SEGURANÇA CIBERNÉTICA EM AMBIENTES RESIDENCIAIS

CYBER SECURITY IN RESIDENTIAL ENVIRONMENTS

Cristian da Silva Oliveira
Fatec Americana – Ministro Ralph Biasi
cristian.oliveira16@fatec.sp.gov.br

Paulo Luiz Fernandes de Souza
Fatec Americana - Ministro Ralph Biasi
paulo.souza115@fatec.sp.gov.br

João Emmanuel D Alkmin Neves
Fatec Americana - Ministro Ralph Biasi
joao.neves11@fatec.sp.gov.br

Resumo

O artigo explora a segurança em redes domésticas, um tema importante diante da crescente dependência das tecnologias de rede em atividades diárias que envolvem dados e informações sigilosas. O objetivo principal é conscientizar usuários sobre a importância da segurança em redes domésticas e orientá-los sobre práticas eficazes para diminuir riscos cibernéticos, melhorando assim a proteção de suas informações pessoais. A metodologia utilizada na pesquisa para fundamentação desse trabalho, envolveu uma análise literária sobre a evolução da Internet e a segurança de redes, além da realização de um questionário que avaliou a percepção e as práticas de segurança dos usuários das redes domésticas. Os resultados do questionário mostram uma consciência razoável sobre a importância de práticas seguras, mas também revelam lacunas significativas na implementação efetiva dessas medidas. A pesquisa sugere que é vital uma educação contínua em cibersegurança para todos os níveis de formação, para garantir que as práticas de segurança sejam atualizadas e aplicadas corretamente, reduzindo a vulnerabilidade das redes domésticas.

Palavras-chave: Cibersegurança, Redes domésticas, Práticas de Segurança

Abstract

The article explores security in home networks, an important topic given the growing dependence on network technologies in daily activities involving sensitive data and information. The main objective is to raise awareness among users about the importance of security on home networks and guide them on effective practices to reduce cyber risks, thus improving the protection of their personal information. The methodology used in the research to support this work involved a literary analysis on the evolution of the Internet and network security, in addition to carrying out a questionnaire that evaluated the perception and security practices of users of home networks. The questionnaire results show a reasonable awareness of the importance of safe practices, but also reveal significant gaps in the effective implementation of these measures. The research suggests that continuous cybersecurity education for all training levels is vital to ensure that security practices are updated and applied correctly, reducing the vulnerability of home networks.

Keywords*: Cybersecurity, Awareness, Security Practices*

1. Introdução

Desde o surgimento dos primeiros computadores, o mundo testemunhou uma revolução sem precedentes em várias esferas da vida humana. O que inicialmente se configurava como uma ferramenta restrita a institutos de pesquisa e a empresas com recursos substanciais, rapidamente se converteu em uma necessidade indispensável para a imensa maioria da população. O avanço da tecnologia não apenas democratizou o acesso aos computadores, mas também transformou o modo como as pessoas se conectam ao mundo. Nesta era digital, a conexão à Internet em casa, predominantemente via redes sem fio, tornou-se um requisito básico para o dia a dia. Com múltiplos dispositivos como *notebook*, *smartphone*, *tablet* e *smart TV* conectados simultaneamente, o uso da Internet se expandiu para além da mera pesquisa, abrangendo trabalho, educação, comunicação e entretenimento.

Contudo, essa conveniência acarreta um conjunto de preocupações significativas no âmbito da Segurança da Informação, destacando-se a proteção das redes domésticas como uma preocupação primordial. Surge, portanto, o problema central: as pessoas estão verdadeiramente seguras ao conectar seus dispositivos pessoais em suas residências, e suas informações pessoais e financeiras estão protegidas contra invasões e uso indevido?

A pesquisa aborda o tema da segurança em redes domésticas, visando esclarecer, o que são essas redes, como surgiram, os riscos associados e, crucialmente, o que pode ser feito para poder proporcionar uma maior proteção nas redes domésticas, baseadas nas medidas informadas no artigo sobre Segurança da Informação ao serem aplicadas. Ao longo deste estudo, serão explorados os protocolos de segurança recomendados e as práticas a serem adotadas para fortalecer a defesa contra ameaças digitais, proporcionando aos usuários as ferramentas, técnicas e procedimentos necessários para proteger suas informações pessoais e evitar acessos não autorizados à sua rede doméstica.

A relevância do presente artigo reside na crescente vulnerabilidade das redes domésticas e na necessidade premente de educar os usuários sobre medidas de segurança eficazes. Ao munir o público com conhecimento e estratégias para aprimorar a segurança de suas conexões domésticas, este trabalho visa contribuir para uma sociedade digital mais segura e informada, onde os riscos de invasão e exposição de dados pessoais sejam minimizados. Conforme destaca Marcondes (2008), a educação contínua sobre segurança cibernética é essencial para reduzir os riscos e capacitar os usuários a protegerem suas informações no ambiente digital cada vez mais interconectado.

2. Referencial Teórico

O computador consolidou-se como uma ferramenta imprescindível, não apenas no contexto empresarial, mas também para uma significativa parcela da população, desempenhando um papel crucial em diversos aspectos da vida cotidiana, como trabalho, estudos, comunicação e lazer. A popularização das redes domésticas facilitou a conexão de múltiplos dispositivos em ambientes residenciais, mas, ao mesmo tempo, trouxe desafios significativos relacionados à segurança dessas redes domésticas.

