Yuri Marques da Silva
Orientador: Júlio Vitor Monteiro Marques

Internet das Coisas: Análise de Riscos e Métodos de Prevenção em um Ambiente Doméstico.

Picos - PI
27 de junho de 2025

Yuri Marques da Silva
Orientador: Júlio Vitor Monteiro Marques

Internet das Coisas: Análise de Riscos e Métodos de Prevenção em um Ambiente Doméstico.

Trabalho de conclusão do curso submetido para Universidade Federal do Piauí como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Universidade Federal do Piauí
Campus Senador Heuvídio Nunes de Barros
Bacharelado em Sistemas de Informação

Picos - PI
27 de junho de 2025

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca José Albano de Macêdo

S586i Silva, Yuri Marques da.
Internet das coisas: análise de riscos e métodos de prevenção em um ambiente doméstico / Yuri Marques da Silva – 2025.
36 f.

1 Arquivo em PDF.
Indexado no catálogo *online* da biblioteca José Albano de Macêdo-CSHNB
Aberto a pesquisadores, com restrições da Biblioteca.

Trabalho de Conclusão de Curso (Graduação) – Universidade Federal do Piauí, Curso de Bacharelado em Sistemas de Informação, Picos, 2025.
"Orientador: Júlio Vitor Monteiro Marques".

1. Sistemas informacionais. 2. Segurança na internet. 3. Mitigação de riscos. I. Silva, Yuri Marques da. II. Marques, Júlio Vitor Monteiro. III. Título.

CDD 005.7

Elaborada por Maria Letícia Cristina Alcântara Gomes
Bibliotecária CRB n° 03/1835

INTERNET DAS COISAS: ANÁLISE DE RISCOS E MÉTODOS DE PREVENSÃO EM UM AMBIENTE DOMÉSTICO

YURI MARQUES DA SILVA

Monografia aprovada como exigência parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Data de Aprovação

Picos – PI, 27 de JUNHO de 2025

gov.br Documento assinado digitalmente
JULIO VITOR MONTEIRO MARQUES
Data: 05/07/2025 15:35:23-0300
Verifique em https://validar.iti.gov.br

Prof. Júlio Vitor Monteiro Marques

gov.br Documento assinado digitalmente
FREDISON MUNIZ DE SOUSA
Data: 07/07/2025 13:27:41-0300
Verifique em https://validar.iti.gov.br

Prof. Fredison Muniz de Sousa

gov.br Documento assinado digitalmente
FRANCISCO DAS CHAGAS IMPERES FILHO
Data: 07/07/2025 16:56:56-0300
Verifique em https://validar.iti.gov.br

Prof. Francisco das Chagas Imperes Filho

Agradecimentos

Agradeço, primeiramente, a Deus, pela vida, pela saúde, pelas forças renovadas a cada dia e por me guiar durante toda essa jornada. Sem Sua presença, nada disso seria possível.

Aos meus familiares em especial minha mãe que sempre batalhou com todas as forças para alcançar esse objetivo, minha eterna gratidão, por todo apoio, incentivo e amor incondicional que sempre me motivaram a seguir em frente, mesmo com todas as dificuldades.

À Livya, que esteve ao meu lado em todos os momentos, me dando suporte sempre que precisei. Sua ajuda fez toda a diferença nessa caminhada.

Agradeço imensamente ao meu orientador, professor Júlio, pela paciência, dedicação, disponibilidade e por compartilhar seus conhecimentos, contribuindo de forma fundamental para a realização deste trabalho.

Aos amigos do curso, que tornaram essa trajetória mais leve, repleta de aprendizados e apoio mútuo.

A todos que, de alguma forma, fizeram parte dessa conquista, meu muito obrigado!

Não fui eu que lhe ordenei? Seja forte e corajoso! Não se apavore, nem se desanime, pois o Senhor, o seu Deus, estará com você por onde você andar.

Josué 1:9

Resumo

A crescente presença da Internet das Coisas no ambiente doméstico tem transformado a forma como as pessoas interagem com seus lares, proporcionando comodidade, automação, eficiência energética e controle remoto de uma série de dispositivos inteligentes. Assistentes virtuais, câmeras de vigilância, sensores, eletrodomésticos inteligentes e sistemas de automação residencial estão cada vez mais integrados às rotinas domésticas, oferecendo praticidade e melhorias na qualidade de vida. Contudo, essa evolução também introduz desafios críticos relacionados à segurança e à privacidade dos usuários. Este trabalho apresenta uma revisão sistemática da literatura com o objetivo de identificar os principais riscos de segurança associados à utilização de dispositivos IoT em residências, além de avaliar os impactos desses riscos e propor métodos de mitigação. A análise dos estudos revelou que os riscos mais recorrentes estão relacionados à utilização de senhas padrão, ausência de atualizações de *firmware*, comunicação sem criptografia e falhas na configuração de segurança dos dispositivos. Esses fatores expõem os ambientes domésticos a ataques como controle remoto não autorizado, interceptação de dados, formação de botnets, sequestro de informações e comprometimento da privacidade dos moradores. Observou-se ainda que a falta de conscientização dos usuários é um fator determinante para o agravamento dessas vulnerabilidades. Como estratégias de mitigação, destacam-se a adoção de autenticação forte, criptografia nas comunicações, atualizações periódicas dos sistemas, segmentação de redes domésticas e a educação dos usuários quanto às boas práticas de segurança. Conclui-se que a segurança em ambientes domésticos inteligentes exige uma abordagem integrada, envolvendo tanto medidas técnicas quanto ações de conscientização, a fim de garantir a proteção das informações e a privacidade dos usuários frente às ameaças presentes no ecossistema IoT.

Palavras-chaves: Ambientes Domésticos Inteligentes. Internet das Coisas. IoT Residencial. Mitigação de Riscos. Riscos em IoT. Segurança em IoT.

Abstract

The growing presence of the Internet of Things in domestic environments has transformed the way people interact with their homes, providing convenience, automation, energy efficiency, and remote control of various smart devices. Virtual assistants, surveillance cameras, sensors, smart appliances, and home automation systems are increasingly integrated into household routines, offering practicality and quality of life improvements. However, this evolution also introduces critical challenges related to user security and privacy. This paper presents a systematic literature review aiming to identify the main security risks associated with the use of IoT devices in residential settings, assess the impact of these risks, and propose mitigation methods. The analysis revealed that the most common risks are related to the use of default passwords, lack of firmware updates, unencrypted communications, and poor security configurations of devices. These vulnerabilities expose domestic environments to attacks such as unauthorized remote control, data interception, botnet formation, data hijacking, and privacy breaches. Furthermore, the lack of user awareness is a significant factor in exacerbating these vulnerabilities. As mitigation strategies, the study highlights the adoption of strong authentication, encryption in communications, regular system updates, network segmentation, and user education on security best practices. The study concludes that ensuring security in smart homes requires an integrated approach that combines technical measures with user awareness to protect information and privacy against threats in the IoT ecosystem.

Keywords: Internet of Things. IoT Risks. IoT Security. Residential IoT. Risk Mitigation. Smart Home Environments.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

IoT	Internet of Things (Internet das Coisas)
IA	Inteligência Artificial
CAGR	Compound Annual Growth Rate (Taxa de Crescimento Anual Composta)
TLS	Transport Layer Security
DTLS	Datagram Transport Layer Security
MFA	Multi-Factor Authentication (Autenticação Multifator)
IDS	Intrusion Detection System
DoS	Denial of Service
DDoS	Distributed Denial of Service
MiTM	Man-in-the-Middle (Ataque do Homem no Meio)
TAP	Test Access Point
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
SH-BARM	Modelo de Análise Comportamental para IoT

Sumário

1 Introdução

A Internet das Coisas, que conecta dispositivos físicos a redes digitais, está revolucionando o ambiente doméstico ao permitir interações mais inteligentes e automatizadas. A presença da *IoT* é cada vez mais comum em diversas áreas residenciais, incluindo desde eletrodomésticos até sistemas de segurança avançados. Conforme dados do relatório de Mordor Intelligence (Mordor Intelligence™ Industry Reports, 2024), o mercado global de dispositivos *IoT* alcançou uma cifra estimada em 98,06 bilhões de dólares no ano atual. Prevê-se que este mercado cresça a uma taxa anual composta (CAGR) de 23,25%, projetando-se que atinja 336,64 bilhões de dólares em um período de cinco anos. Essa expansão acentuada é um indicativo da demanda crescente por soluções tecnológicas que facilitam uma vida mais prática e eficiente.

Entretanto, a expansão da Internet das Coisas no ambiente doméstico e corporativo não é desprovida de desafios, particularmente no âmbito da segurança da informação. Segundo (CARVALHO; SANTOS; GONÇALVES, 2022), muitos dispositivos de *IoT*, que incluem desde dispositivos ativados por voz até eletrodomésticos inteligentes, não foram inicialmente projetados com a segurança como elemento central. Essa lacuna no design pode criar vulnerabilidades críticas que são potencialmente exploráveis por agentes maliciosos. No trabalho de (BORTOLI; BALTAZAR, 2023), os autores enfatizam que cada dispositivo *IoT* atua como um potencial ponto de vulnerabilidade dentro de redes residenciais e corporativas, servindo como portais de entrada que podem desencadear ataques cibernéticos em larga escala. A proliferação desses dispositivos amplia exponencialmente a superfície de ataque de uma rede, de modo que a segurança falha de um único dispositivo pode comprometer todo o sistema. Portanto, a segurança em *IoT* se apresenta como uma área crítica que exige atenção imediata e contínua para garantir a proteção efetiva de dados e infraestruturas conectadas.

