UNIVERSIDADE ESTADUAL DO PIAUÍ

CAMPUS DRA. JOSEFINA DEMES

CURSO DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

IRANILDO CHAGAS DE SOUSA

A SEGURANÇA DE DISPOSITIVOS IOT E COMO VULNERABILIDADES PODEM SER EXPLORADAS POR HACKERS

FLORIANO

2025

IRANILDO CHAGAS DE SOUSA

A SEGURANÇA DE DISPOSITIVOS IOT E COMO VULNERABILIDADES PODEM SER EXPLORADAS POR HACKERS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciências da Computação da Universidade Estadual do Piauí, como requisito parcial à obtenção do grau de bacharel em Ciência da Computação.

Orientador: Me. Danilo Borges da Silva.

FLORIANO

2025

A Segurança de Dispositivos IoT e como Vulnerabilidades podem ser Exploradas por Hackers

Iranildo Chagas de Sousa[1], **Danilo Borges da Silva**[1]

[1]Universidade Estadual do Piauí (UESPI)
Floriano – PI – Brasil

iranildocdes@aluno.uespi.br, danilo@prp.uespi.br

Abstract. *The security of Internet of Things (IoT) devices faces critical challenges due to vulnerabilities often exploited by hackers. Through a methodological approach based on literature review and secondary data analysis, this work identifies key weaknesses, evaluates current protection practices, proposes enhancements, and examines the impact of cyberattacks across various sectors. Findings reveal that inadequate updates and poor authentication management are recurring issues, underscoring the need for more effective strategies and stakeholder collaboration to mitigate risks and advance the field.*
Keywords: *IoT Security. Vulnerabilities. Risk Mitigation.*

Resumo. *A segurança de dispositivos IoT (Internet of Things) enfrenta desafios críticos devido a vulnerabilidades frequentemente exploradas por hackers. Este trabalho, conduzido por meio de revisão de literatura e análise de dados secundários, identifica fraquezas, avalia práticas de proteção, propõe melhorias e analisa o impacto dos ataques em diferentes setores. Os resultados destacam que a ausência de atualizações regulares e a gestão inadequada de autenticação são problemas recorrentes, reforçando a urgência de estratégias mais eficazes e colaboração entre partes interessadas para mitigar riscos e promover avanços na área.*
Palavras-chave: *Segurança de IoT. Vulnerabilidades. Mitigação de Riscos.*

1. Introdução

O avanço da conectividade proporcionado pela Internet das Coisas (*Internet of Things* – IoT) transformou o cotidiano, trazendo conveniência, automação e eficiência a diversos setores. No entanto, essa crescente integração tecnológica também expôs um novo panorama de riscos e desafios relacionados à segurança. Dispositivos IoT, muitas vezes projetados com foco na funcionalidade e facilidade de uso, podem apresentar vulnerabilidades exploráveis por agentes mal-intencionados. Esses ataques podem resultar em interrupções de serviço, comprometimento de dados confidenciais e até mesmo impactos em infraestruturas críticas.

A ausência de atualizações regulares, configurações inadequadas e mecanismos frágeis de autenticação ampliam significativamente o potencial de exploração em dispositivos IoT. Além disso, a limitada capacidade computacional de muitos desses dispositivos impede a adoção de mecanismos de segurança avançados, demandando soluções que equilibrem proteção e desempenho. Nesse contexto, compreender essas vulnerabilidades

e desenvolver estratégias eficazes para mitigá-las é essencial para assegurar a segurança em um ambiente cada vez mais interconectado (CARVALHO; SANTOS; GONÇALVES, 2022).

A conscientização sobre riscos e a adoção de práticas adequadas são passos essenciais para fortalecer a proteção em dispositivos IoT. Medidas como auditorias regulares e *frameworks* adaptados às especificidades desses dispositivos têm se mostrado eficazes na mitigação de vulnerabilidades. A colaboração entre fabricantes, pesquisadores e profissionais de segurança é fundamental para desenvolver tecnologias inovadoras e proativas que enfrentem esses desafios (LOPES; ROSSATO; SILVA, 2023).