2.1 Redes domésticas

A Internet surgiu nos Estados Unidos em 1969, como resultado da ARPANET, desenvolvida para proteger dados militares durante a Guerra Fria. No Brasil, o contato inicial ocorreu em 1989 para fins de pesquisa, e em 1995 foi comercializada para uso doméstico, inicialmente por conexões dial-up. Desde então, evoluiu para banda larga e redes sem fio (Vicentini *et al.*, 2005; Mancilla, 2014)

Para Marcondes (2008), rede doméstica é um sistema que as pessoas têm em suas casas, permitindo que os computadores interajam e compartilhem informações entre si. O acesso à Internet requer a contratação de um provedor de serviços, responsável por disponibilizar a conexão. Inúmeros desses provedores oferecem equipamentos que viabilizam a conexão sem fio, permitindo que diferentes dispositivos compatíveis com essa tecnologia se conectem à rede.

Como aponta Marcondes (2008), as formas mais usuais de configurar redes em casa incluem o uso de conexões por cabos e sem fio. Embora a conexão por cabo possa oferecer velocidades superiores, a opção sem fio é frequentemente preferida pela sua conveniência, custo-benefício e versatilidade. Isso se deve ao fato de que permite a conexão de uma variedade de dispositivos móveis — como *smartphones*, televisões, *notebooks*, *tablets*, entre outros — desde que estes sejam compatíveis com conexão sem fio, facilitando a mobilidade dos usuários na área de cobertura do sinal.

Segundo FasterCapital (2024), a tecnologia das redes sem fio se destaca pela mobilidade e conveniência, pois permite conexões à Internet de qualquer lugar no alcance de uma rede sem fio. Isso possibilita o acesso *online* sem a necessidade de estar fixo em um local, facilitando o uso da Internet em casa, cafeterias, aeroportos ou em movimento, além disso, a rede sem fio é uma opção econômica, pois dispensa o uso de cabos e infraestruturas

custosas. Sua configuração simples e rápida faz dele uma escolha vantajosa tanto para residências, permitindo a conexão de múltiplos dispositivos à Internet com facilidade e sem custo adicional.

Chavatte (2024), ressalta a importância da proteção das redes domésticas, que facilitam o compartilhamento de recursos como Internet, impressoras, arquivos e outros dispositivos. Essas redes estão suscetíveis a diversos riscos, como ataques de *hackers*, vírus e Malware. Segundo o autor, o roteador desempenha um papel crucial nesse contexto, conectando a rede doméstica à Internet e distribuindo o sinal Wi-Fi. Além disso, o roteador oferece um painel de configurações que permite aos usuários ajustar os parâmetros de segurança tanto no próprio roteador quanto no sistema operacional, tornando assim as redes domésticas menos vulneráveis.

Listam-se algumas configurações importantes que Chavatte (2024) indica para ajustar no painel do roteador, visando aumentar a segurança da rede sem fio:

- Nome da Rede Wi-Fi (SSID): escolha um nome único e não revelador.
- Senha da Rede Wi-Fi: utilize senhas fortes e altere-as regularmente.
- Tipo de Criptografia: prefira WPA2 ou WPA3 em detrimento de WEP ou WPA.
- Ocultação da Rede Wi-Fi: oculte sua rede, mas esteja ciente das possíveis complicações de compatibilidade.
- Filtragem de Endereços MAC: defina quais dispositivos podem acessar sua rede.
- Desativação do WPS: evite conexões facilitadas que possam ser exploradas por *hackers*.
- Atualização do *Firmware*: mantenha o *firmware* atualizado para corrigir vulnerabilidades.

Conforme Chavatte (2024), o sistema operacional desempenha um papel crucial na gestão dos recursos do sistema e dos programas, incorporando diversas configurações de segurança que podem influenciar diretamente a segurança da sua rede doméstica. Segue uma lista de configurações que podem ser ajustadas no sistema:

- Tipo de Rede: escolha entre rede pública, privada ou de domínio, dependendo do ambiente.

- *Firewall* do Windows: mantenha ativado para fortalecer a defesa contra possíveis ataques externos.
- Antivírus do sistema: mantenha ativado e atualizado para detectar ameaças.
- Atualizações do sistema: instale regularmente atualizações para corrigir vulnerabilidades e melhorar o desempenho

Para Fernandes *et al.* (2015), uma rede se torna suscetível a ataques quando intrusos mal-intencionados conseguem adentrar, modificar ou eliminar dados sigilosos, ou até paralisar o funcionamento do sistema. No entanto, a adoção de medidas de segurança, a implementação de tecnologias avançadas e a utilização de protocolos específicos podem reforçar a proteção dessas redes.

2.2 Principais Ataques Cibernéticos

De acordo com Mascarenhas Neto e Araújo (2019), o cenário atual de ataques cibernéticos, se tornaram mais acessíveis e frequentes, não se limitando apenas a indivíduos com amplo conhecimento tecnológico. Isso ocorre devido à facilidade de acesso a ferramentas e métodos de ataque. Neste contexto, é criada uma espécie de guerra entre profissionais de Segurança da Informação, cujo papel é proteger organizações contra esses ataques, e os atacantes, que buscam comprometer a Segurança da Informação. Mascarenhas Neto e Araújo (2019), afirmam que os ataques são variados e classificados conforme as técnicas utilizadas e os objetivos pretendidos.