Outro desafio relevante é a falta de conscientização dos usuários sobre os riscos de segurança em dispositivos *IoT*. (BARBIERI, 2022) destaca que muitos ataques exploram falhas básicas de configuração, como senhas fracas, *firmware* desatualizado e a adoção de dispositivos inseguros, enfatizando a necessidade de orientar os usuários sobre boas práticas de proteção. De forma complementar, (LIMA, 2023) reforça que a segurança em soluções *IoT* depende também do comportamento dos usuários finais, sendo essencial ações como a troca de senhas padrão, atualizações regulares e a segmentação de redes domésticas. Ambos os autores alertam que, sem uma cultura de segurança, as vulnerabilidades são amplificadas e comprometem a proteção da privacidade e dos dados pessoais. A conscientização contínua, aliada a iniciativas educativas dos fabricantes e da comunidade técnica, é vista como um pilar fundamental para o fortalecimento da segurança nos ambientes domésticos conectados.

Diante disso, este trabalho propõe uma revisão da literatura com o objetivo de identificar os principais riscos de segurança associados ao uso de dispositivos IoT em ambientes domésticos, avaliar seus impactos e apresentar métodos eficazes de mitigação, com ênfase na integração entre soluções técnicas e a conscientização dos usuários quanto às boas práticas de segurança, considerando-os como agentes fundamentais na proteção dos sistemas. A postura proativa dos usuários, ao adotar medidas simples representa uma camada de defesa tão importante quanto os mecanismos tecnológicos. Ao preencher essa lacuna, busca-se oferecer um panorama consolidado e crítico que possa orientar tanto pesquisas futuras quanto ações práticas para melhorar a segurança nas residências conectadas.

1.1 Objetivos

Esta seção apresenta os objetivos principais e específicos desta revisão sistemática.

1.1.1 Objetivo Geral

O objetivo deste trabalho é realizar uma revisão sistemática sobre os riscos de segurança associados aos dispositivos de Internet das Coisas em ambientes domésticos, os impactos desses riscos na privacidade e segurança dos usuários e os métodos para mitigar tais riscos, visando melhorar a segurança e a privacidade dos usuários.

1.1.2 Objetivo Específicos

1. Realizar a identificação e análise dos riscos de segurança associados aos dispositivos de Internet das Coisas em ambientes domésticos, por meio de uma revisão sistemática da literatura.

2. Avaliar o impacto potencial de cada risco sobre a privacidade e a segurança dos usuários de dispositivos IoT, com base na análise crítica de estudos existentes.

3. Investigar e apresentar estratégias eficazes para a mitigação desses riscos, a partir da revisão da literatura, com o objetivo de promover a conscientização e a educação dos usuários sobre práticas seguras de utilização.

1.2 Organização do Trabalho

Nesta subseção, apresenta-se a organização deste trabalho. O Capítulo 2, "Referencial Teórico", embasa o entendimento do leitor nos demais tópicos, abordando conceitos fundamentais sobre a IoT, Segurança da Informação e Segurança em IoT. O Capítulo 3, "Trabalhos Relacionados", aborda estudos prévios relevantes para o tema. Em seguida, o Capítulo 4, "Metodologia", descreve os procedimentos adotados para a realização desta

revisão sistemática, incluindo o planejamento, a condução e a extração de dados. O Capítulo 5, "Resultados", apresenta os achados da pesquisa, detalhando os riscos identificados em ambientes domésticos com IoT, os métodos de mitigação propostos e a importância da conscientização dos usuários. O Capítulo 6, "Desafios de Pesquisa e Direções", discute as limitações do estudo e sugere caminhos para futuras investigações. Finalmente, o Capítulo 7, "Conclusão", sintetiza os principais resultados, as contribuições do trabalho e as recomendações finais.

2 Referencial Teórico

Esta seção apresenta conceitos fundamentais para a melhor compreensão do estudo, abordando a Internet das Coisas, a segurança da informação e a segurança em *IoT*.

2.1 Internet das Coisas

A Internet das Coisas representa um avanço tecnológico, baseada em Internet e objetos inteligentes (GALEGALE et al., 2016). A Internet das Coisas é um conceito que se refere à presença generalizada de diversos objetos e dispositivos em nosso ambiente, que se conectam, seja por meio de redes com fio ou sem fio, esses objetos possuem endereços únicos e são capazes de se comunicar entre si, colaborando para desenvolver novas aplicações e serviços, além de alcançar objetivos comuns (GAITAN; GAITAN; UNGUREAN, 2014). A *IoT* permite a coleta e troca de dados entre dispositivos que adotam a tecnologia, mostrando potencial de melhorar a eficiência, conveniência nas diversas áreas que atua contribuindo para tomada de decisões baseadas em informações precisas e atualizadas.

A Internet das Coisas conecta dispositivos que são usados no dia a dia para facilitar a comunicação e integrar-se a internet, como eletrodomésticos, aplicativos e carros (CNN Brasil, 2023). Mais de 27 bilhões de dispositivos já estão conectados e se conversam no mundo (PACETE, Luiz Gustavo , 2022). Estima-se que em 2025, o impacto econômico da *IoT* pode alcançar entre 4 a 11 trilhões de dólares por ano (MANYIKA et al., 2023). Esse crescimento é impulsionado pela crescente adoção de tecnologias *IoT* em diversos setores, que permite não apenas a otimização de processos e redução de custos, mas também a criação de novos modelos de negócios e oportunidades de receita. Os sistemas *IoT* caracterizam-se pela sua universalidade, aplicando-se a diversos setores da sociedade e da indústria, incluindo a automação residencial, cidades inteligentes, saúde, agricultura, entre outros (PINHEIRO, 2023).

Dentre as diversas áreas a *IoT* está transformando a área da saúde com o uso de dispositivos vestíveis que monitoram continuamente os sinais vitais dos pacientes, permitindo intervenções rápidas em caso de anomalias e melhorando a gestão de condições crônicas. Um exemplo é o monitoramento remoto de pacientes diabéticos, onde dispositivos *IoT* específicos podem medir os níveis de glicose no sangue e enviar alertas em tempo real para os profissionais de saúde (KITSIOU et al., 2017). Já na agricultura a Internet das Coisas, permite o compartilhamento de grandes volumes de dados dos mais variados tipos com grande fluidez, alimentando diversas etapas do processo produtivo, tais como detecção e monitoramento de atividades agropecuárias, processamento industrial de alimentos e análise preditiva das variáveis meteorológicas (BERTOLLO; CASTILLO; BUSCA,).

No cenário doméstico, a Internet das Coisas está assumindo um papel predominante com dispositivos interconectados e possibilitando a conexão de objeto para objeto (GONÇALVES, 2019). A automação residencial como ilustra a Figura 1 no qual representa a multiconectividade de dispositivos que podem existir em uma casa inteligente, é um dos aspectos mais visíveis e populares da *IoT*. Dispositivos como termostatos inteligentes, iluminação automatizada e fechaduras eletrônicas podem ser controlados remotamente por meio de aplicativos. Isso não apenas proporciona conforto, permitindo ajustes à distância, mas também contribui para a eficiência energética ao otimizar o uso de eletricidade (PEREIRA, Rafael, 2023). A internet das coisas utilizada no ambiente doméstico vem revolucionando a forma como vivemos em nossos lares, tornando-os mais inteligentes e eficientes.

Figura 1 – Casa inteligente. Fonte: (macrovector, 2018)

2.2 Segurança da Informação

Na sociedade informatizada, o papel da segurança da informação é fundamental (SILVA; STEIN, 2007). Como ilustra a Figura 2 a segurança da informação é um conjunto de práticas essenciais que visam seguir seus pilares que são a integridade, disponibilidade e confidencialidade dos dados, sejam eles físicos ou virtuais. Os problemas de segurança da informação são em geral provocados por pessoas mal-intencionadas que buscam algum tipo de vantagem, seja ela monetária, política ou intelectual (MACHADO, 2014).

A falta de conscientização dos usuários, referente aos perigos das suas ações e das ameaças no contexto da tecnologia da informação, levam a uma maior ocorrência de incidentes de segurança (MARINHO; BODÊ, 2022). A maioria das violações de segurança é atribuída a erros humanos, frequentemente decorrentes da falta de conhecimento sobre práticas seguras e das ameaças emergentes. A ausência de treinamento adequado e

Figura 2 – Pilares da segurança da informação. Fonte: (Protiviti, 2023)

a compreensão limitada dos perigos associados às ações cotidianas podem resultar em consequências severas, como vazamentos de dados e ataques cibernéticos bem-sucedidos (BADA; SASSE; NURSE, 2019).

Com o estilo de vida contemporâneo, em que, praticamente, todas as nossas atividades, sejam elas digitais ou físicas, são gravadas constantemente, é fundamental estabelecer o mínimo de segurança e privacidade das nossas informações (KADOW; CAMARGO, 2016). A informação é um ativo muito desejado e valioso tanto para uma pessoa como para uma organização, devendo obrigatoriamente estar protegido de acessos não autorizados (FERNANDES, 2018). Portanto torna-se de extrema importância a segurança da informação para o mundo digital em que vivemos.

