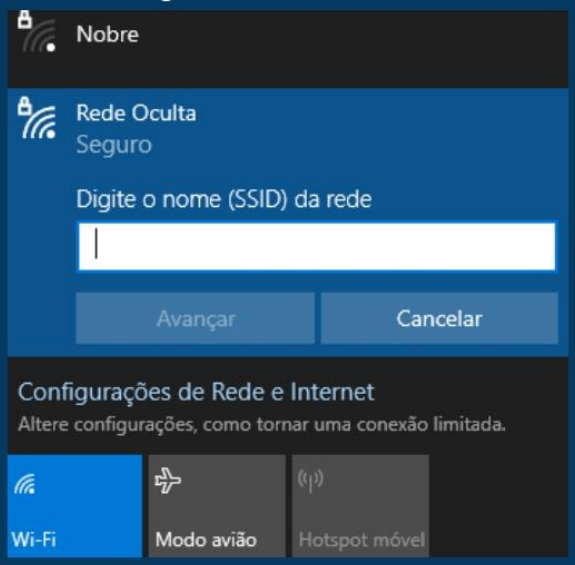
Configuração da rede sem fio 2

6) Para desativar o SSID Broadcast e tornar a rede menos visível para hackers, no roteador, na aba de configuração em 'Ajustes da rede sem fio de 2,5GHz e na 5GHz' seleciona-se a opção 'Habilitar Wireless Oculto' e salva-se tal configuração. Após a rede ser reiniciada a nome da rede torna-se oculto.

Figura 9 – Opção Habilitar Wireless Oculto selecionada

Fonte: Cardoso; Souza, 2023.

Figura 10 – Rede ocultada



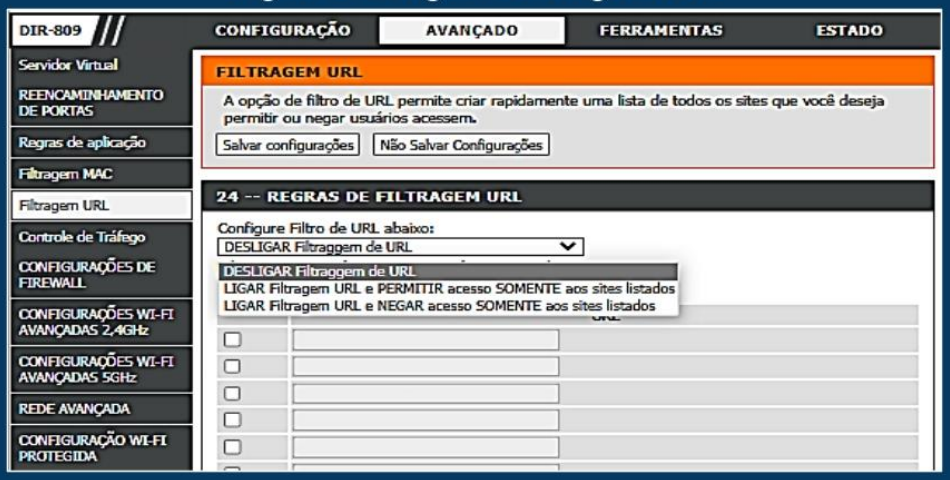
Fonte: Cardoso; Souza, 2023.

7) Após aplicadas as configurações os dados da rede devem ser informados manualmente, sendo 'SSID' e 'Senha'.

Configuração da rede sem fio 2

8) Na aba ‘Avançado’ em Filtragem URL são realizadas as configurações, nesse caso, colocando os sites que desejasse bloquear nos espaços em brancos e seleciona a opção ‘LIGAR Filtragem URL e NEGAR acesso SOMENTE aos sites listados’ e basta salvar e reiniciar a interface.’

Figura 11 – Regras de filtragem URL



Fonte: Cardoso; Souza, 2023.

Figura 12 – Regras criadas

Fonte: Cardoso; Souza, 2023.

9) Aqui estão apenas generalizações para configurações em roteadores que sejam mais avançados, não foram realizados testes no laboratório devido à limitações na interface do roteador utilizado. São elas: (6) Atualização do firmware; (7) Controle de potência do sinal Wi-Fi; (8) Configuração do firewall da interface do roteador.

