doi.org/10.51891/rease.v12i7.29127

VULNERABILIDADES E ESTRATÉGIAS DE MITIGAÇÃO EM IoT DOMÉSTICA: UMA REVISÃO INTEGRATIVA DA LITERATURA

VULNERABILITIES AND MITIGATION STRATEGIES IN HOME IOT: AN INTEGRATIVE LITERATURE REVIEW

Glaucia Nunes de Lima Santos[1]
Samira Dias Silva[2]
Paulo Cristiano Abreu de Jesus[3]
Gleisson Amaral Mendes[4]

RESUMO: A Internet das Coisas (IoT) tem promovido a integração de dispositivos inteligentes em ambientes domésticos, ampliando a conectividade e a automação residencial. Entretanto, essa expansão intensifica os desafios de segurança cibernética e privacidade dos usuários. Este estudo investigou as principais vulnerabilidades em dispositivos IoT domésticos e as estratégias de mitigação descritas na literatura. Realizou-se uma revisão integrativa conduzida conforme o PRISMA 2020 e estruturada pela estratégia PICo, com buscas nas bases CAPES, *Scopus*, *Web of Science*, IEEE *Xplore* e ACM *Digital Library*, resultando na seleção de 12 estudos publicados entre 2018 e 2024. A análise temática identificou três categorias: camada de dispositivo, camada de rede e camada de usuário. Os resultados apontam que as vulnerabilidades mais recorrentes são senhas padrão, firmware desatualizado, protocolos inseguros e baixa conscientização dos usuários. As estratégias de mitigação mais recomendadas envolvem autenticação robusta, criptografia, segmentação de redes e educação em segurança digital. Como contribuição original, propõe-se um Framework de Segurança IoT Doméstica, composto por taxonomia de vulnerabilidades, matriz de mitigação e modelo conceitual integrado. Conclui-se que a proteção da IoT doméstica requer abordagem integrada que articule tecnologia, educação e regulação.

Palavras-chave: Internet das Coisas. Segurança Cibernética. IoT Doméstica. Vulnerabilidades. Estratégias de Mitigação.

[1]Graduanda em Engenharia de Software – Bacharelado, Universidade do Estado do Pará (UEPA) - Concórdia do Pará, Pará, Brasil.
[2]Graduanda em Engenharia de Software – Bacharelado, Universidade do Estado do Pará (UEPA) - Concórdia do Pará, Pará, Brasil.
[3]Mestrando em Processos e Tecnologias Educacionais em Rede Nacional ProfEducaTec. Universidade do Estado do Pará (UEPA) / Campus XXII – Ananindeua, Pará, Brasil.
[4]Doutorando em Ciências Ambientais, Docente na Universidade do Estado do Pará (UEPA) / Campus XXII – Ananindeua, Pará, Brasil.

ABSTRACT: The Internet of Things (IoT) has fostered the integration of smart devices into home environments, expanding connectivity and home automation. However, this expansion intensifies cybersecurity and user privacy challenges. This study investigated key vulnerabilities in home IoT devices and mitigation strategies described in the literature. An integrative review was conducted following PRISMA 2020 guidelines and structured using the PICo strategy; searches were performed across CAPES, Scopus, Web of Science, IEEE Xplore, and ACM Digital Library databases, resulting in the selection of 12 studies published between 2018 and 2024. Thematic analysis identified three categories: device layer, network layer, and user layer. Results indicate that the most recurring vulnerabilities are default passwords, outdated firmware, insecure protocols, and low user awareness. The most recommended mitigation strategies involve robust authentication, encryption, network segmentation, and digital security education. As an original contribution, a Home IoT Security Framework is proposed, comprising a vulnerability taxonomy, a mitigation matrix, and an integrated conceptual model. The study concludes that protecting home IoT requires an integrated approach that coordinates technology, education, and regulation.

Keywords: Internet of Things. Cybersecurity. Home IoT. Vulnerabilities. Mitigation Strategies.

1. INTRODUÇÃO

A Internet das Coisas (IoT – *Internet of Things*) representa uma das mais significativas transformações tecnológicas da era digital. Sua expansão tem possibilitado a integração entre dispositivos físicos e sistemas computacionais por meio da internet, permitindo a troca contínua de dados e a automação de processos nos mais diversos setores da sociedade. No ambiente doméstico, essa tecnologia tem sido amplamente incorporada por meio de dispositivos como câmeras de monitoramento, assistentes virtuais, televisores conectados, fechaduras eletrônicas e eletrodomésticos inteligentes (SANTAELLA et al., 2013).

O crescimento exponencial desses dispositivos tem modificado significativamente a forma como as pessoas interagem com a tecnologia em suas residências. Segundo a *International Data Corporation* (IDC, 2023), o número de dispositivos IoT conectados no mundo deve ultrapassar 21 bilhões em 2025, impulsionado pelo avanço das redes de comunicação e pela crescente demanda por soluções inteligentes. Entretanto, à medida que mais equipamentos integram redes domésticas, aumentam também os desafios relacionados à proteção de dados, privacidade e segurança cibernética.

Embora a Internet das Coisas ofereça inúmeros benefícios, sua rápida expansão tem revelado fragilidades importantes no que diz respeito à segurança dos dispositivos conectados. Muitos equipamentos são desenvolvidos com foco prioritário em funcionalidades e desempenho, enquanto aspectos relacionados à segurança da informação recebem atenção

limitada durante as etapas de projeto e implementação (HASSAN et al., 2024). Como consequência, diversas vulnerabilidades permanecem presentes nesses dispositivos, tornando-os potenciais alvos de ataques cibernéticos.