A segurança da informação não é apenas uma questão técnica, mas também uma responsabilidade compartilhada que exige conscientização e vigilância contínuas para mitigar riscos e proteger informações valiosas em um ambiente digital cada vez mais complexo. A evolução constante das ameaças e técnicas de ataque reforça a necessidade de medidas de segurança robustas e atualizadas para proteger dados sensíveis e garantir a integridade dos sistemas (ANDERSON, 2020).

2.3 Segurança em IoT

Sabendo que alguns dispositivos são projetados sem prioridade na segurança (CARVALHO; SANTOS; GONÇALVES, 2022), é essencial que os fabricantes de dispositivos IoT incorporem práticas de segurança e que os usuários finais estejam cientes dessas medidas. A falta de segurança embutida nos dispositivos pode levar a sérias vulnerabilidades que são exploradas por cibercriminosos. Como os dispositivos estão conectados, eles também enfrentam a ameaça de ataques cibernéticos (CARVALHO; SANTOS; GONÇALVES, 2022). A interconexão entre os dispositivos amplia a superfície de ataque, tornando crucial a adoção de medidas de segurança abrangentes e integradas. Uma rede de comunicação que utiliza técnicas de proteção se torna um alvo mais complexo, as potenciais

vulnerabilidades são menos numerosas e, caso existam, tornam-se mais desafiadoras de serem exploradas (BERLANDA, 2021). Implementar uma infraestrutura de comunicação segura não apenas dificulta as ações dos atacantes, mas também fortalece a resiliência do sistema como um todo.

A possibilidade de roubo ou outro acesso não autorizado aos dados ou sistemas desenvolvidos em torno da *IoT* significa que a segurança cibernética precisa ser vista como prioridade para a implementação de sistemas confiáveis (SANTOS; SALES, 2015). Este cenário impõe uma responsabilidade significativa tanto para fabricantes quanto para usuários, que devem estar constantemente vigilantes e informados sobre as melhores práticas de segurança. Como na *IoT* todos os dispositivos estão interconectados, um dispositivo que esteja mal protegido e conectado na internet poderá consequentemente afetar toda a segurança (FIGUEIRA, 2016). A falta de proteção adequada em um único dispositivo pode comprometer a segurança de toda a rede, demonstrando a importância de uma abordagem holística para a segurança da *IoT*. A consequência disso é a vulnerabilidade dos usuários dos dispositivos *IoT* na rede, podendo deixar suas informações expostas e abrir portas para invasões e ataques mais sofisticados.

Dentro de diversas possibilidades de aplicação da *IoT* encontra-se o cenário das casas inteligentes (GONÇALVES, 2019). A domótica, ou automação residencial, está se tornando cada vez mais comum, trazendo conveniência e facilidade no dia a dia dos usuários. No entanto, a *IoT* residencial apresenta vários riscos de segurança devido a redes locais vulneráveis, dispositivos *IoT* fracos e comunicação de dados não criptografada entre sensores (SUPARNA; MANJAIAH, 2022). Esses fatores tornam as residências inteligentes alvos atrativos para cibercriminosos. Os dispositivos podem expor os consumidores a um ecossistema de dispositivos e sensores que coletam dados indiscriminadamente (HUREL; LOBATO, 2018). A coleta massiva de dados sem o devido controle e segurança pode resultar em sérias violações de privacidade. Casas com recursos de *IoT* e dispositivos inteligentes podem ser facilmente invadidas a partir dos dados que são coletados, colocando em risco a segurança dos moradores e a integridade de suas informações pessoais (PEREIRA; SENO, 2022).

Os usuários frequentemente subestimam o valor apropriado atribuído a medidas de segurança necessárias para que seus dispositivos conectados à internet estejam minimamente protegidos dentro de suas redes (PEREIRA; SENO, 2022). Essa subestimação pode resultar em configurações de segurança inadequadas e na utilização de dispositivos sem as devidas atualizações de segurança. Dessa forma, a negligência dos usuários em relação à segurança de seus dispositivos residenciais não apenas compromete sua própria proteção, mas também contribui para a ampliação do déficit de padronização de segurança nos dispositivos *IoT*. É crucial que os usuários sejam educados sobre a importância de atualizar regularmente seus dispositivos e implementar medidas de segurança eficazes para proteger suas redes e informações pessoais.

3 Trabalhos Relacionados

Esta seção apresenta trabalhos relacionados. A Tabela 1 apresenta os trabalhos de acordo com três critérios específicos: critério I - avalia se o trabalho aborda os riscos associados à Internet das Coisas; critério II - verifica se o trabalho propõe ou discute estratégias para mitigar os riscos identificados na Internet das Coisas; critério - III verifica a capacidade do trabalho de conscientizar o leitor sobre os riscos da Internet das Coisas; critério - IV avalia se o trabalho enfatiza a conscientização do usuário como uma medida de segurança primária e complementar aos mecanismos técnicos na mitigação dos riscos relacionados a *IoT* no ambiente doméstico.

A tabela também expõe os tipos dos trabalhos, classificando-os como revisão da literatura ou revisão sistemática, diferenciando-os principalmente pelo rigor metodológico. Enquanto a revisão da literatura apresenta uma análise mais ampla e sem metodologia rígida, a revisão sistemática segue um processo estruturado e criterioso para selecionar e analisar estudos.

Tabela 1 – Comparação dos trabalhos relacionados.

Trabalho	**Tipo do Trabalho**	**Critério I**	**Critério II**	**Critério III**	**Critério IV**
(BASTOS; SHACKLETON; EL-MOUSSA, 2018)	Revisão da literatura	Sim	Sim	Sim	Não
(KUYUCU; BAHTIYAR; İNCE, 2019)	Revisão da literatura	Sim	Sim	Sim	Não
(ITEN; WAGNER; RöSCHMANN, 2021)	Revisão sistemática	Sim	Sim	Sim	Não
(BARBIERI, 2022)	Revisão da literatura	Sim	Sim	Sim	Sim
(LIMA, 2023)	Revisão da literatura	Sim	Sim	Sim	Sim
(DHANRAJ et al., 2024)	Revisão da literatura	Sim	Sim	Sim	Não
(ALZAYLAEE, 2025)	Revisão sistemática	Sim	Sim	Sim	Não

Os diversos estudos abordam os riscos de segurança e privacidade em ambientes *IoT*, especialmente em *smart homes*. (KUYUCU; BAHTIYAR; İNCE, 2019) realizaram uma revisão dos principais problemas de segurança, propondo práticas de proteção na comunicação entre dispositivos. (ALZAYLAEE, 2025) apresentou uma revisão sistemática sobre vulnerabilidades em *smart homes* e avaliou técnicas como *IA* e *blockchain* para mitigação. (ITEN; WAGNER; RöSCHMANN, 2021) exploraram métodos de identificação e tratamento de riscos, enquanto (BASTOS; SHACKLETON; EL-MOUSSA, 2018) mapearam tecnologias e riscos de segurança em ambientes residenciais e urbanos conectados.

No que diz respeito à proteção da privacidade, (DHANRAJ et al., 2024) propuseram abordagens em múltiplas camadas para minimizar exposições em smart homes.(BARBIERI, 2022) analisou vulnerabilidades em dispositivos *IoT* residenciais, destacando falhas comuns como autenticação fraca e protocolos inseguros, além de sugerir práticas preventivas para usuários finais. (LIMA, 2023) explorou soluções de segurança para ambientes residenciais conectados, reforçando a necessidade de conscientização e boas práticas de uso.

A presente revisão sistemática além de identificar os principais riscos de segurança

associados à *IoT* no ambiente doméstico, bem como métodos de mitigação propostos na literatura dá ênfase à conscientização dos usuários como um pilar tão importante quanto os mecanismos técnicos, evidenciando que a integração entre soluções tecnológicas e ações educativas é essencial para aumentar a resiliência das redes domésticas frente às ameaças cibernéticas. Reforçando a necessidade de estratégias integradas de segurança, conscientização dos usuários e adoção de tecnologias emergentes no fortalecimento da proteção em ambientes inteligentes.

4 Metodologia

Esta seção detalha a metodologia empregada para a realização desta Revisão Sistemática da Literatura. O objetivo principal foi coletar e analisar informações disponíveis na literatura para compreender os riscos existentes relacionados à Internet das Coisas em ambientes domésticos, os métodos de prevenção e mitigação aplicáveis a esses problemas, e o nível de compreensão e conscientização dos usuários sobre a segurança nesse contexto. Seguindo os passos propostos por (KITCHENHAM, 2004), o processo de revisão foi dividido em três etapas principais: planejamento, condução e extração de dados. A Figura 3 ilustra as etapas e seus detalhes.