Dada a complexidade dos desafios de segurança em dispositivos IoT, é indispensável uma abordagem sistemática para compreender e mitigar suas vulnerabilidades. Este estudo analisa essas fragilidades e suas implicações na segurança cibernética, contribuindo tanto para o avanço acadêmico quanto para a formulação de diretrizes práticas úteis a pesquisadores, fabricantes e profissionais da área.

Este trabalho tem como objetivo principal investigar de forma abrangente as vulnerabilidades dos dispositivos IoT, destacando como elas são exploradas por hackers e os impactos resultantes em diferentes setores. Para atingir essa meta, a pesquisa se concentra em identificar as principais fraquezas desses dispositivos, detalhando suas origens e consequências. Além disso, avalia a eficácia das práticas de segurança atuais, como protocolos e frameworks, propondo melhorias baseadas em evidências.

A partir dessa análise, recomendações robustas são desenvolvidas, considerando tanto aspectos técnicos quanto a viabilidade prática, com o intuito de promover uma segurança mais eficaz. O estudo também examina os impactos dos ataques cibernéticos em contextos variados, como residências inteligentes, instalações industriais e infraestruturas governamentais, evidenciando a necessidade de soluções personalizadas para diferentes cenários.

A relevância desta pesquisa está em evidenciar a urgência de enfrentar as falhas de segurança em uma tecnologia amplamente integrada ao cotidiano das pessoas e às operações críticas de diversos setores. Ao abordar os riscos associados aos dispositivos IoT, o estudo busca preencher lacunas na literatura, especialmente no que diz respeito a métodos eficazes para mitigar vulnerabilidades e proteger esses dispositivos contra ameaças cibernéticas.

Além de contribuir para o avanço do conhecimento científico, este trabalho explora aplicações práticas das estratégias de segurança propostas, oferecendo soluções viáveis para diferentes contextos. Essas abordagens não apenas mitigam riscos imediatos, mas também estabelecem uma base sólida para futuras investigações, fortalecendo continuamente a infraestrutura cibernética global.

As próximas seções deste trabalho estão organizadas da seguinte forma. A Seção 2 descreve a metodologia utilizada. Na Seção 3, são apresentados os trabalhos obtidos da revisão de literatura e seus principais achados. A Seção 4, apresenta os achados compilados da pesquisa, detalhando as implicações das vulnerabilidades identificadas e as propostas de melhorias. Por fim, na Seção 5, oferece um resumo das contribuições do estudo e sugere direções para futuras pesquisas na área.

2. Metodologia

A metodologia adotada foi uma revisão narrativa da literatura, incluindo uma análise detalhada de textos relacionados ao tema. As informações foram coletadas por meio de bases de dados acadêmicas como *Scielo*, *Capes* e *Google Acadêmico*, além de livros e periódicos científicos, considerando materiais em português, inglês e espanhol.

Conforme apontado por Dourado e Ribeiro (2023), essa estratégia de revisão literária fornece uma base sólida para os dados, pois sintetiza contribuições de diversas fontes selecionadas, ajudando a identificar lacunas em estudos anteriores.

Para a compilação da bibliografia, foi realizada uma análise qualitativa dos textos e uma leitura detalhada dos resumos de cada documento. A seleção temporal do material trouxe publicações entre 2019 a 2024, com exceções para trabalhos de caráter clássico, garantindo assim uma compreensão atualizada e abrangente do tema, fortalecendo a base para os resultados da pesquisa e enriquecendo o corpo científico relacionado ao assunto.

3. Trabalhos Relacionados

A IoT é uma inovação tecnológica que oferece conectividade e automação avançadas, sendo mais que notório, a mesma apresenta também desafios significativos no tocante à segurança e privacidade. A ausência de padrões entre dispositivos de variados fabricantes maximiza a complexidade de gerenciamento e o risco de ataques cibernéticos. Segundo Carvalho, Santos e Gonçalves (2022), para mitigar essas ameaças, é crucial que se adote práticas de segurança como criptografia, autenticação forte e atualizações constantes.