- *Phishing*: Os ataques de *Phishing* envolvem o envio de *e-mails* ou mensagens falsas para induzir as pessoas a revelarem informações confidenciais, como senhas e informações financeiras.
- *Malware*: Isso inclui vírus, *trojans*, *ransomware* e outros tipos de software malicioso projetado para danificar ou explorar sistemas e dados.
- Ataques de negação de serviço (DDoS): Os ataques DDoS buscam sobrecarregar os servidores de um site ou serviço, tornando-o inacessível para usuários legítimos.
- Ataques de engenharia social: Esses ataques exploram a manipulação psicológica para enganar as pessoas e obter informações confidenciais

- Ataques de Força Bruta: esses ataques tentam obter acesso a sistemas ou contas ao tentar todas as combinações possíveis de senhas até encontrar a correta.
- *Man-in-the-Middle* (MitM): os ataques MitM ocorrem quando um invasor intercepta e altera as comunicações entre duas partes sem o conhecimento delas.
- Exploração de vulnerabilidades: ataques que se aproveitam de falhas de segurança em software ou sistemas para ganhar acesso não autorizado.
- Ataques a dispositivos IoT (Internet das Coisas): com o aumento de dispositivos conectados, os cibercriminosos buscam explorar vulnerabilidades em dispositivos IoT para ganhar acesso à rede.
- Roubo de identidade: os criminosos cibernéticos buscam obter informações pessoais para se passar por outra pessoa, geralmente para fins fraudulentos.
- Ataques a redes sem fio: tentativas de explorar vulnerabilidades em redes sem fio para obter acesso não autorizado.

É importante notar que o cenário de ameaças cibernéticas está em constante evolução, e novos métodos e técnicas podem surgir ao longo do tempo. Portanto, é fundamental manter sistemas e software atualizados, implementar boas práticas de segurança e estar ciente das ameaças mais recentes.

2.3 Segurança das Redes

Segundo Fernandes *et al.* (2015), a vulnerabilidade em redes doméstica é maior, pelo fato que os usuários não possuem conhecimento sobre segurança em redes, ou não se preocuparem em seguir os protocolos, regras e não investem em ferramentas que poderiam trazer uma proteção maior.

De acordo com Miranda (2017), ter uma rede de conexão sem fio protegida, é necessário ativar a segurança, autenticação e criptografia do roteador. A autenticação é feita com uma senha, evitando acesso não autorizado. Já a criptografia garante a confidencialidade dos dados que estão trafegando na rede.

Na criptografia os dados são transmitidos de forma não sequencial, o que dificulta entender as informações contidas neles (Fernandes *et al.*, 2015). Essa técnica assegura o sigilo, pois apenas usuários autorizados e autenticados podem acessar as informações, e

também garante a integridade, ao assegura ao usuário que as informações estão corretas e não foram interferidas externamente.

Segundo Miranda (2017), é possível encontrar orientações valiosas para fortalecer a segurança em redes, tanto com fio quanto sem fio, assim como para implementar políticas de segurança. As sugestões apresentadas incluem:

- Manter o dispositivo atualizado constantemente é crucial, não só por trazer melhorias de segurança, mas também por corrigir vulnerabilidades que podem ser exploradas por ataques. Cada atualização documenta as mudanças feitas, facilitando a compreensão das brechas de segurança que podem existir quando o sistema não está atualizado.
- Utilizar um *firewall* é essencial para bloquear acessos não autorizados ao seu computador, protegendo-o contra *hackers* e softwares maliciosos.
- Os softwares antivírus são projetados para identificar e eliminar vírus que infectem a memória do computador, *e-mails*, CDs, e outras fontes. É fundamental manter esses programas atualizados e executá-los regularmente.
- O uso de roteadores para compartilhar conexões oferece benefícios adicionais de segurança, já que muitos deles incluem *firewalls* e recursos como tradução de endereços IPs (NATs) para proteger sua rede.
- Evite se conectar como administrador, pois muitos programas maliciosos requerem privilégios de administrador para serem instalados. Para tarefas comuns, como navegar na Internet ou verificar *e-mails*, é mais seguro estar logado como usuário comum.
- Para redes sem fio, é imprescindível criar uma chave de segurança para ativar a criptografia dos dados, garantindo que apenas usuários autorizados possam acessar e trocar informações na rede.
- Alterar o nome de administrador e senha do roteador é essencial, já que muitos modelos vêm com essas informações padrão. Mudá-las ajuda a prevenir acessos não autorizados ao equipamento.

Nesse contexto, Macedo *et al.* (2018) destacam duas práticas essenciais para aprimorar a proteção da informação em redes:

- Criação de senhas: deve-se adotar senhas fortes e memoráveis, evitando dados pessoais, sequências de teclado e palavras comuns. As senhas ideais são longas, combinam letras maiúsculas e minúsculas, números e símbolos, e, de preferência, têm um significado pessoal para o usuário, garantindo tanto segurança quanto facilidade de memorização.