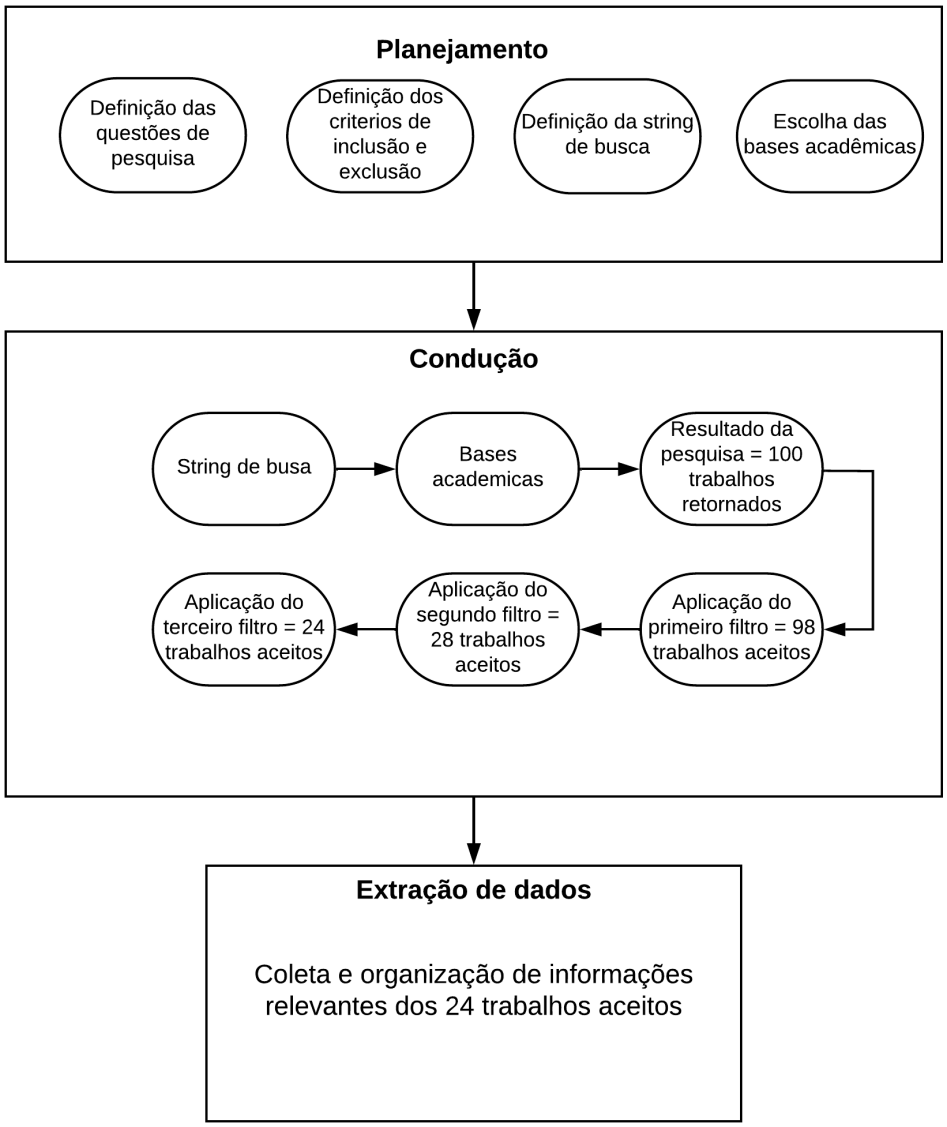

Figura 3 – Fluxograma da metodologia.

4.1 Planejamento

No planejamento foram definidas as questões de pesquisa voltadas para a extração de informações incluindo as seguintes questões: “Quais são os principais riscos de segurança para dispositivos *IoT* em ambientes domésticos?”, “Quais técnicas de mitigação têm sido propostas?”, “Como a conscientização dos usuários pode influenciar a segurança na *IoT* doméstica?” e “Quais as práticas eficazes na redução de vulnerabilidades em ambientes domésticos que utilizam a *IoT*?”. Houve também a definição dos critérios de inclusão (I) e exclusão (E): (I) Estudos publicados a partir de 2016; (I) Estudos que abordem a segurança da *IoT* em ambientes domésticos;(I) Estudos que identifiquem os principais riscos e metodologias de mitigação; (E) Estudos publicados antes de 2016; (E) Estudos que tratem de *IoT* em contextos distintos do doméstico; (E) Estudos que não discutam soluções de mitigação ou que tratem apenas de aspectos técnicos de funcionalidade sem abordagem de segurança.

Nesta etapa de planejamento foi definida também a string de busca "*IoT security"OR "home IoT risks"OR "IoT risk mitigation*"construída com base na estratégia de abrangência sem perda de foco, visando capturar estudos que abordem tanto aspectos gerais de segurança em IoT, quanto riscos específicos no ambiente doméstico e as estratégias de mitigação adotadas. Por fim a escolha das bases onde o *Google Scholar* foi selecionado por sua abrangência multidisciplinar, pois agrega resultados de diversas bases de dados e repositórios institucionais, já a base *IEEE Xplore* foi escolhida por ser uma fonte altamente especializada em engenharia, computação e tecnologia da informação, oferecendo artigos de conferências, periódicos e padrões com rigor técnico elevado, o que é essencial para garantir a qualidade e relevância científica dos estudos incluídos.

4.2 Condução

Na etapa de condução foi aplicada a string de busca "*IoT security"OR "home IoT risks"OR "IoT risk mitigation*"nas bases acadêmicas *Google Scholar* e *IEEE Xplore* retornando inicialmente 100 artigos relacionados ao tema, na figura 4 há a presença de algumas outras bases que se deu pelo fato de que a base *Google Scholar* retorna trabalhos de diversas outras bases, os trabalhos passaram por três etapas distintas de filtragem resultando em uma seleção final de 24 artigos aceitos. A Figura 4 ilustra as bases de dados consultadas, a quantidade de trabalhos aceitos em cada fase de filtragem e o detalhamento da aplicação de cada critério de seleção.

	PESQUISA INICIAL	1º FILTRO	2º FILTRO	3º FILTRO	EXTRAÇÃO DE DADOS
BASES	100 ARTIGOS RETORNADOS	2 ARTIGOS REMOVIDOS	28 ARTIGOS ACEITOS	24 ARTIGOS ACEITOS	**TAXA DE ACEITAÇÃO**
IEEE Xplore	71	2	22	19	79.17%
MDPI	3	0	1	1	4.16%
ScienceDirect	4	0	0	0	0.0%
Outros	22	0	5	4	16.66%
CRITÉRIOS	Ano >= 2016 Linguagem em Inglês	1º Filtro Documentos duplicados	2º Filtro Critérios de inclusão e exclusão aplicados no titulo e no resumo	3º Filtro Critérios de inclusão e exclusão aplicados no texto completo	

Figura 4 – Tabela de filtros.

4.3 Extração de dados

Na fase de extração de dados, foram coletadas e organizadas informações relevantes dos estudos selecionados, considerando os seguintes aspectos: identificação dos principais riscos associados ao uso da IoT em ambientes domésticos, descrição das técnicas e métodos de mitigação propostos e análise do nível de conscientização dos usuários quanto às ameaças.

Posteriormente, as informações extraídas foram sistematizadas para apoiar a construção do capítulo seguinte. A análise realizada teve como objetivo identificar padrões recorrentes, evidenciar lacunas existentes na literatura e apontar tendências emergentes relacionadas à segurança da IoT em ambientes domésticos.

5 Resultados

Os riscos associados ao uso doméstico de dispositivos *IoT* são diversos e relevantes, mas podem ser amplamente mitigados por meio da combinação entre soluções tecnológicas eficazes e usuários capacitados e conscientes. Nos estudos analisados, identificou-se uma variedade de vulnerabilidades que evidenciam a fragilidade da infraestrutura digital nas residências modernas. Para enfrentar esse cenário, foram propostas diversas estratégias de defesa, dentre as quais a conscientização dos usuários se destaca como um elemento fundamental. Quando devidamente informados, os usuários tendem a adotar medidas de proteção, tornando-se agentes ativos na segurança de seus lares conectados. Essa integração entre tecnologia e conhecimento é essencial para promover um ambiente doméstico digital mais seguro.

5.1 Riscos

Os estudos analisados apontam uma variedade de riscos críticos à segurança de dispositivos *IoT* em ambientes domésticos. Entre esses riscos, diversos autores identificaram a autenticação fraca, a falta de atualizações de *software* e a comunicação insegura, deixando a ideia de serem os riscos mais recorrentes nos dispositivos *IoT* utilizados em ambientes domésticos.

A autenticação fraca é exposta nos trabalhos dos autores (JAMES, 2019a), (ALRAWI et al., 2019), (GAMUNDANI; PHILLIPS; MUYINGI, 2018), (JAMES, 2019b) e (RAJKHAN; SONG, 2021), onde mostram que esse risco é causado principalmente pelo uso de senhas padrão não alteradas pelos usuários, pela ausência de autenticação multifatorial e pela limitação dos mecanismos de segurança nativos dos dispositivos. Como consequência, ocorre o acesso não autorizado por atacantes, permitindo o controle indevido de funções domésticas e resultando em violação da privacidade dos moradores.

A falta de atualizações de *software* também é amplamente discutida pelos autores (JAMES, 2019a), (DAR et al., 2024), (RYOO; TJOA; RYOO, 2018) e (AIKEN; RYOO; RIZVI, 2020), mostrando em seus estudos que esse risco é atribuído à negligência de fabricantes, que deixam de fornecer suporte contínuo aos dispositivos, à ausência de sistemas automáticos de atualização, além da baixa conscientização dos usuários sobre a importância dessas correções. Isso expõe os dispositivos a vulnerabilidades já conhecidas, que podem ser exploradas em ataques direcionados, como a formação de *botnets* (redes de computadores infectados e controlados remotamente para fins maliciosos) e infecção por *ransomware* (vírus que bloqueia o acesso aos dados e exige pagamento para liberá-los).