Deste modo, o futuro da IoT depende de sua capacidade de evoluir de maneira segura e responsável sem perder de vista os meios de segurança adequados. A pesquisa e o desenvolvimento avançado das tecnologias de segurança são vitais para atenuar vulnerabilidades e livrar os usuários dos ataques cibernéticos. Devido à ausência de atualizações rotineiras e correção para normalizar falhas de segurança, os riscos se tornam elevados, propiciando que dispositivos desatualizados se tornem alvos vulneráveis a software conhecidos ou código malicioso que exploram falhas deixadas por esses dispositivos (CARVALHO; SANTOS; GONÇALVES, 2022).

Os sistemas de IoT desempenham um papel importante no cenário atual, pois promovem uma conexão direta com dispositivos do meio digital. Não obstante, esses sistemas têm se mostrado vulneráveis a ataques cibernéticos, revelando falhas na segurança que, muitas vezes, não são abordadas adequadamente durante o ciclo de desenvolvimento. Essa negligência tem gerado muitas consequências aos usuários, pois os deixam à mercê dos mais variados ataques do mundo digital (LOPES; ROSSATO; SILVA, 2023).

A IoT envolve dispositivos sem fio com capacidades computacionais limitadas, onde a falta de criptografia no envio de dados deixa esses dispositivos vulneráveis e alvos de ataques. A detecção dessas vulnerabilidades geralmente se baseia em bases de dados que listam como conhecidas, ou seja, a baixa capacidade computacional, que os tornam, alvos fáceis (BREZOLIN et al., 2022).

A seguir, serão apresentados diversos trabalhos sobre: Vulnerabilidades Comuns em Dispositivos IoT (Seção 3.1); Práticas de Segurança e Mitigação de Riscos (Seção 3.2); e Impacto e Implicações de Ataques a Dispositivos IoT (Seção 3.3).

3.1. Vulnerabilidades Comuns em Dispositivos IoT

A prevalência de senhas fracas e padrão nos dispositivos constitui um dos principais riscos, facilitando ataques de acesso não autorizado (CARVALHO; SANTOS; GONÇALVES, 2022). Esta seção explora as práticas correntes e as deficiências observadas na gestão de senhas, além de sugerir métodos para melhorar a segurança através de uma gestão de autenticação mais eficiente.

Muitos dispositivos são comercializados com senhas facilmente acessíveis e, frequentemente, os usuários finais não alteram essas credenciais predefinidas, deixando uma abertura clara para explorações mal-intencionadas. A substituição de senhas padrão por opções personalizadas e complexas é uma medida inicial vital, embora muitas vezes negligenciada (BREZOLIN et al., 2022).

A implementação de sistemas de Autenticação Multi Fator (do inglês, *Multi-Factor Authentication* – MFA) apresenta-se como uma solução robusta para reforçar a segurança, já que ela exige que o usuário forneça dois ou mais fatores de verificação antes de conceder acesso, complicando os esforços de intrusão. No entanto, há limitações de hardware e necessidades de usabilidade que podem comprometer a implementação de medidas de segurança rigorosas (VIVIANI; RODRIGUEZ, 2022).

Para superar essas barreiras, recomenda-se o desenvolvimento de políticas de segurança que incluam a educação dos usuários sobre a importância das senhas e a utilização de MFA sempre que possível. Também é imprescindível que os fabricantes incorporem requisitos mais restritos na fase de projeto, garantindo que incentivem e facilitem a configuração segura por parte dos usuários (CARVALHO; SANTOS; GONÇALVES, 2022).

A configuração inadequada inicial, que prioriza a facilidade de instalação, expõe os dispositivos a diversas ameaças, como portas de rede não seguras e a falta de segmentação, permitindo que atacantes se movam livremente pela infraestrutura. Para garantir a segurança da rede, é essencial implementar *firewalls* robustos, segmentação e sistemas de detecção de intrusões. Essas práticas evitam a propagação de ataques para áreas críticas. Dada a diversidade dos dispositivos, é fundamental que administradores de rede ajustem as configurações de segurança conforme o ambiente e o tipo de dispositivo, sem comprometer a funcionalidade (BREZOLIN et al., 2022).