- *Backups*: A realização de cópias de segurança é crucial para proteger dados contra perdas causadas por falhas de hardware, problemas elétricos, erros de *software* ou ataques cibernéticos. Os *backups* permitem a recuperação de dados e a restauração de versões anteriores de sistemas ou arquivos, assegurando a continuidade e a integridade da informação.

3. Materiais e Métodos

Este artigo visa esclarecer a segurança em redes domésticas, abordando sua evolução, os riscos envolvidos e as estratégias de proteção. O embasamento teórico foi desenvolvido por meio de uma revisão bibliográfica sobre a história e evolução da Internet e das redes domésticas, com foco nos desafios de segurança gerados pela democratização do acesso. A pesquisa também analisou os principais ataques cibernéticos, identificando as ameaças mais comuns às redes domésticas e discutindo as tecnologias e práticas de segurança recomendadas.

A coleta de dados, realizada em abril de 2024, utilizou as bases de dados Google Acadêmico e SciELO, com filtros aplicados a publicações entre 2005 e 2024, nas categorias de artigos, *e-books* e publicações de especialistas, conforme detalhado na Tabela 01.

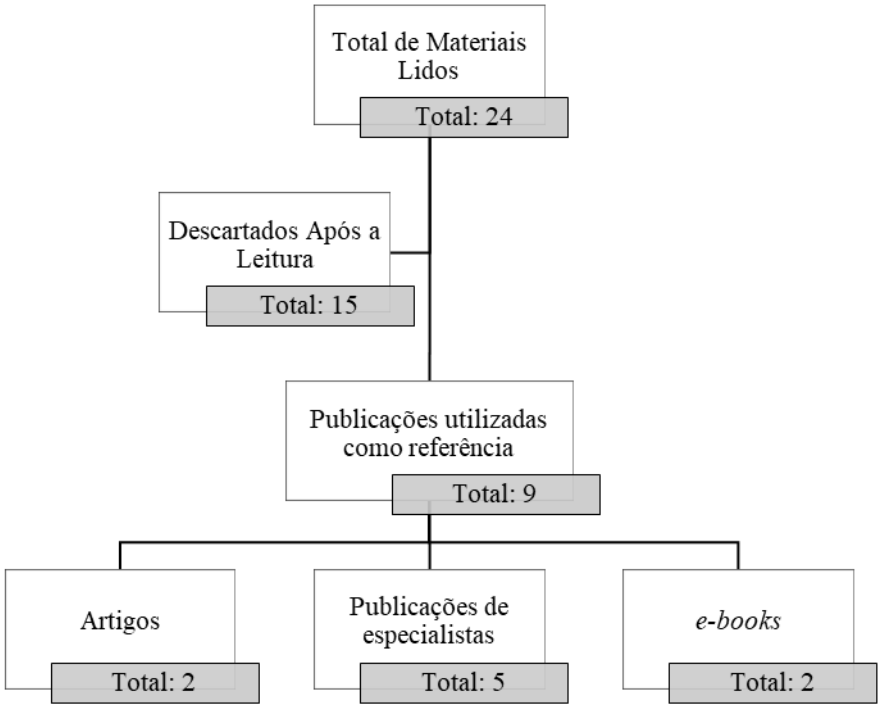
Tabela 01 – Bases de Dados

Base de Dados	Termos	Nº de Publicações
Google Acadêmico	Evolução da Internet	411
	Segurança em redes domésticas	245
	Desafios de segurança em redes domésticas	81
	Ataques cibernéticos em redes domésticas	166
	Práticas para segurança em redes domésticas	41
SciELO	Evolução da Internet	172
	Segurança em redes domésticas	34
	Desafios de segurança em redes domésticas	18
	Ataques cibernéticos em redes domésticas	52
	Práticas para segurança em redes domésticas	9

Fonte: Autores (2024)

Realizou-se, então, uma análise desses materiais, foram selecionados os que estavam alinhados com o tema central deste estudo, enquanto os que não atendiam aos critérios foram descartados. O conjunto de materiais analisados incluiu 10 artigos, 12 publicações de especialistas e 2 *e-books*, totalizando 24 fontes revisadas. Dessas, 8 artigos e 7 publicações foram excluídos, resultando na utilização de 9 fontes para embasar o presente trabalho. A Figura 1 apresenta o organograma dos materiais utilizados para a construção do artigo.

Figura 1 – Organograma dos materiais utilizados



Fonte: Autores (2024)

Após a revisão da literatura, foi realizada uma pesquisa exploratória de abordagem quantitativa, visando coletar opiniões, comportamentos e experiências dos indivíduos em relação ao tema. A coleta de dados foi feita por meio de um questionário elaborado no Google Forms, cujos resultados serão apresentados e analisados na próxima seção.