Já a comunicação insegura aparece nos trabalhos de (JAMES, 2019a), (ALI et al., 2017), (JAMES, 2019b), (SIVAPRIYAN et al., 2021) e (KABIR; GOPE; MOHANTY,

2023), sendo associada à utilização de protocolos de comunicação desprotegidos, à transmissão de dados sem criptografia e à falta de autenticação nas interações entre dispositivos. As consequências diretas incluem a interceptação de informações sensíveis (*eavesdropping*), a modificação maliciosa de comandos transmitidos e a violação da confidencialidade e integridade da rede doméstica.

Um ataque marcante envolvendo dois desses três riscos mais relatados foi o ataque da *botnet* Mirai, em 2016, que sequestrou milhares de dispositivos *IoT* como câmeras IP e roteadores com configuração padrão e desatualizados para lançar ataques *DDoS* (Uso indevido de diversos dispositivos na internet usados para atacar simultaneamente um sistema ou sites.) massivos, como o que derrubou os servidores da empresa Dyn que oferecia serviços de domínio, afetando plataformas como *Twitter* e *Netflix*.

A seguir, a Tabela 2 abrange os principais riscos identificados nos estudos, suas causas, consequências e os respectivos autores, com o objetivo de sintetizar de forma clara as vulnerabilidades mais recorrentes em ambientes domésticos com IoT.

Tabela 2 – Riscos de segurança em ambientes domésticos com IoT, suas causas e consequências, conforme os trabalhos analisados.

Trabalho	**Risco Identificado**	**Causas**	**Consequências**
(BUGEJA; JACOBSSON; DAVIDSSON, 2016)	Exposição de dados e controle remoto	Dispositivos expostos; protocolos inseguros	Interceptação; sabotagem; manipulação de ambiente
(ALI et al., 2017)	Interceptação e modificação de mensagens	Protocolos inseguros; ausência de autenticação	Comprometimento da integridade; ataques DoS
(GAMUNDANI; PHILLIPS; MUYINGI, 2018)	Spoofing, força bruta, eavesdropping	Credenciais fracas; falta de criptografia	Acesso não autorizado; DoS; perda de dados
(RYOO; TJOA; RYOO, 2018)	Ransomware e violação de privacidade	Falhas em software/hardware; rede mal protegida	Bloqueio de sistemas; vazamento de dados
(VARGHESE; HAYAJNEH, 2018)	Ataques a voz e câmeras; má configuração	Falta de autenticação; ausência de atualizações	Acesso remoto; rastreamento indesejado
(SHOURAN; ASHARI; PRIYAMBODO, 2019)	Controle não autorizado e uso malicioso	Dispositivos inseguros; interconexão excessiva	Invasão de privacidade; ataques com botnets
(JAMES, 2019a)	Autenticação fraca e comunicação insegura	Protocolos frágeis; ausência de atualizações	Acesso indevido; interceptação de dados
(ALRAWI et al., 2019)	Configurações inseguras; heterogeneidade	Credenciais padrão; múltiplas plataformas	Controle indevido; falhas de interoperabilidade
(JAMES, 2019b)	Falha de autenticação e comunicação	Implementação insegura; ausência de atualizações	Acesso remoto malicioso; interceptação de dados
(AGAZZI, 2020)	Senhas fracas e comunicação aberta	Falta de criptografia; dispositivos mal projetados	Interceptação de dados; ataques DDoS
(AIKEN; RYOO; RIZVI, 2020)	Falta de atualizações e botnets	Uso de senhas padrão; ignorância do usuário	Invasões em massa; uso em ataques externos
(DIK et al., 2020)	Falta de isolamento; autenticação fraca	Redes únicas; senhas fracas	Ataques laterais; perda de controle da rede
(PARSONS; PANAOUSIS; LOUKAS, 2021)	Falta de padronização e malware	Tecnologias diversas; rede doméstica desprotegida	Ataques em rede remota; vazamento de dados
(SIVAPRIYAN et al., 2021)	Eavesdropping, hijacking e DoS	Ausência de criptografia; autenticação fraca	Perda de controle; interrupções de serviço
(TRABELSI, 2021)	Acesso a câmeras; DoS; MiTM	Firmware desatualizado; arquitetura exposta	Controle externo; interrupções; violação da rede
(RAJKHAN; SONG, 2021)	Credenciais padrão e falta de transparência	Usuários não alteram padrões; fabricantes negligentes	Acesso indevido; exposição de dados pessoais
(SHARBAF, 2022)	Falta de conscientização e padronização	Usuário despreparado; políticas inexistentes	Ampliação da superfície de ataque; acessos não autorizados
(WANG et al., 2022)	TAP mal configurado e DDoS	Regras erradas; plataformas não autenticadas	Vazamento de dados; comportamento inesperado
(SINGH; SINGH; NEGI, 2023)	Coleta indevida e malware	Falta de autenticação forte; uso de senhas fracas	Vazamento de dados; invasão da privacidade
(KABIR; GOPE; MOHANTY, 2023)	Falhas de comunicação e integração insegura	Sistemas de diferentes fornecedores; políticas conflitantes	Estados críticos; consequências perigosas
(MILENKOVIć et al., 2023)	Perda de privacidade e controle	Interface simplificada; falhas de design	Invasão; uso indevido; bloqueio de serviços
(VARDAKIS et al., 2024)	Acesso não autorizado e danos físicos	Senhas fracas; vulnerabilidades na rede	Controle total do dispositivo; falha de segurança
(DELICADO et al., 2024)	Invasão da privacidade e hacking	Firmware vulnerável; falta de proteção física	Roubo de dados; controle externo não autorizado
(DAR et al., 2024)	Firmware desatualizado; ataques físicos	Falta de manutenção; acesso físico fácil	Invasão de dispositivos; roubo de identidade

A análise dos estudos revelou que os principais riscos de segurança em ambientes domésticos com IoT estão relacionados, principalmente, à autenticação fraca, ausência de atualizações de firmware (sistema operacional básico responsável por fazer o dispositivo funcionar corretamente) e comunicação insegura. Esses riscos são causados, sobretudo, pelo uso de senhas padrão, falta de criptografia, negligência dos fabricantes e desconhecimento dos usuários. Como consequência, os dispositivos ficam vulneráveis a acessos não autorizados, interceptação de dados, controle remoto indevido, formação de botnets, ataques DoS e comprometimento da privacidade dos moradores. Esses fatores ampliam significativamente a superfície de ataque nas residências conectadas, tornando a segurança um desafio constante.

5.2 Métodos de Mitigação

Entre os métodos de mitigação propostos nos estudos analisados, três se destacam por sua recorrência e eficácia na proteção de dispositivos IoT em ambientes domésticos: autenticação forte, criptografia nas comunicações e atualizações regulares de *firmware* e *software* (parte lógica do dispositivo). Esses métodos são apontados por diversos autores como fundamentais para mitigar os principais riscos relacionados à segurança, como acesso não autorizado, interceptação de dados e exploração de vulnerabilidades conhecidas.

A autenticação forte, abordada por autores como (JAMES, 2019a), (ALRAWI et al., 2019), (GAMUNDANI; PHILLIPS; MUYINGI, 2018), (JAMES, 2019b) e (RAJKHAN; SONG, 2021), tem como objetivo dificultar o acesso de agentes mal-intencionados aos dispositivos. Esse método combate diretamente o risco de autenticação fraca, uma das falhas mais comuns, muitas vezes causada pelo uso de senhas padrão ou credenciais simples. As soluções propostas incluem autenticação multifatorial, autenticação baseada em certificados e reforço na configuração inicial do dispositivo, garantindo que apenas usuários autorizados possam operá-los.

Já a criptografia nas comunicações, presente nos trabalhos de (ALI et al., 2017), (SIVAPRIYAN et al., 2021), (JAMES, 2019b), (RYOO; TJOA; RYOO, 2018) e (KABIR; GOPE; MOHANTY, 2023), visa proteger a integridade e a confidencialidade dos dados transmitidos entre dispositivos e serviços conectados. Esse método atua diretamente contra os riscos de comunicação insegura, *eavesdropping* e ataques *man-in-the-middle* (ataque em que o criminoso se coloca secretamente entre duas partes que estão se comunicando espionando e intercptando informações), permitindo que informações sensíveis, como comandos ou dados pessoais, não sejam interceptadas ou modificadas por terceiros. Os protocolos sugeridos incluem TLS, DTLS e criptografia ponta a ponta que são protocolos de segurança usados para proteger a troca de informações entre dois dispositivos pela internet ou por uma rede local.

A terceira medida amplamente recomendada é a realização de atualizações regulares

dos dispositivos, conforme defendido por (JAMES, 2019a), (DAR et al., 2024), (RYOO; TJOA; RYOO, 2018) e (AIKEN; RYOO; RIZVI, 2020). A ausência de atualizações é uma porta aberta para exploração de vulnerabilidades conhecidas e infecções por *malware*, como *botnets* e *ransomwares*. As atualizações automáticas ou assistidas permitem que os dispositivos recebam correções de segurança assim que forem disponibilizadas pelos fabricantes, aumentando a resiliência contra ataques emergentes.