Recomenda-se também que os fabricantes integrem melhores práticas de segurança de rede no projeto e desenvolvimento de produtos, como a oferta de guias de configuração detalhados e ferramentas automatizadas que ajudam na implementação de uma configuração segura desde a inicialização (VIVIANI; RODRIGUEZ, 2022). A criptografia e a proteção de dados em dispositivos IoT representam áreas críticas que frequentemente revelam inadequações, comprometendo a integridade e a confidencialidade das informações transmitidas ou armazenadas. Em muitos casos, as chaves não são armazenadas de maneira segura ou são geradas e distribuídas sem os devidos cuidados, o que pode facilitar o acesso indevido por pessoas não autorizadas. A falta de políticas de renovação e revogação de chaves também é uma preocupação, pois permite que chaves comprometidas continuem a ser usadas, aumentando o período de vulnerabilidade dos dispositivos (NOBREGA et al., 2024).

Para superar essas barreiras, é preciso que os desenvolvedores implementem

políticas rigorosas de criptografia, incluindo o uso de algoritmos aprovados por agências de normatização e a adoção de práticas sólidas de gestão de chaves. Além disso, deve-se incentivar a pesquisa e o desenvolvimento de soluções de criptografia que sejam adequadas às limitações específicas, equilibrando segurança e desempenho (GOMES, 2019). O fortalecimento da criptografia e da proteção de dados é, portanto, relevante para assegurar a proteção e a privacidade das informações em um mundo cada vez mais conectado. As medidas adotadas protegem os dados dos usuários e fortalecem a confiança no uso da tecnologia IoT em aplicações sensíveis e críticas.

A variedade de hardware e sistemas operacionais utilizados cria uma complexidade no desenvolvimento e distribuição de *patches* que sejam compatíveis e eficazes em todos os contextos. Esta fragmentação dificulta a aplicação uniforme de atualizações, aumentando o risco de exposição a vulnerabilidades conhecidas que não são corrigidas de maneira tempestiva (BREZOLIN et al., 2022). Outro desafio é a limitação de recursos dos próprios dispositivos, que muitas vezes possuem capacidade de processamento e armazenamento insuficientes para suportar atualizações frequentes ou robustas. Esse cenário é agravado pela falta de uma infraestrutura de gerenciamento de atualizações centralizada, fazendo com que muitos permaneçam com software desatualizado por longos períodos, se não indefinidamente (GOMES, 2019).

Estratégias como atualizações incrementais e o uso de micro serviços podem facilitar a implementação de melhorias de segurança sem sobrecarregar os dispositivos. Além disso, é imperativo que fabricantes e desenvolvedores implementem políticas de ciclo de vida de software que incluam suporte estendido para atualizações, garantindo que todos os dispositivos recebam os *patches* necessários durante toda sua vida útil (VIVIANI; RODRIGUEZ, 2022).

Para mitigar esses riscos, é preciso implementar práticas de desenvolvimento seguro desde o início do projeto de interfaces, englobando a aplicação de princípios de segurança como a minimização de dados, onde apenas as informações necessárias são expostas, e a validação rigorosa de todas as entradas recebidas pelas interfaces. Além disso, a autenticação e autorização devem ser reforçadas utilizando *tokens* de acesso, certificados e outras técnicas que assegurem que apenas usuários e dispositivos verificados possam acessar funcionalidades críticas (GOMES, 2019).

3.2. Práticas de Segurança e Mitigação de Riscos

A MFA combina algo que o usuário sabe (como uma senha), algo que o usuário possui (como um *token* de hardware ou um código enviado para um dispositivo móvel), e algo que o usuário é (como dados biométricos). A utilização de múltiplos fatores de autenticação complica os esforços dos invasores, pois mesmo que uma das credenciais seja comprometida, as outras ainda protegerão o acesso (BOECKL et al., 2019).