Quadro 1 – Atualização do firmware do roteador

1. **Preparação:**
   - Verifique o modelo do roteador e a versão atual do firmware. Isso geralmente pode ser encontrado no painel de administração do roteador ou no manual do usuário.
   - Certifique-se de ter uma conexão estável à internet e, de preferência, conecte-se ao roteador via cabo Ethernet.
   - Faça backup das configurações do roteador, caso seja necessário reconfigurá-lo após a atualização.
2. **Download:**
   - Acesse o site do fabricante do roteador e navegue até a página de suporte e downloads.
   - Localize a seção de firmware e procure a versão mais recente disponível para o seu modelo de roteador.
   - Faça o download do arquivo do firmware em seu computador.
3. **Instalação:**
   - Acesse o painel de administração do roteador digitando o endereço IP do roteador na barra de endereço do navegador. O endereço IP padrão varia de acordo com o fabricante do roteador, mas geralmente é 192.168.0.1 ou 192.168.1.1.
   - Faça login no painel de administração do roteador com o nome de usuário e senha padrão ou os detalhes de login personalizados.
   - Navegue até a seção de firmware ou atualização de software e faça o upload do arquivo do firmware que você baixou anteriormente.
   - Aguarde o processo de atualização ser concluído. O roteador pode reiniciar automaticamente durante o processo.
   - Após a atualização ser concluída, faça login novamente no painel de administração do roteador e verifique se todas as configurações foram mantidas e se o firmware foi atualizado com sucesso.

Fonte: Cardoso; Souza, 2023.

10) Aqui estão apenas generalizações para configurações em roteadores que sejam mais avançados, não foram realizados testes no laboratório devido à limitações na interface do roteador utilizado. São elas: (6) Atualização do firmware; (7) Controle de potência do sinal Wi-Fi; (8) Configuração do firewall da interface do roteador.

Quadro 2 – Configurações de controle do potência do sinal Wi-Fi

- 1. Acesse as configurações do roteador: Conecte-se ao roteador usando um cabo de rede ou um dispositivo conectado à rede. Abra um navegador da web e insira o endereço IP do roteador na barra de endereço. Insira o nome de usuário e a senha para acessar as configurações do roteador.
- 2. Localize as configurações sem fio: As configurações sem fio geralmente estão localizadas em um menu de configurações separado. Procure por um menu de "Wireless" ou "Wi-Fi".
- 3. Ative o controle de potência: Procure por uma opção de "Potência de Transmissão" ou "Transmit Power". Ative essa opção para permitir o controle de potência. Em alguns roteadores, você pode ajustar a potência de transmissão em um intervalo de 1-100%, enquanto outros podem ter configurações mais específicas.
- 4. Ajuste a potência de transmissão: Ajuste a potência de transmissão de acordo com as necessidades da sua rede. Se a rede cobre uma área pequena, reduzir a potência de transmissão pode economizar energia e reduzir interferências. Se a rede cobre uma área grande ou tem muitos obstáculos, aumentar a potência de transmissão pode melhorar o alcance e a qualidade do sinal.
- 5. Salve as alterações: Depois de fazer as alterações, clique em "Salvar" ou "Aplicar" para salvar as alterações e sair do menu de configurações sem fio.

Fonte: Cardoso; Souza, 2023.

10) Aqui estão apenas generalizações para configurações em roteadores que sejam mais avançados, não foram realizados testes no laboratório devido à limitações na interface do roteador utilizado. São elas: (6) Atualização do firmware; (7) Controle de potência do sinal Wi-Fi; (8) Configuração do firewall da interface do roteador.