Um amostra real de um desses métodos de mitigação em prática se deu quando em 2019, usuários da empresa *Ring* relataram invasões a câmeras domésticas causadas pelo uso de senhas fracas ou reutilizadas, exploradas por meio de *credential stuffing* que é uma técnica em que hackers usam senhas vazadas de outros serviços para tentar acessar novas contas. Em resposta, a empresa tornou obrigatória, em 2020, a autenticação em duas etapas, exigindo um código adicional via *SMS* ou *e-mail*. Após essa medida, os acessos não autorizados com o mesmo padrão cessaram, demonstrando a eficácia da autenticação em duas etapas na proteção dos dispositivos e reforçando a confiança dos usuários na marca.

A Tabela 3 apresenta um panorama detalhado dos métodos de mitigação descritos nos estudos, destacando suas aplicações e os efeitos esperados.

Tabela 3 – Métodos de mitigação aplicados à segurança de dispositivos IoT em ambientes domésticos, conforme os trabalhos analisados.

Trabalho	**Método de Mitigação**	**Descrição ou Aplicação**	**Objetivo ou Efeito Esperado**
(BUGEJA; JACOBSSON; DAVIDSSON, 2016)	Criptografia local e controle de dispositivos expostos	Restrições a interfaces remotas e expostas	Minimizar riscos de manipulação remota
(ALI et al., 2017)	Protocolos criptografados (TLS/DTLS)	Estabelecimento de canais seguros	Reduzir ataques man-in-the-middle
(GAMUNDANI; PHILLIPS; MUYINGI, 2018)	Certificados digitais e autenticação baseada em criptografia	Validação de identidade com pares confiáveis	Garantir autenticidade e mitigar spoofing
(RYOO; TJOA; RYOO, 2018)	Firewalls, criptografia e backups automáticos	Defesa de perímetro e integridade de dados	Evitar ransomware e perda de informações
(VARGHESE; HAYAJNEH, 2018)	Atualizações e autenticação via tokens seguros	Renovação contínua do sistema e autenticação moderna	Proteger contra controle remoto e rastreamento
(JAMES, 2019a)	Autenticação forte e atualizações automáticas	Substituição de senhas padrão; atualização periódica do firmware	Prevenir acesso não autorizado e corrigir falhas conhecidas
(ALRAWI et al., 2019)	Autenticação multifator (MFA)	Requer mais de uma forma de verificação de identidade	Reduzir risco de invasões por senhas fracas
(JAMES, 2019b)	Criptografia TLS e gestão de credenciais	Proteção de dados durante a transmissão	Impedir eavesdropping e interceptações
(SHOURAN; ASHARI; PRIYAMBODO, 2019)	Segmentação de rede	Isolamento de dispositivos em redes diferentes	Conter movimentação lateral de ameaças
(AIKEN; RYOO; RIZVI, 2020)	Atualizações automáticas e autenticação reforçada	Gerenciamento de segurança e notificações	Eliminar brechas conhecidas e proteger acesso
(AGAZZI, 2020)	Educação do usuário e guias de boas práticas	Materiais explicativos para configuração segura	Reduzir riscos por má configuração
(SIVAPRIYAN et al., 2021)	IDS e criptografia ponta a ponta	Monitoramento do tráfego e proteção de dados	Detectar ataques e garantir confidencialidade
(RAJKHAN; SONG, 2021)	Gestão de credenciais e limitação de acesso padrão	Troca de senhas padrão e permissões granulares	Minimizar riscos por credenciais expostas
(SHARBAF, 2022)	Adoção de padrões interoperáveis (ZigBee, Z-Wave)	Uso de tecnologias amplamente testadas	Evitar vulnerabilidades por protocolos proprietários
(WANG et al., 2022)	Isolamento de plataformas e verificação de regras TAP	Regras explícitas para automações seguras	Evitar ações imprevistas e falhas operacionais
(KABIR; GOPE; MOHANTY, 2023)	Autenticação mútua e criptografia bidirecional	Verificação dupla de entidades e integridade dos dados	Evitar falsificações e interferência em comunicações
(MILENKOVIć et al., 2023)	Modelagem de risco e análise de ameaças	Aplicação de frameworks como STRIDE	Antecipar vulnerabilidades e planejar respostas
(DAR et al., 2024)	Atualizações regulares e controle físico de acesso	Atualização de firmware e proteção física dos dispositivos	Evitar exploração local e acesso físico indevido
(DELICADO et al., 2024)	Auditoria periódica e análise de vulnerabilidades	Verificações regulares da integridade e segurança dos dispositivos	Corrigir falhas antes da exploração

Entre os métodos de mitigação mais eficazes, destacam-se a autenticação forte, a criptografia nas comunicações e as atualizações periódicas dos dispositivos. Essas práticas visam prevenir acessos não autorizados, evitar interceptação de dados, impedir a propagação de malware e a exploração de vulnerabilidades conhecidas. Consequentemente, reduzem riscos como sequestro de dados, controle externo dos dispositivos, formação de botnets e vazamento de informações sensíveis. Adicionalmente, medidas como segmentação de redes e auditorias periódicas fortalecem a proteção, tornando os ambientes domésticos mais resilientes frente às ameaças presentes no ecossistema IoT.

5.3 Conscientização dos Usuários

Os estudos analisados destacam a conscientização dos usuários como um elemento crucial para a segurança em ambientes domésticos com IoT. Os autores (JAMES, 2019a), (ALRAWI et al., 2019), (DAR et al., 2024), (SHARBAF, 2022), (RYOO; TJOA; RYOO, 2018), (AGAZZI, 2020) apontam que a falta de conhecimento técnico dos usuários finais é uma das principais causas de exposição a riscos. A negligência em aspectos básicos de segurança, como a troca de senhas padrão, a atualização de *firmware* e a configuração adequada de dispositivos, contribui diretamente para o aumento das vulnerabilidades.

Os trabalhos dos autores (GAMUNDANI; PHILLIPS; MUYINGI, 2018), (WANG et al., 2022), (TRABELSI, 2021) mostram que a problemática central está no fato de que muitos dispositivos são utilizados com as configurações padrão de fábrica e operados por usuários que não compreendem os riscos associados a práticas inseguras. Essa lacuna favorece o surgimento de ameaças como acesso não autorizado, coleta indevida de dados, formação de *botnets* e interceptação de informações. A ausência de conscientização transforma o elo mais fraco do sistema em uma vulnerabilidade crítica.

Por outro lado, os trabalhos de (MILENKOVIć et al., 2023) e (ALI et al., 2017) ressaltam que usuários bem informados desempenham um papel essencial na mitigação de riscos. A adoção de práticas como o uso de senhas fortes e exclusivas, a realização frequente de atualizações, a atenção a comportamentos anômalos nos dispositivos e a configuração correta da rede doméstica pode prevenir ataques e reduzir a superfície de ataque.

Além disso, (SHARBAF, 2022), (RYOO; TJOA; RYOO, 2018) e (AGAZZI, 2020) expõem em seus trabalhos que campanhas educativas, guias práticos para configuração segura e modelos de análise comportamental (como o SH-BARM) são estratégias eficazes para promover mudanças positivas no comportamento dos usuários. Portanto, os estudos mostram que a conscientização dos usuários é um componente tão importante quanto os mecanismos técnicos de defesa, sendo considerada por diversos autores como a primeira camada de proteção em sistemas IoT domésticos.

Os estudos analisados deixam evidente que a conscientização dos usuários é um dos pilares fundamentais para a segurança em ambientes domésticos inteligentes. A falta de conhecimento sobre práticas básicas, como a troca de senhas, atualizações e configurações seguras, contribui diretamente para o aumento das vulnerabilidades. Usuários bem informados tendem a adotar medidas preventivas e a reduzir significativamente os riscos associados. Portanto, além das soluções técnicas, promover campanhas educativas, materiais de orientação e treinamentos é essencial para fortalecer a segurança e minimizar os impactos das ameaças no uso da IoT residencial.

6 Desafios de Pesquisa e Direções

A presente revisão sistemática adotou uma abordagem estruturada para identificar os principais riscos de segurança associados à IoT no ambiente doméstico, bem como métodos de mitigação propostos na literatura. Os resultados indicam que, embora existam diversas soluções técnicas disponíveis como autenticação multifator e atualizações regulares, a conscientização do usuário permanece como um fator crítico na efetividade dessas medidas. A análise evidenciou ainda a importância da integração entre medidas técnicas e ações educativas para aumentar a resiliência das redes domésticas.

Apesar dos achados relevantes, o estudo apresenta algumas limitações que merecem ser consideradas. A primeira diz respeito à delimitação temática por concentrar a análise exclusivamente no uso da IoT em ambientes domésticos, o que exclui outras áreas igualmente importantes, como saúde, agricultura e indústria. Essa escolha, embora estratégica para manter o foco e a profundidade da análise, reduz a abrangência dos resultados. Além disso, observou-se que, embora a quantidade de publicações sobre IoT seja crescente, muitos estudos carecem de foco direto na segurança ou não detalham estratégias de mitigação com profundidade. Isso limitou o número de fontes aplicáveis e pode ter restringido o mapeamento completo das práticas mais eficazes.