O uso de gestão dinâmica de senhas, onde as senhas são regularmente alteradas e devem atender a critérios rigorosos de complexidade, reduz a janela de oportunidade para que senhas roubadas ou descobertas sejam utilizadas em ataques. No mais, a implementação de políticas de bloqueio automático após tentativas de login fracassadas pode deter ataques de força bruta, limitando o número de vezes que as senhas podem ser testadas por um atacante (SANTOS, 2020).

A biometria oferece outra camada de segurança, utilizando características físicas

únicas dos usuários, como impressões digitais, reconhecimento facial ou de íris, para reforçar a autenticação. Esses métodos são cada vez mais adotados devido à sua dificuldade de falsificação e à conveniência para o usuário. Contudo, é importante que os dados biométricos sejam armazenados e processados com altos padrões de segurança para prevenir qualquer possibilidade de comprometimento (LOPES; ROSSATO; SILVA, 2023).

A implementação de *firewalls* e sistemas de detecção de intrusão servem como a primeira linha de defesa contra acessos não autorizados e ataques maliciosos, protegendo dispositivos e dados sensíveis de explorações externas. Eles atuam como barreiras que impedem o acesso não autorizado, enquanto permitem comunicações legítimas. Para dispositivos IoT, onde o volume e a diversidade de tráfego podem ser grandes, *firewalls* configurados adequadamente são cruciais para bloquear tentativas de acesso malicioso e filtrar tipos de tráfego potencialmente perigosos (LIMA, 2023).

Os sistemas de detecção de intrusão complementam os *firewalls* ao identificar atividades suspeitas dentro da rede, uma vez que eles monitoram continuamente o tráfego de rede em busca de padrões anormais que possam indicar uma tentativa de intrusão ou uma violação de segurança. Estes sistemas utilizam tanto assinaturas de ataques conhecidos quanto técnicas de aprendizado de máquina para detectar anomalias, proporcionando uma camada adicional de segurança ao identificar ameaças que podem não ser bloqueadas apenas por *firewalls* (BOECKL et al., 2019).

A configuração deve ser adaptada especificamente ao ambiente, considerando o tipo de dispositivos e a natureza das comunicações que normalmente ocorrem dentro da rede, o que envolve a definição de políticas de segurança que refletem as necessidades específicas e os riscos associados a cada dispositivo, bem como a segmentação da rede para isolar sistemas mais críticos ou vulneráveis. A manutenção contínua inclui a atualização regular das regras de *firewalls* e das assinaturas de detecção de intrusão, além do ajuste contínuo das políticas de segurança baseadas nas novas vulnerabilidades descobertas e nas mudanças no ambiente operacional (SANTOS, 2020).

Medidas como fechaduras biométricas ou eletrônicas, cartões de acesso e códigos numéricos podem ser empregados para garantir que apenas pessoal autorizado tenha acesso aos dispositivos. A gestão de acesso deve ser rigorosamente monitorada e revisada periodicamente para adaptar-se a mudanças no pessoal ou nos níveis de autorização (LIMA, 2023). A vigilância visual ajuda a deter invasores e fornece registros visuais que podem ser usados para investigações após incidentes. O teste de penetração regular é uma prática crítica para a proteção de sistemas, especialmente em um ambiente de dispositivos IoT, onde novas vulnerabilidades e métodos de ataque são constantemente desenvolvidos. Esta técnica de avaliação de defesa envolve simulações de ataque meticulosas projetadas para descobrir e explorar fraquezas nos sistemas.

Ao simular ataques externos e internos, os testes de penetração ajudam a identificar pontos fracos no software e hardware e também nas práticas operacionais que podem comprometer a proteção de dispositivos IoT. Esta análise abrangente permite que as organizações ajustem suas estratégias de defesa, fortalecendo as barreiras contra ataques reais (TENAGLIA, 2024).

O teste também ajuda a avaliar a capacidade de resposta da organização a incidentes de segurança, como a eficiência dos protocolos de resposta a incidentes, a rapidez com

que a equipe pode conter e mitigar um ataque, e a robustez dos processos de recuperação. Tais testes são fundamentais para garantir que a organização possa prevenir a maioria dos ataques e responder eficazmente àqueles que são inevitáveis (GOMES, 2022).