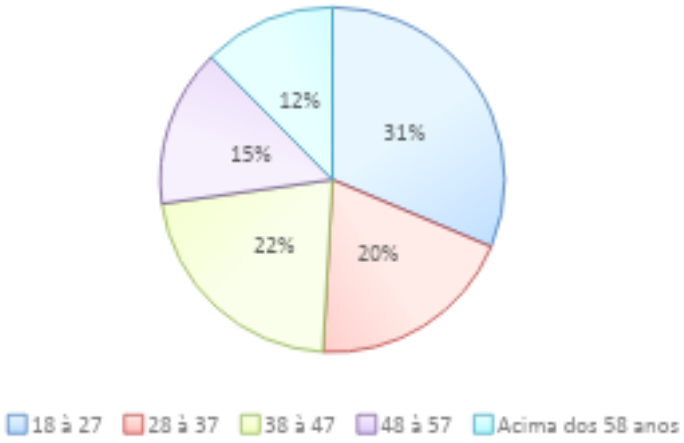
4. Resultados e Discussões

A pesquisa se caracteriza por uma análise qualitativa das informações coletadas na literatura, com ênfase na identificação de padrões, recomendações de segurança e melhores práticas. O texto discute a importância crítica da segurança em redes domésticas em face do

crescente número de dispositivos conectados e da evolução contínua das ameaças cibernéticas e analisa como o conhecimento sobre as melhores práticas de segurança e a implementação de medidas de proteção adequadas são fundamentais para diminuir os riscos associados. O estudo desse artigo combinou uma revisão bibliográfica e a formulação de uma pesquisa via questionário, resultando em uma pesquisa mista com aspecto quantitativo, contribuindo de maneiras diferentes para conclusão desse trabalho, onde a revisão bibliográfica feita por meio de publicações, ajudou formar uma base teórica e a pesquisa feita via questionário classificada como quantitativa, possibilitou a coleta de dados diretamente de indivíduos, permitindo análises estatísticas.

Ao analisar os dados provenientes do questionário do Google, a primeira questão abordou a faixa etária dos participantes. Dos 169 respondentes, observou-se uma distribuição variada nas faixas etárias. Cerca de 31% situaram-se entre 18 e 27 anos, 20% entre 28 e 37 anos, 22% entre 38 e 47 anos, 15% entre 48 e 57 anos, enquanto 12% estavam acima de 58 anos. Destaca-se que, embora a pesquisa tenha alcançado uma gama diversificada de idades, a maior concentração de respostas originou-se do grupo mais jovem, compreendido entre 18 e 27 anos. Esta distribuição está representada na Figura 2, evidenciando a proporção de respostas em cada faixa etária.

Figura 2 – Distribuição da faixa etária dos participantes.

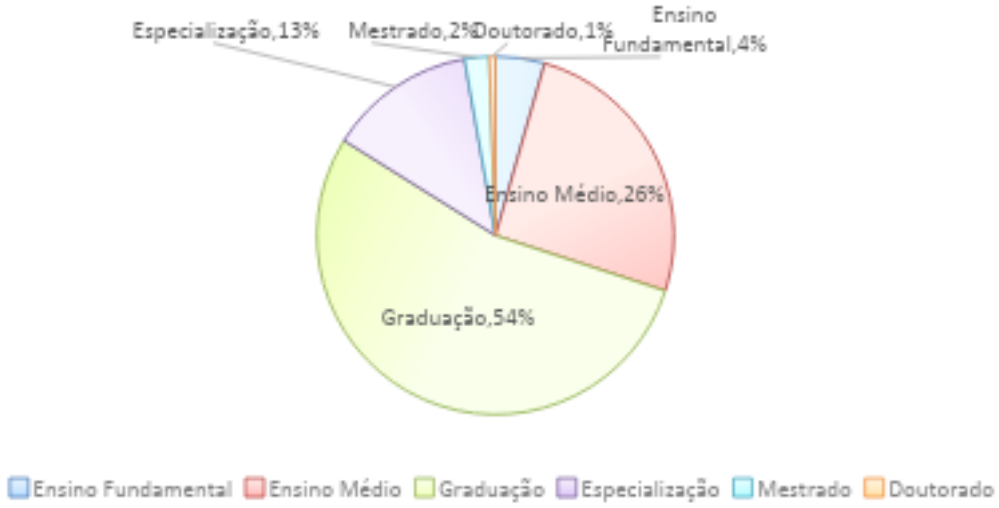


Fonte: Autores (2024)

Com relação ao grau de escolaridade, referente a pergunta 2, representada na Figura 3, das pessoas que responderam ao questionário, observou-se que 2% têm Ensino

fundamental, 26% possuem o Ensino médio, 54% Graduação, 13% Especialização, 2% Mestrado e 1% doutorado. A maioria dos respondentes possui ensino superior, representando a maioria significativa em relação às outras categorias de formação. Isso pode indicar que o público-alvo da pesquisa ou o tema de interesse possuem uma maior relevância, ou acessibilidade para indivíduos com um nível de educação mais elevado.

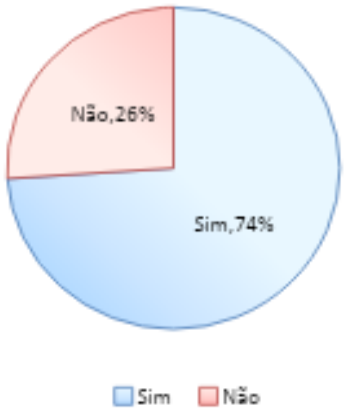
Figura 3 – Distribuição do Grau de escolaridade



Fonte: Autores (2024)

Ao averiguar à opinião das pessoas sobre a terceira questão, representada na Figura 4, sobre elas estarem cientes dos riscos associados ao uso de conexão sem fio sem as devidas medidas de segurança, 74%, diz estar ciente dos riscos, isso indica uma boa conscientização, embora ainda haja uma parcela significativa 26% que não está ciente desses riscos.