Para superar essas limitações, pesquisas futuras podem ampliar o escopo para incluir outros contextos de aplicação da IoT, comparando, por exemplo, o nível de maturidade em segurança entre ambientes residenciais e corporativos. Além disso, seria benéfico adotar metodologias mistas que combinem revisão sistemática com estudos empíricos, como entrevistas com usuários e testes de penetração em dispositivos reais. Outra direção promissora é a análise longitudinal de políticas de segurança implementadas pelos fabricantes, bem como o impacto de campanhas educativas na mudança de comportamento dos usuários. Esses caminhos podem oferecer uma visão mais holística e prática sobre os desafios de segurança em ambientes conectados.

7 Conclusão

A crescente inserção da Internet das Coisas em ambientes residenciais tem transformado significativamente a forma como os usuários interagem com seus lares. A automação, a conveniência e a conectividade oferecidas pelos dispositivos inteligentes trazem consigo uma série de benefícios, mas também introduzem novos riscos relacionados à segurança da informação e à privacidade dos dados pessoais. Este trabalho teve como objetivo identificar os principais riscos associados à IoT em residências, avaliar seus impactos, reunir estratégias eficazes de mitigação, por meio de uma revisão sistemática da literatura científica e conscientizar os usuários sobre o uso de boas práticas de segurança.

A análise evidenciou que os riscos mais recorrentes envolvem autenticação fraca, ausência de atualizações de *firmware* e comunicação sem criptografia, expondo os dispositivos a acessos não autorizados, interceptações e ataques cibernéticos. Dentre os métodos de mitigação mais citados na literatura, destacam-se a implementação de autenticação forte, como o uso de autenticação multifator, o emprego de criptografia nas comunicações e a realização de atualizações periódicas dos sistemas. Outras práticas relevantes incluem segmentação de rede, auditorias regulares e, especialmente, a conscientização dos usuários como forma de reduzir a superfície de ataque nos lares conectados.

Quanto à viabilidade das medidas de proteção, muitas podem ser implementadas diretamente pelos próprios usuários, mesmo sem conhecimento técnico avançado, como a troca imediata de senhas padrão por senhas fortes, a ativação da autenticação em duas etapas, a atualização regular do *firmware* dos dispositivos e o uso de redes *Wi-Fi* separadas para equipamentos *IoT*. No entanto, outras ações dependem da iniciativa dos fabricantes, como oferecer dispositivos com autenticação forte habilitada por padrão, suporte a atualizações automáticas e criptografia ativa desde a instalação. Cabe também ao poder público estabelecer padrões mínimos de segurança voltados a esse tipo de tecnologia, promovendo uma regulamentação mais robusta.

Como contribuição, este trabalho oferece uma síntese crítica e atualizada sobre as principais ameaças e soluções no contexto da *IoT* residencial, servindo de base para novos estudos, boas práticas de desenvolvimento e políticas públicas. Um diferencial importante da pesquisa foi a ênfase na conscientização dos usuários como primeira linha de defesa, destacando que a segurança em ambientes inteligentes não pode se basear apenas em medidas técnicas, mas exige também educação digital contínua. Para pesquisas futuras, recomenda-se a realização de estudos empíricos que avaliem a eficácia dos métodos sugeridos, bem como o desenvolvimento de soluções com tecnologias emergentes, como *blockchain* (registro digital seguro, onde as informações são armazenadas em conjuntos ligados entre si) e *inteligência artificial*.

Referências

AGAZZI, A. E. *Smart Home, security concerns of IoT*. 2020. Disponível em: <https://arxiv.org/abs/2007.02628>. Citado 3 vezes nas páginas 26, 29 e 30.

AIKEN, W.; RYOO, J.; RIZVI, S. An internet of things (iot) security assessment for households. In: *2020 International Conference on Software Security and Assurance (ICSSA)*. [S.l.: s.n.], 2020. p. 53–59. Citado 4 vezes nas páginas 24, 26, 28 e 29.

ALI, W. et al. Iot based smart home: Security challenges, security requirements and solutions. In: *2017 23rd International Conference on Automation and Computing (ICAC)*. [S.l.: s.n.], 2017. p. 1–6. Citado 5 vezes nas páginas 24, 26, 27, 29 e 30.

ALRAWI, O. et al. Sok: Security evaluation of home-based iot deployments. In: *2019 IEEE Symposium on Security and Privacy (SP)*. [S.l.: s.n.], 2019. p. 1362–1380. Citado 5 vezes nas páginas 24, 26, 27, 29 e 30.

ALZAYLAEE, M. K. A systematic review of security vulnerabilities in smart home devices and mitigation techniques. *IJCSNS*, v. 25, n. 3, p. 206, 2025. Citado na página 19.

ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. [S.l.]: Wiley, 2020. Citado na página 17.

BADA, M.; SASSE, A. M.; NURSE, J. R. C. *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* 2019. Disponível em: <https://arxiv.org/abs/1901-.02672>. Citado na página 17.

BARBIERI, C. E. F. Vulnerabilidades de dispositivos iot em smart homes. 004, 2022. Citado 2 vezes nas páginas 12 e 19.

BASTOS, D.; SHACKLETON, M.; EL-MOUSSA, F. Internet of things: A survey of technologies and security risks in smart home and city environments. In: *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. [S.l.: s.n.], 2018. p. 1–7. Citado na página 19.

BERLANDA, R. G. Guia de segurança da informação para a conectividade de dispositivos iot. 2021. Citado na página 18.

BERTOLLO, M.; CASTILLO, R. A.; BUSCA, M. D. Internet das coisas (iot) e novas dinâmicas da produção agrícola no campo brasileiro. Citado na página 15.

BORTOLI, K. U. d.; BALTAZAR, N. C. Segurança em iot. 004, 2023. Citado na página 12.

BUGEJA, J.; JACOBSSON, A.; DAVIDSSON, P. On privacy and security challenges in smart connected homes. In: *2016 European Intelligence and Security Informatics Conference (EISIC)*. [S.l.: s.n.], 2016. p. 172–175. Citado 2 vezes nas páginas 26 e 29.

CARVALHO, A. F. A. d.; SANTOS, C. M. L.; GONÇALVES, L. V. Segurança em iot. 2022. Citado 2 vezes nas páginas 12 e 17.

CNN Brasil. *Internet das Coisas: o que é, como funciona e exemplos de uso*. 2023. Disponível em: https://www.cnnbrasil.com.br/tecnologia/internet-das-coisas/. Acesso em: 07 de maio 2024. Citado na página 15.

DAR, A. A. et al. Strategic security audit protocol: Safeguarding smart home iot devices against vulnerabilities. In: *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*. [S.l.: s.n.], 2024. p. 1386–1391. Citado 5 vezes nas páginas 24, 26, 28, 29 e 30.

DELICADO, A. et al. *A Internet das Coisas em Contexto Doméstico: Dimensões Sociais*. [S.l.], 2024. Projeto Engage$_{I}oTfinanciadopelaFCT(EXPL/SOC-SOC/1375/2021).Disponívelem$:<*https* : /-/*repositorio.ulisboa.pt/bitstream*/10451/65121/3-/*ICS_ADelicado_JRowland_MTruninger_CMour%C3%A3o_MRosales_A_Internet-.pdf*>.*Citado2vezesnaspáginas26e* 29.

DHANRAJ, T. et al. A review on mitigating privacy risks in iot-enabled smart homes. *Computer Networks and Communications*, v. 2, p. 132–147, 05 2024. Citado na página 19.

DIK, D. et al. Key issues of information security of smart home systems. In: *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*. [S.l.: s.n.], 2020. p. 1–7. Citado na página 26.

FERNANDES, N. O. C. Segurança da informação. 2018. Citado na página 17.

FIGUEIRA, V. P. "internet das coisas": um estudo sobre questões de segurança, privacidade e infraestrutura. Universidade Federal Fluiminense, 2016. Citado na página 18.

GAITAN, N.-C.; GAITAN, V. G.; UNGUREAN, I. A survey on the internet of things software arhitecture. *International Journal of Advanced Computer Science and Applications*, 2014. Citado na página 15.

GALEGALE, G. P. et al. Internet das coisas aplicada a negócios-um estudo bibliométrico. *JISTEM-Journal of Information Systems and Technology Management*, SciELO Brasil, v. 13, n. 3, p. 423–438, 2016. Citado na página 15.

GAMUNDANI, A. M.; PHILLIPS, A.; MUYINGI, H. N. An overview of potential authentication threats and attacks on internet of things(iot): A focus on smart home applications. In: *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. [S.l.: s.n.], 2018. p. 50–57. Citado 5 vezes nas páginas 24, 26, 27, 29 e 30.

GONÇALVES, R. L. M. Automatização residencial: um estudo de caso da aplicação da internet das coisas. 2019. Citado 2 vezes nas páginas 16 e 18.

HUREL, L. M.; LOBATO, L. C. Segurança e privacidade para a internet das coisas. *Minas Gerais: Instituto Igarapé*, 2018. Citado na página 18.

ITEN, R.; WAGNER, J.; RöSCHMANN, A. Z. On the identification, evaluation and treatment of risks in smart homes: A systematic literature review. *Risks*, v. 9, n. 6, 2021. ISSN 2227-9091. Disponível em: <https://www.mdpi.com/2227-9091/9/6/113>. Citado na página 19.