Muitos padrões de segurança e regulamentos exigem demonstrações regulares de que as infraestruturas críticas estão protegidas contra violações conhecidas e emergentes. Por meio dos testes de penetração, as organizações podem documentar suas iniciativas de segurança e demonstrar conformidade com os requisitos regulatórios, evitando multas e outras penalidades (LIMA, 2023).

3.3. Impacto e Implicações de Ataques a Dispositivos IoT

Os ataques cibernéticos em ambientes residenciais envolvendo dispositivos IoT têm implicações que vão além do simples inconveniente, afetando a privacidade, a segurança e a confiança dos indivíduos em suas próprias casas. À medida que mais dispositivos domésticos são conectados à Internet, desde câmeras até eletrodomésticos inteligentes, o potencial de danos resultantes de violações da proteção aumenta consideravelmente (SILVA, 2021).

Câmeras e microfones conectados podem ser hackeados para espionar os moradores, coletando informações pessoais sensíveis sem o seu consentimento. Essa violação da privacidade compromete a segurança pessoal, e também pode ter repercussões psicológicas, como ansiedade e desconfiança em relação à tecnologia usada diariamente (LEMA; FREITAS, 2021). Ataques a dispositivos domésticos inteligentes podem resultar em prejuízos financeiros diretos. Por exemplo, a manipulação de sistemas de automação residencial pode levar a gastos excessivos de energia ou danos a equipamentos valiosos. *Hackers* podem aumentar o uso de sistemas de aquecimento ou resfriamento, resultando em contas de energia inflacionadas, ou podem causar falhas operacionais que exigem reparos ou substituições caras (BROCHADO et al., 2023).

Sistemas de fechaduras inteligentes e alarmes, se violados, podem permitir acesso físico não autorizado a residências, expondo os habitantes a riscos de furto ou pior. A habilidade de controlar remotamente tais dispositivos oferece aos criminosos uma maneira de entrar em casas sem necessidade de força física (DIAS; ARAÚJO, 2023).

As brechas de segurança frequentemente resultam em custos diretos, que incluem despesas com a identificação e correção da falha de segurança, a recuperação de dados perdidos ou corrompidos e as medidas legais necessárias para responder a litígios ou multas impostas por reguladores. Igualmente, as organizações podem enfrentar a necessidade de investir em novas tecnologias de proteção e na capacitação de funcionários, visando fortalecer suas defesas contra futuros ataques (SOARES; RABÊLO, 2024).

A perda de confiança do consumidor é um dos maiores impactos econômicos, pois pode levar a uma diminuição sustentada nas receitas, uma vez que clientes preocupados com a defesa de seus dados pessoais podem optar por levar seu negócio para concorrentes, resultando em uma queda de participação de mercado para a empresa afetada. A reputação da marca, uma vez danificada, pode requerer anos e recursos financeiros consideráveis para ser restaurada (SILVA, 2021).

Após uma brecha de segurança, é comum que as ações de uma empresa sofram uma queda imediata, refletindo a resposta negativa do mercado. A volatilidade resultante

pode afetar o valor de mercado da empresa de forma prolongada, dependendo da gravidade da brecha e da eficácia da resposta da empresa (SOUZA, 2024). As brechas têm implicações econômicas mais amplas, afetando as empresas individuais, setores inteiros e, em alguns casos, economias nacionais. Por exemplo, ataques a infraestruturas críticas podem resultar em perturbações econômicas generalizadas, como interrupções no fornecimento de serviços essenciais e aumentos nos custos de seguros (LEMA; FREITAS, 2021).

As organizações devem perceber que o custo de prevenção é frequentemente muito menor do que o custo de remediar suas consequências. Adotar uma abordagem robusta e holística para a proteção cibernética é essencial para proteger os dados e sistemas organizacionais e para salvaguardar a saúde econômica da empresa e a confiança de seus *stakeholders* (BROCHADO et al., 2023).