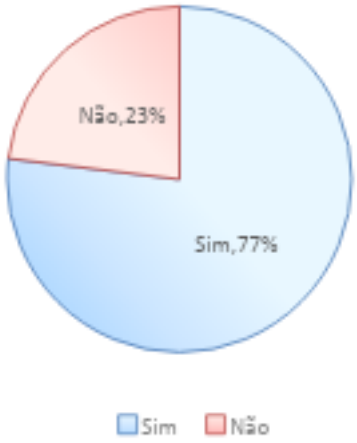
Figura 4 – Risco associados a conexão sem fio



Fonte: Autores (2024)

A quarta questão apontada na Figura 5, é referente ao conhecimento das pessoas sobre a criação de senhas seguras. Ao examinar as respostas sobre a criação de senhas forte 76,9% afirmam que sabem como criar uma senha forte para sua rede sem fio, indicando que a maioria dos usuários tem conhecimento básico de uma das mais importantes práticas de segurança digital, no entanto, ainda existe um grupo de 23,1% que não possui essa informação, o que pode representar uma vulnerabilidade.

Figura 5 – Criação de Senha forte



Fonte: Autores (2024)

Com relação à análise das respostas sobre estratégias para criar senhas forte, mostrada na Figura 6, observou-se que 80% usam letras maiúsculas e minúsculas números e caracteres especiais como estratégia para criar senhas seguras, isso é considerado uma prática exemplar em termos de segurança digital. Um número muito pequeno de pessoas ainda usa senhas constituídas apenas de números 3% ou apenas de letras 2%. Estas são estratégias consideravelmente menos seguras, pois tais senhas são mais fáceis de serem decifradas por ataques de força bruta.

Apesar do conhecimento sobre a importância de senhas fortes e a conscientização sobre os riscos serem altos, ainda há um alto número de usuários que podem não estar aplicando essas práticas corretamente. Isso pode abrir brechas para ataques cibernéticos.

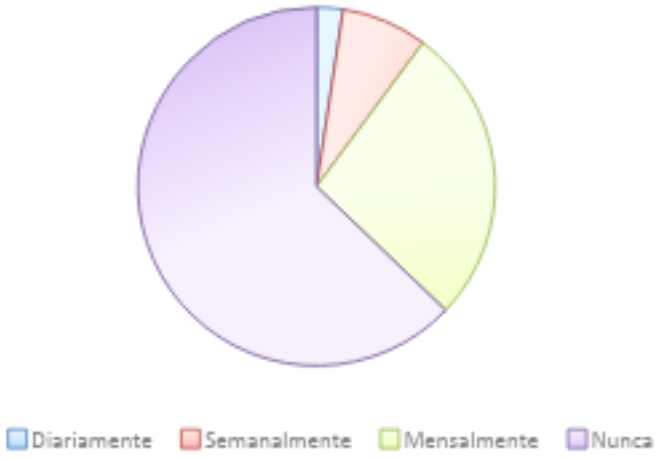
Educação continuada em cibersegurança é crucial, mesmo aqueles que estão cientes dos riscos e conhecem as práticas recomendadas podem se beneficiar de revisões frequentes e atualizações sobre novas ameaças e técnicas de proteção.

Figura 6 – Estratégias para Senhas seguras

Fonte: Autores (2024)

A sexta pergunta, representada na Figura 7, é sobre atualizações de segurança. Ao analisar as respostas, cerca de 2%, das pessoas verifica e aplica atualizações de segurança em seus dispositivos conectados diariamente, enquanto semanalmente 8%, um número ligeiramente maior, 27% atualizam seus dispositivos mensalmente e 63%, a maior parte dos pesquisados, nunca verifica ou aplica atualizações de segurança. Esse é um dado preocupante, ao deixar os dispositivos vulneráveis a ataques cibernéticos.

Figura 7 – Frequência das atualizações de segurança



Fonte: Autores (2024)

A questão de número 7, representada na Figura 8, traz dados sobre Ataques Cibernéticos sofridos. Cerca de 30%, um terço dos respondentes, afirmaram ter sido vítimas de um ataque cibernético por meio de

suas redes domésticas, enquanto não 70%, a maioria, nunca experimentou um ataque cibernético, o que pode ser atribuído tanto à sorte quanto a medidas de segurança eficazes.

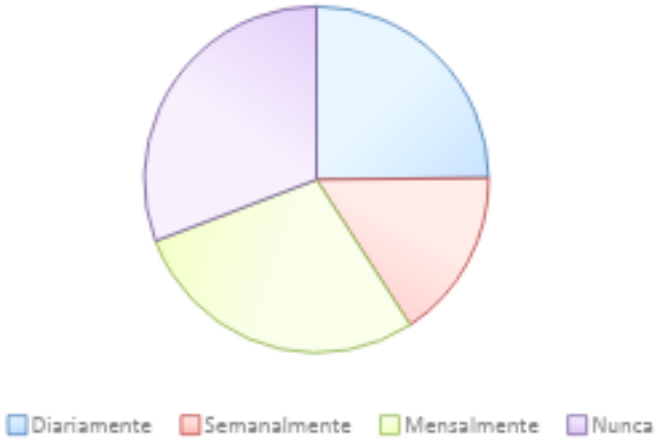
Figura 8 – Vítimas de ataques cibernéticos

Fonte: Autores (2024)

A oitava questão se refere a alteração de configurações de fábrica. As respostas representadas na Figura 9, mostra que 25,4% sempre mudam as configurações de fábrica de seus dispositivos conectados, o que é recomendável para melhorar a segurança, 16,6% fazem isso frequentemente, 29% raramente fazem alterações nas configurações padrão e 30,8%, nunca mudam as configurações de fábrica, mantendo potencialmente as senhas padrão e configurações menos seguras, o que pode facilitar ataques.