JAMES, F. Iot cybersecurity based smart home intrusion prevention system. In: *2019 3rd Cyber Security in Networking Conference (CSNet)*. [S.l.: s.n.], 2019. p. 107–113. Citado 6 vezes nas páginas 24, 26, 27, 28, 29 e 30.

JAMES, F. A risk management framework and a generalized attack automata for iot based smart home environment. In: *2019 3rd Cyber Security in Networking Conference (CSNet)*. [S.l.: s.n.], 2019. p. 86–90. Citado 4 vezes nas páginas 24, 26, 27 e 29.

KABIR, S.; GOPE, P.; MOHANTY, S. P. A security-enabled safety assurance framework for iot-based smart homes. *IEEE Transactions on Industry Applications*, v. 59, n. 1, p. 6–14, 2023. Citado 4 vezes nas páginas 25, 26, 27 e 29.

KADOW, A.; CAMARGO, C. Internet das coisas: vulnerabilidade, privacidade e pontos de segurança. *Revista Competência*, v. 9, n. 1, p. 153–161, 2016. Citado na página 17.

KITCHENHAM, B. Procedures for performing systematic reviews. *Keele, UK, Keele Univ.*, v. 33, 08 2004. Citado na página 21.

KITSIOU, S. et al. Effectiveness of mhealth interventions for patients with diabetes: An overview of systematic reviews. *PLoS One*, v. 12, n. 3, p. e0173160, 2017. Disponível em: <https://doi.org/10.1371/journal.pone.0173160>. Citado na página 15.

KUYUCU, M. K.; BAHTIYAR, ; İNCE, G. Security and privacy in the smart home: A survey of issues and mitigation strategies. In: *2019 4th International Conference on Computer Science and Engineering (UBMK)*. [S.l.: s.n.], 2019. p. 113–118. Citado na página 19.

LIMA, G. V. d. N. *Uma visão geral sobre segurança em soluções iot para ambientes residenciais*. Dissertação (B.S. thesis), 2023. Citado 2 vezes nas páginas 12 e 19.

MACHADO, F. N. R. *Segurança da informação: princípios e controle de ameaças*. [S.l.]: Saraiva Educação SA, 2014. Citado na página 16.

macrovector. *Internet das coisas: conheça as tendências*. 2018. https://conectaja.proteste.org.br/internet-das-coisas-para-sua-casa/. Accessed: 2024–23. Citado 2 vezes nas páginas 8 e 16.

MANYIKA, J. et al. *Unlocking the Potential of the Internet of Things: Executive Summary*. 2023. Disponível em: <https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx>. Citado na página 15.

MARINHO, R. A.; BODÊ, J. Gamificação aplicada a programas e campanhas de conscientização de segurança da informação. In: *FatecSeg-Congresso de Segurança da Informação*. [S.l.: s.n.], 2022. Citado na página 16.

MILENKOVIć, M. et al. Analysis of iot devices security for household applications. In: *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*. [S.l.: s.n.], 2023. p. 1490–1495. Citado 3 vezes nas páginas 26, 29 e 30.

Mordor Intelligence™ Industry Reports. *Tamanho do mercado de dispositivos IoT e análise de participação – Tendências e previsões de crescimento (2024 – 2029)*. 2024. Disponível em: https://www.mordorintelligence.com/pt/industry-reports/iot-devices-market. Acesso em: 22 de abril 2024. Citado na página 12.

PACETE, Luiz Gustavo . *IoT: até 2025, mais de 27 bilhões de dispositivos estarão conectados*. 2022. Disponível em: https://forbes.com.br/forbes-tech/2022/08/iot-ate-2025-mais-de-27-bilhoes-de-dispositivos-estarao-conectados/. Acesso em: 10 de maio 2024. Citado na página 15.

PARSONS, E. K.; PANAOUSIS, E.; LOUKAS, G. How secure is home: Assessing human susceptibility to iot threats. In: *Proceedings of the 24th Pan-Hellenic Conference on Informatics*. New York, NY, USA: Association for Computing Machinery, 2021. (PCI '20), p. 64–71. ISBN 9781450388979. Disponível em: <https://doi.org/10.1145/3437120-.3437277>. Citado na página 26.

PEREIRA, J. C.; SENO, G. P. Segurança e privacidade na internet das coisas. 171, 2022. Citado na página 18.

PEREIRA, Rafael. *Transformando o Lar: Como Utilizar a Internet das Coisas (IoT) em Sua Residência*. 2023. Disponível em: https://www.dio.me/articles/transformando-o-lar-como-utilizar-a-internet-das-coisas-iot-em-sua-residencia. Acesso em: 07 de maio 2024. Citado na página 16.

PINHEIRO, P. A. A. *SmartHoming: sistema IoT de gestão de cuidados e segurança domésticos*. Tese (Doutorado), 2023. Citado na página 15.

Protiviti. *Pilares da Segurança da Informação*. 2023. https://www.protiviti.com.br/cybersecurity/pilares-seguranca-da-informacao/. Accessed: 2024-07-21. Citado 2 vezes nas páginas 8 e 17.

RAJKHAN, N. W.; SONG, J. Iot smart home devices' security, privacy, and firmware labeling system. In: *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. [S.l.: s.n.], 2021. p. 1874–1880. Citado 4 vezes nas páginas 24, 26, 27 e 29.

RYOO, J.; TJOA, S.; RYOO, H. An iot risk analysis approach for smart homes (work-in-progress). In: *2018 International Conference on Software Security and Assurance (ICSSA)*. [S.l.: s.n.], 2018. p. 49–52. Citado 6 vezes nas páginas 24, 26, 27, 28, 29 e 30.

SANTOS, C. C.; SALES, J. D. A. O desafio da privacidade na internet das coisas. *GESTÃO. Org*, Universidade Federal de Pernambuco (UFPE), v. 13, n. 4, p. 282–290, 2015. Citado na página 18.

SHARBAF, M. S. Iot driving new business model, and iot security, privacy, and awareness challenges. In: *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*. [S.l.: s.n.], 2022. p. 1–4. Citado 3 vezes nas páginas 26, 29 e 30.

SHOURAN, Z.; ASHARI, A.; PRIYAMBODO, T. K. Internet of things (iot) of smart home: Privacy and security. *International Journal of Computer Applications*, v. 182, n. 39, p. 1–5, February 2019. ISSN 0975–8887. Disponível em: <https://www.ijcaonline-.org/archives/volume182/number39/shouran-2019-ijca-918450.pdf>. Citado 2 vezes nas páginas 26 e 29.

SILVA, D. R. Pilar da; STEIN, L. M. Segurança da informação: uma reflexão sobre o componente humano. *Ciências & Cognição*, Instituto de Ciências Cognitivas, v. 10, p. 46–53, 2007. Citado na página 16.

SINGH, J.; SINGH, G.; NEGI, S. Evaluating security principals and technologies to overcome security threats in iot world. In: *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. [S.l.: s.n.], 2023. p. 1405–1410. Citado na página 26.

SIVAPRIYAN, R. et al. Analysis of security challenges and issues in iot enabled smart homes. In: *2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*. [S.l.: s.n.], 2021. p. 1–6. Citado 4 vezes nas páginas 24, 26, 27 e 29.

SUPARNA, N.; MANJAIAH, D. Implementation and performance analysis of idea in iot-based smart home networks. p. 212–216, 2022. Citado na página 18.

TRABELSI, Z. Iot based smart home security education using a hands-on approach. In: *2021 IEEE Global Engineering Education Conference (EDUCON)*. [S.l.: s.n.], 2021. p. 294–301. Citado 2 vezes nas páginas 26 e 30.

VARDAKIS, G. et al. Review of smart-home security using the internet of things. *Electronics*, v. 13, n. 16, 2024. ISSN 2079-9292. Disponível em: <https://www.mdpi-.com/2079-9292/13/16/3343>. Citado na página 26.

VARGHESE, J.; HAYAJNEH, T. A framework to identify security and privacy issues of smart home devices. In: *2018 9th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*. [S.l.: s.n.], 2018. p. 135–143. Citado 2 vezes nas páginas 26 e 29.

WANG, Z. et al. A survey on iot-enabled home automation systems: Attacks and defenses. *IEEE Communications Surveys Tutorials*, v. 24, n. 4, p. 2292–2328, 2022. Citado 3 vezes nas páginas 26, 29 e 30.

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO DIGITAL NA BIBLIOTECA "JOSÉ ALBANO DE MACEDO"

Identificação do Tipo de Documento

( ) Tese

( ) Dissertação

(X) Monografia

( ) Artigo

Eu, **Yuri Marques da Silva**, autorizo com base na Lei Federal nº 9.610 de 19 de Fevereiro de 1998 e na Lei nº 10.973 de 02 de dezembro de 2004, a biblioteca da Universidade Federal do Piauí a divulgar, gratuitamente, sem ressarcimento de direitos autorais, o texto integral da publicação Internet das Coisas: Análise de Riscos e Métodos de Prevenção em um Ambiente Doméstico de minha autoria, em formato PDF, para fins de leitura e/ou impressão, pela internet a título de divulgação da produção científica gerada pela Universidade.

Picos-PI 07 de julho de 2025.

gov.br Documento assinado digitalmente
YURI MARQUES DA SILVA
Data: 07/07/2025 12:35:17-0300
Verifique em https://validar.iti.gov.br

_____

Assinatura