As abordagens legais e regulamentações ajudam na resposta a incidentes de segurança, estabelecendo regras para proteger dados e infraestruturas (SOARES; RABÊLO, 2024). Leis como o GDPR (*General Data Protection Regulation*) na União Europeia e o HIPAA (*Health Insurance Portability and Accountability Act*) nos Estados Unidos impõem requisitos rigorosos para a proteção de dados pessoais e de saúde. Elas exigem que as organizações adotem medidas preventivas, realizem avaliações de risco e preservem a privacidade dos dados, sob pena de penalidades. Além disso, essas regulamentações exigem que as brechas sejam notificadas, como no caso do GDPR, que obriga o reporte de violações em até 72 horas após sua descoberta, garantindo uma resposta rápida para minimizar danos (SOUZA, 2024).

Ao exigir que as organizações informem os afetados por violações de segurança, os regulamentos promovem uma maior consciência sobre os riscos de segurança cibernética entre consumidores e forçam as empresas a manterem altos padrões de proteção de dados. Esta abordagem protege os indivíduos e eleva o nível de confiança do público em tecnologias e serviços digitais (DIAS; ARAÚJO, 2023).

A aplicação destas leis é facilitada através de agências reguladoras que têm autoridade para investigar violações, impor sanções e orientar as organizações sobre como melhorar suas práticas de segurança. Este sistema de fiscalização e penalidade serve como um forte dissuasor contra a negligência em cibersegurança e ajuda a estabelecer um ambiente digital mais seguro (SOARES; RABÊLO, 2024).

4. Resultados e Discussões

Os resultados obtidos nesta investigação bibliográfica elucidam várias dimensões cruciais relacionadas às vulnerabilidades dos dispositivos IoT e as estratégias para mitigar esses riscos. Se revelou que a insegurança das credenciais de acesso está entre as falhas mais prevalentes, onde senhas fracas ou padrões são utilizadas repetidamente, facilitando o acesso não autorizado. Este achado sublinha a necessidade de sistemas de autenticação mais robustos, que incorporem métodos multifatoriais e gestão dinâmica de credenciais.

Muitos dispositivos IoT são implantados com configurações de fábrica inadequadas para ambientes operacionais reais, o que os expõe a riscos adicionais. Este aspecto destaca a importância de customizar a segurança de acordo com o contexto específico de uso, bem como a necessidade de ferramentas automatizadas que possam auxiliar os usuários na configuração segura.

A análise dos impactos de ataques a dispositivos IoT demonstrou que as consequências vão além da perda de dados ou funcionalidade, afetando a integridade física e a confiança nos sistemas digitais como um todo. Os danos podem ser extensos, especialmente quando infraestruturas críticas estão envolvidas, sugerindo uma reavaliação das estratégias de segurança em níveis macro e micro.

A discussão dos resultados aponta para uma série de recomendações práticas e diretrizes que podem ser adotadas por fabricantes, desenvolvedores e usuários finais. Entre estas: a implementação de uma governança de segurança mais integrada e a promoção de uma cultura de segurança consciente emergem como elementos chave. Tais medidas elevam o nível de proteção nos indivíduos e fortalecem a resiliência da rede IoT.

5. Considerações Finais

Para atingir as metas estabelecidas, esta pesquisa conduziu uma investigação detalhada sobre a segurança de dispositivos IoT e como vulnerabilidades, nos mesmos, podem ser exploradas por *hackers*, por meio de uma revisão bibliográfica extensa e rigorosa. As fontes selecionadas proporcionaram uma perspectiva abrangente sobre o assunto e facilitaram a avaliação das evidências coletadas.

Ao concluir o estudo, constatou-se que a grande maioria dos dispositivos continua vulnerável a múltiplos tipos de ataques cibernéticos, corroborando as hipóteses iniciais de que muitas das práticas de segurança atuais são insuficientes para lidar com as ameaças contemporâneas. As análises realizadas destacam a prevalência de problemas relacionados à gestão de autenticações e à falta de atualizações de proteção regulares, enfatizando a necessidade crítica de melhorias nestas áreas.