Essas respostas indicam uma necessidade significativa de conscientização e melhoria nas práticas de segurança cibernética em redes domésticas. A maioria dos usuários não realiza atualizações regulares de segurança e muitos não alteram as configurações de fábrica, aumentando os riscos de segurança. Dada a proporção relativamente alta de pessoas que já foram vítimas de ataques cibernéticos, essas práticas poderiam ser revisadas e melhoradas para aumentar a proteção geral.

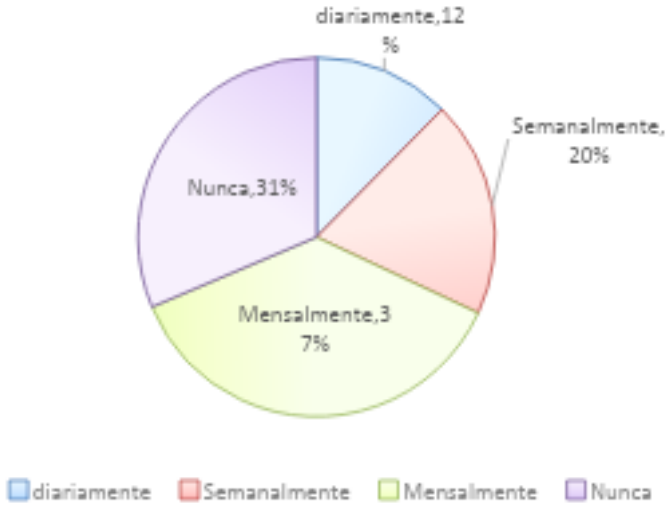
Figura 9 – Alteração de configuração de fábrica



Fonte: Autores (2024)

A análise da última questão sobre a realização de backups, apresentada na Figura 10, revelou os seguintes resultados: 37% realizam backups mensalmente, o que indica uma consciência da importância da proteção de dados, mas sem uma necessidade de atualizações frequentes. Por outro lado, 31% nunca fazem backup, sugerindo falta de conscientização. Outros 20% realizam backups semanalmente, possivelmente devido à maior necessidade de segurança. Finalmente, 12% fazem backups diariamente, o que pode refletir uma dependência crítica dos dados ou uma alta preocupação com sua segurança.

Figura 10 – Realização de backup



Fonte: Autores (2024)

Ao analisar as respostas do questionário e os dados apresentados, é possível traçar relações entre as características pessoais dos participantes e sua relação com a Segurança da Informação aplicada a redes domésticas. Isso será explorar em conjunto com os principais tipos de ataques a redes domésticas previamente mencionados.

- Senhas fracas e Estratégias de Criação de Senhas (Questões 4 e 5): A maioria dos participantes afirma estar ciente dos riscos associados ao uso de senhas fracas, e a grande parte deles sabe como criar uma senha forte. No entanto, ainda há uma parcela que não tem esse conhecimento ou não aplica essa prática corretamente, o que pode deixar suas redes vulneráveis a ataques de força bruta.
- Falta de atualização de *firmware* (Questão 6): Um número alarmante de participantes nunca verifica ou aplica atualizações de segurança em seus dispositivos conectados. Isso representa uma grande vulnerabilidade, pois dispositivos desatualizados são alvos fáceis para exploração de vulnerabilidades e ataques cibernéticos.
- Configurações padrão de fábrica (Questão 8): Uma proporção significativa de participantes não altera as configurações padrão de fábrica de seus dispositivos conectados. Isso aumenta os riscos de ataques, pois senhas padrão e configurações de fábrica são conhecidas e exploradas por *hackers*.

Ao relacionar esses pontos com os dados pessoais dos participantes, observou-se que a conscientização sobre práticas de segurança digital é alta, especialmente entre aqueles com maior nível de escolaridade. No entanto, ainda há uma lacuna na implementação efetiva dessas práticas, especialmente entre os mais jovens e aqueles com menor nível de escolaridade. Isso destaca a necessidade de educação contínua em cibersegurança para todos os públicos. Para melhorar a segurança em redes domésticas, é crucial:

- Promover conscientização sobre a importância de senhas fortes, atualizações regulares de *firmware* e configurações personalizadas de segurança.
- Oferecer treinamento e recursos educacionais acessíveis para ensinar aos usuários como implementar e manter práticas de segurança eficazes.

- Incentivar o uso de criptografia de dados em redes domésticas e o cuidado ao utilizar redes, Wi-Fi públicas.
- Facilitar o acesso a informações e ferramentas para proteger dispositivos IoT e garantir que eles sejam regularmente atualizados e configurados corretamente.

Essas medidas podem ajudar a reduzir a vulnerabilidade das redes domésticas e proteger as informações pessoais dos usuários contra os ataques cibernéticos.