Quadro 3 – Configurações de controle do potência do sinal Wi-Fi

- **Conecte-se ao roteador:** Abra um navegador da web e digite o endereço IP padrão do roteador na barra de endereço. Isso geralmente é algo como 192.168.0.1 ou 192.168.1.1. Pressione Enter para acessar a página de administração do roteador.
- **Faça login no roteador:** Insira o nome de usuário e a senha corretos para fazer login na página de administração do roteador. Se você nunca alterou essas informações, verifique o manual do usuário do roteador ou consulte a documentação do fabricante para obter as credenciais padrão.
- **Acesse as configurações do firewall:** Navegue pela interface de administração do roteador até encontrar a seção de configurações de firewall. Isso pode variar dependendo do modelo do roteador, mas geralmente é encontrado em "Configurações avançadas", "Segurança" ou "Firewall".
- **Ative o firewall:** Se o firewall estiver desativado, localize a opção para ativá-lo e marque a caixa de seleção correspondente.
- **Configurar as regras do firewall:** A maioria dos roteadores permite criar regras de firewall personalizadas para controlar o tráfego de entrada e saída. Você pode configurar regras para bloquear portas específicas, IP's ou serviços, ou permitir apenas determinados tipos de tráfego. Consulte a documentação do fabricante ou o manual do usuário do roteador para obter instruções detalhadas sobre como adicionar regras de firewall específicas.
- **Defina políticas de segurança:** Algumas interfaces de roteador permitem definir políticas de segurança gerais para o firewall. Você pode selecionar um nível de segurança pré-definido, como "Alto", "Médio" ou "Baixo", ou personalizar as configurações de segurança de acordo com suas necessidades. Essas políticas de segurança ajudam a determinar o quão restritivo o firewall será em relação ao tráfego.
- **Salve as configurações:** Após configurar as regras e as políticas de segurança do firewall, certifique-se de salvar as alterações feitas nas configurações.
- **Reinicie o roteador:** Após salvar as configurações, é recomendável reiniciar o roteador para que as alterações no firewall entrem em vigor.

Fonte: Cardoso; Souza, 2023.

Fatores infraestruturais

1) ATUALIZAÇÃO DO FIRMWARE DO ROTEADOR:

- **1.1. Significado para ambientes SOHO:** Em um ambiente SOHO, o roteador é o componente central da infraestrutura de rede, conectando todos os dispositivos e permitindo acesso à Internet. Manter o firmware do roteador atualizado é crucial para garantir a segurança dos dados e a estabilidade da rede.

- **1.2. Benefícios da atualização:** As atualizações de firmware geralmente incluem correções de segurança, aprimoramentos de desempenho e novos recursos. Ao atualizar o firmware regularmente, os usuários podem se beneficiar de patches que corrigem vulnerabilidades conhecidas e melhoram a proteção contra ameaças cibernéticas

2) INSTALAÇÃO DE PATCHES DE SEGURANÇA:

- **2.1. Importância em ambientes SOHO:** Em ambientes SOHO, onde os recursos de segurança podem ser limitados, a instalação de patches de segurança é fundamental para garantir a proteção dos dados. Esses patches corrigem falhas de segurança e vulnerabilidades que podem ser exploradas por hackers.

- **2.2. Práticas recomendadas:** É essencial adotar uma abordagem proativa para a instalação de patches de segurança em todos os dispositivos da rede SOHO. Certifique-se de aplicar as atualizações de software e firmware disponibilizadas pelos fabricantes, pois elas contêm correções críticas para vulnerabilidades conhecidas.

Fatores infraestruturais

3) ESCOLHA DE DISPOSITIVOS DE QUALIDADE:

- **3.1. Considerações para ambientes SOHO:** Ao selecionar dispositivos para um ambiente SOHO, é fundamental escolher produtos de qualidade e confiáveis. Esses dispositivos costumam oferecer melhores recursos de segurança e suporte contínuo de atualizações.

- **3.2. Avaliação de marcas e fabricantes:** Antes de adquirir um roteador ou outros dispositivos de rede, pesquise sobre as marcas e fabricantes. Dê preferência a empresas estabelecidas, que possuam reputação de segurança e que ofereçam atualizações regulares de firmware para seus dispositivos.

4) CONSIDERAÇÕES FINAIS DO CAPÍTULO

- Em ambientes SOHO, a proteção da informação é fundamental, mesmo com recursos limitados. Os fatores infraestruturais desempenham um papel crucial nessa proteção. Garantir a atualização do firmware do roteador, a instalação de patches de segurança e a escolha de dispositivos de qualidade são medidas essenciais para mitigar riscos de segurança e proteger os dados. Ao adotar essas práticas, os usuários de ambientes SOHO podem fortalecer a segurança de sua rede e garantir a confidencialidade, integridade e disponibilidade de suas informações.