No entanto, a continuidade das pesquisas é importante para desenvolver soluções mais eficazes e adaptadas às novas realidades tecnológicas. Este trabalho também destaca a importância de uma colaboração mais estreita entre fabricantes de dispositivos, desenvolvedores de software e profissionais de segurança cibernética, visando uma abordagem holística e integrada que possa garantir a defesa dos dispositivos IoT em um cenário de ameaças em constante evolução.

Referências

BOECKL, K. et al. Considerações para gerenciar riscos de privacidade e segurança cibernética na Internet das Coisas (IoT). *Artigo de Diário*, 2019. 5, 6

BREZOLIN, U. Q. et al. Um método para detecçao de vulnerabilidades através da análise do tráfego de rede IoT. In: SBC. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*. [S.l.], 2022. p. 447–460. 3, 4, 5

BROCHADO, L. A. d. S. et al. Segurança de dispositivos IoT: Análise de vulnerabilidades de uma câmera IP. *Artigo de Diário*, Florianópolis, SC., 2023. 7, 8

CARVALHO, A. F. A. d.; SANTOS, C. M. L.; GONÇALVES, L. V. Segurança em IoT. *Artigo de Diário*, 2022. 2, 3, 4

DIAS, K. W. W.; ARAÚJO, F. C. de. O desafio da regulamentação da Internet das Coisas – IoT. *Global Dialogue*, v. 6, n. 3, p. 138–152, 2023. 7, 8

DOURADO, S.; RIBEIRO, E. Metodologia qualitativa e quantitativa. *Editora chefe Profª Drª Antonella Carvalho de Oliveira Editora executiva Natalia Oliveira Assistente editorial*, p. 12, 2023. 3

GOMES, E. Mitigação de riscos para Internet das Coisas – IoT com uso de honeypot de baixa interatividade. *Artigo de Diário*, 2022. 7

GOMES, J. T. C. *Riscos e vulnerabilidades dos equipamentos IoT em unidades de saúde*. Tese (Doutorado) — Escola Superior de Tecnologia e Gestão, 2019. 5

LEMA, M. C. D.; FREITAS, M. Ataques ransomware. *SEMINÁRIO DE TECNOLOGIA GESTÃO E EDUCAÇÃO*, v. 3, n. 1, 2021. 7, 8

LIMA, G. V. d. N. *Uma visão geral sobre segurança em soluções IoT para ambientes residenciais*. Dissertação (B.S. thesis) — Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, 2023. 6, 7

LOPES, F. C.; ROSSATO, D. B.; SILVA, C. V. R. da. Segurança cibernética: Boas práticas para desenvolvimento e operações de aplicações IoT. *Revista Brasileira de Mecatrônica*, v. 5, n. 4, p. 01–20, 2023. 2, 3, 6

NOBREGA, V. S. d. et al. Guia de codificação segura de dispositivos IoT. *Artigo de Diário*, Joinville, SC, 2024. 4

SANTOS, F. F. D. *Tecnologias IoT na Segurança Industrial*. Dissertação (Mestrado) — Universidade NOVA de Lisboa (Portugal), 2020. 5, 6

SILVA, W. d. *Gestão Urbana Integrada para Cidades Inteligentes através da Infraestrutura de Iluminação Pública com a implantação da Internet das Coisas (IoT)*. 2021. 7

SOARES, R.; RABÊLO, R. As implicações e os desafios da defesa cibernética em referência às tecnologias emergentes. *Hoplos Revista de Estudos Estratégicos e Relações Internacionais*, v. 8, n. 14, p. 65–86, 2024. 7, 8

SOUZA, S. B. d. Análise de ataques de ransomware: Identificação e medidas de segurança efetivas. *Artigo de Diário*, Pontifícia Universidade Católica de Goiás, 2024. 8

TENAGLIA, M. R. Simulação de ataques cibernéticos nos dispositivos IoT em ambientes de saúde. 18. *Artigo de Diário*, Pontifícia Universidade Católica de Goiás, 2024. 6

VIVIANI, F. P.; RODRIGUEZ, L. M. G. Categorização de vulnerabilidades de segurança em sistemas de IoT. *Revista dos Trabalhos de Iniciação Científica*, 2022. 4, 5