À medida que as redes domésticas se tornarem mais complexas, com um número crescente de dispositivos conectados, é fundamental que os usuários adotem práticas de segurança abrangentes, incluindo senhas fortes, criptografia de dados e manutenção regular de firmware. Essas medidas são essenciais para reduzir as vulnerabilidades e proteger as informações pessoais contra ameaças crescentes.

5. Considerações Finais

O presente artigo investigou a evolução e a importância das redes domésticas na sociedade contemporânea, ressaltando a necessidade premente de segurança cibernética nesse contexto. Embora as redes domésticas tenham oferecido vantagens, como o acesso facilitado à Internet, a segurança dessas redes tornou-se uma preocupação crucial devido ao aumento das ameaças virtuais, como invasões e vazamento de informações pessoais.

Os objetivos do projeto de pesquisa propuseram fornecer informações e diretrizes específicas para conscientizar os usuários sobre a importância da segurança em suas redes domésticas, destacando a necessidade de ativar recursos de segurança nos roteadores e a implementação de medidas adicionais, como *firewalls* e softwares antivírus.

A análise das respostas do questionário revelou algumas tendências e preocupações importantes. Apesar do alto nível de conscientização sobre práticas de segurança cibernética, houve uma lacuna notável entre o conhecimento e a aplicação efetiva dessas práticas. A maioria dos respondentes não realizou atualizações de segurança de forma regular, o que é preocupante, considerando que essas atualizações são cruciais para proteger os dispositivos contra vulnerabilidades. Além disso, a manutenção das configurações padrão em muitos dispositivos elevou o risco de ataques, e uma parcela significativa dos participantes já foi vítima de incidentes cibernéticos.

Portanto, estratégias de educação e conscientização devem ser continuamente atualizadas e adaptadas para abordar essas lacunas de maneira eficaz, assegurando que todos os usuários possam proteger-se contra ameaças cibernéticas. Empresas e organizações que oferecem produtos e serviços relacionados à tecnologia e segurança digital devem considerar esses resultados ao desenvolver materiais educativos e funcionalidades de produtos, tornando as configurações de segurança mais acessíveis e incentivando práticas mais seguras entre os usuários.

Referências

CHAVATTE, J. C. Segurança em redes domésticas no Windows. 2024. Disponível em: https://home.vexorsolucoes.tech/EscudoDigital/seguranca-em-redes-domesticas-no-windows Acesso em 22 abr. 2024.

FASTERCAPITAL. **Sem fio: explorando as maravilhas da atualização da tecnologia Wi Fi.** 14 Mar 2024. Disponível em: https://fastercapital.com/pt/contente/Sem-fio--explorando-as-maravilhas-da-atualizacao-da-tecnologia-Wi-Fi.html. Acesso em: 29 abr. 2024.

FERNANDES, G. A.; PINHO, J. G.; SIQUEIRA, T. R.; GONÇALVES, G. F.; CRISTOVAO, A. M. **A importância da segurança de redes no cenário atual**: estudo com método Delphi. XXXV ENCONTRO NACIONAL DE ENGENHARIA DE PRODUCAO Perspectivas Globais para a Engenharia de Produção Fortaleza, CE, Brasil, 13 a 16 de outubro de 2015. Disponível em: https://abepro.org.br/biblioteca/TN_STO_213_262_27211.pdf . Acesso em: 23 nov. 2023.

MACEDO, R. T. FRANCISCATTO, R. CUNHA, G. B. D. BERTLINI, C. **Redes de computadores** – 1. ed. – Santa Maria, RS: UFSM, NTE, 2018. 1 e-book. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/18351/Curso_Lic-Comp_Redes-Computadores.pdf?sequence=1&isAllowed=y. Acesso em: 18 abr. 2024.

MANCILLA, O. R. **A importância da Internet para o desenvolvimento das vendas no Brasil**. Trabalho de conclusão de curso, 2014. Disponível em: https://cepein.femanet.com.br/BDigital/arqTccs/1111390013.pdf. Acesso em: 7 nov. 2023.

MARCONDES, E. **O que é uma rede de computadores doméstica**. Disponível em: http://ctrlaltdelalltv.blogspot.com/2008/07/o-que-uma-rede-de-computadores-domstica.html?m=1 . Publicado em 20 de julho de 2008. Acesso em: 7 nov. 2023.

MASCARENHAS NETO, P. T. ARAUJO, V. J. **Segurança da Informação: uma visão sistêmica para implantação em organizações**. João Pessoa: Editora da UFPB, 2019. Disponível em: http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/download/209/75/905-1?inline=1. Acesso em: 11 abr. 2024.

MIRANDA, M. S. **Segurança em redes wi-fi**. Publicado em 25 de setembro de 2017. Disponível em: https://blog.winco.com.br/seguranca-em-redes-wi-fi/ . Acesso em: 7 nov. 2023.

VICENTINI, L.; LANZONI, E.; FRANZOTTI, V.; YONENAGA, W. H. **Introdução da tecnologia de voz sobre IP em redes corporativas**. XXXIII - **Congresso Brasileiro de ensino de engenharia**. Ano 2005. Disponível em: : https://www.abenge.org.br/cobenge/legado/arquivos/14/artigos/SP-9-22177077877-1118945677392.pdf . Acesso em: 23 nov. 2023.