Solução de problemas

1) ANÁLISE DE INTERFERÊNCIAS:

- **1.1. Identificação de interferências:** Interferências de outras redes sem fio, dispositivos eletrônicos, eletrodomésticos e outros equipamentos podem afetar negativamente o desempenho da rede wireless. É importante identificar e mitigar essas interferências.

- **1.2. Estratégias para minimizar interferências:** Posicione o roteador em uma área livre de obstáculos e longe de dispositivos que possam causar interferências. Experimente diferentes canais de frequência para encontrar o menos congestionado. Considere o uso de redes 5 GHz, que tendem a ter menos interferências.

2) VERIFICAÇÃO DE CONFLITOS DE ENDEREÇOS IP:

- **2.1. Identificação de conflitos:** Conflitos de endereços IP podem ocorrer quando dois ou mais dispositivos na rede estão usando o mesmo endereço IP, causando problemas de conectividade. É importante identificar e resolver esses conflitos.

- **2.2. Renovação do endereço IP:** Verifique se os dispositivos na rede estão configurados para obter um endereço IP automaticamente (DHCP). Se houver conflitos, tente renovar os endereços IP dos dispositivos afetados ou atribuir manualmente endereços IP exclusivos.

Solução de problemas

3) ATUALIZAÇÃO DOS DRIVES DOS DISPOSITIVOS:

- **3.1. Importância dos drivers atualizados:** Os drivers são responsáveis por fornecer comunicação adequada entre o dispositivo e o sistema operacional. Drivers desatualizados podem causar problemas de conectividade na rede sem fio.

- **3.2. Verificação e atualização dos drivers:** Verifique se os drivers dos adaptadores de rede sem fio estão atualizados. Acesse o site do fabricante ou utilize ferramentas de atualização automática para garantir que os drivers estejam na versão mais recente.

4) CONSIDERAÇÕES FINAIS DO CAPÍTULO:

- **4.1. Ao enfrentar problemas de rede wireless em ambientes SOHO, a solução eficaz de problemas é essencial para manter a conectividade confiável. Analisar interferências, verificar conflitos de endereços IP, atualizar drivers de dispositivos e revisar a configurações do roteador são as melhores recomendações.**

Em um ambiente SOHO, garantir uma rede wireless confiável e segura é essencial para a produtividade e proteção das informações. Neste guia, abordamos diversos tópicos relacionados à solução de problemas em redes wireless, considerando o contexto específico de ambientes SOHO.

Destacamos a importância da criptografia de dados, recomendando a configuração da rede wireless com protocolos WPA2 ou superiores, garantindo que as informações transmitidas estejam protegidas contra interceptação e acesso não autorizado.

Além disso, ressaltamos a necessidade de utilizar senhas fortes e exclusivas, utilizando aplicativos como o Password Generator para criá-las. Também abordamos a importância da restrição de acesso por meio da filtragem de endereços MAC, permitindo apenas dispositivos autorizados na rede.

Para evitar a visibilidade indesejada da rede, recomendamos desativar o SSID Broadcast ou ocultar o SSID, dificultando o acesso para pessoas mal-intencionadas.

Outros aspectos mencionados incluem a atualização regular do firmware do roteador, que traz correções de segurança e melhorias de desempenho, bem como a verificação e atualização dos drivers dos dispositivos para evitar problemas de conectividade.

Por fim, enfatizamos a importância do controle de potência do sinal Wi-Fi para limitar o alcance da rede, evitando acesso não autorizado, e a configuração adequada do firewall do roteador para filtrar pacotes de dados e proteger os dispositivos conectados contra ameaças externas.

Ao seguir essas orientações e implementar as melhores práticas de segurança, você estará fortalecendo sua rede wireless e garantindo um ambiente SOHO seguro, confiável e produtivo.

Acesso ao site do Guia: https://sites.google.com/view/projetoifap/home?authuser=0