Entre os principais problemas identificados na literatura destacam-se o uso de senhas padrão fornecidas pelos fabricantes, mecanismos de autenticação inadequados, ausência de criptografia robusta, falhas em atualizações de firmware e protocolos de comunicação inseguros. Heartfield et al. (2018) propuseram uma taxonomia abrangente de ameaças cyber-físicas em casas inteligentes, classificando 25 tipos distintos de ataques segundo vetores de ataque, impacto nos sistemas e impacto na vida doméstica, evidenciando a complexidade e diversidade das ameaças que afetam ambientes residenciais conectados.

Outro fator que contribui para o aumento dos riscos está relacionado ao comportamento dos próprios usuários. Oliveira et al. (2024) apontam que grande parte dos consumidores possui conhecimento limitado sobre práticas de segurança digital, desconhecendo procedimentos básicos como alteração de senhas padrão, atualização periódica de sistemas e configuração adequada dos dispositivos. Essa falta de conscientização amplia significativamente a superfície de ataque disponível para cibercriminosos.

A preocupação com a segurança em ambientes IoT torna-se ainda mais relevante quando se considera a natureza dos dados coletados por esses dispositivos. Informações relacionadas a hábitos de consumo, localização geográfica, rotinas familiares e dados de saúde podem ser armazenadas e transmitidas continuamente. Paz et al. (2023) alertam que, caso esses dados sejam acessados indevidamente, os impactos podem envolver não apenas prejuízos financeiros, mas também graves violações de privacidade e comprometimento da integridade dos usuários.

Outro aspecto relevante refere-se à ausência de padrões universais de segurança para dispositivos IoT. Embora existam iniciativas regulatórias e recomendações internacionais voltadas à proteção desses sistemas, muitos fabricantes ainda adotam práticas heterogêneas de desenvolvimento, resultando em níveis variados de proteção (BOECKL et al., 2019). Em diversos casos, os dispositivos permanecem sem atualizações de segurança após poucos anos de comercialização, aumentando sua exposição a vulnerabilidades conhecidas.

Nesse contexto, torna-se fundamental compreender quais são as principais ameaças que afetam os dispositivos IoT domésticos e quais medidas podem ser implementadas para reduzir os riscos associados ao seu uso. Al-Garadi et al. (2020) demonstram que métodos de machine learning e deep learning representam abordagens promissoras para detecção de ataques em

ecossistemas IoT, identificando padrões anômalos de comportamento e antecipando ameaças ainda desconhecidas.

A relevância desta pesquisa está associada ao crescimento contínuo da Internet das Coisas no ambiente residencial e à necessidade de fortalecer mecanismos de proteção capazes de garantir a privacidade, a confidencialidade e a integridade das informações. Walterscheid, Huijts e Van Sintemaartensdijk (2024) evidenciam que consumidores tendem a adotar práticas mais seguras quando recebem informações claras sobre os riscos, reforçando a importância de estudos que subsidiem ações educativas e regulatórias.

Diante desse cenário, surge o seguinte problema de pesquisa: quais são as principais vulnerabilidades presentes nos dispositivos IoT domésticos e quais estratégias podem ser adotadas para mitigar os riscos de segurança associados? O objetivo geral consiste em investigar as principais vulnerabilidades em dispositivos IoT domésticos e identificar estratégias eficazes para sua mitigação, por meio de revisão integrativa da literatura contemplando estudos nacionais e internacionais publicados entre 2018 e 2024.

2. METODOLOGIA

2.1 DELINEAMENTO DA PESQUISA

A presente pesquisa caracteriza-se como uma revisão integrativa da literatura, conduzida com o objetivo de identificar, analisar e sintetizar as evidências científicas acerca das vulnerabilidades de segurança presentes em dispositivos de Internet das Coisas (IoT) utilizados em ambientes domésticos, bem como as estratégias propostas para mitigação desses riscos. A revisão integrativa foi adotada por possibilitar a incorporação de estudos com diferentes delineamentos metodológicos, permitindo uma compreensão ampla e sistematizada do fenômeno investigado e favorecendo a produção de novos modelos conceituais fundamentados na literatura.

O desenvolvimento da pesquisa seguiu as seis etapas propostas por Whittemore e Knafl (2005), posteriormente sistematizadas por Souza, Silva e Carvalho (2010) e Ercole, Melo e Alcoforado (2014): (I) definição da questão de pesquisa; (II) estabelecimento dos critérios de elegibilidade; (III) busca e seleção dos estudos; (IV) extração e organização dos dados; (V) análise crítica e síntese das evidências; e (VI) apresentação dos resultados. A adoção desse protocolo metodológico contribui para assegurar maior rigor científico, transparência e reprodutibilidade ao processo investigativo.

2.2 FORMULAÇÃO DA QUESTÃO NORTEADORA

A questão norteadora foi formulada pela estratégia *Population, Interest e Context* - PICo (SANTOS; PIMENTA; NOBRE, 2007), assegurando coerência entre pergunta, critérios de elegibilidade e seleção dos estudos. Neste estudo, a População (P) corresponde aos dispositivos e usuários de Internet das Coisas em ambientes domésticos; o Fenômeno de Interesse (I) refere-se às vulnerabilidades de segurança cibernética e às estratégias propostas para mitigação dos riscos; e o Contexto (Co) compreende os ambientes residenciais inteligentes (smart homes), caracterizados pela integração de dispositivos conectados em redes domésticas. A partir dessa estrutura, definiu-se a seguinte questão norteadora: Quais são as principais vulnerabilidades presentes em dispositivos IoT domésticos e quais estratégias têm sido propostas na literatura para mitigar os riscos de segurança associados a esses dispositivos?

2.3 ESTRATÉGIA DE BUSCA

A busca bibliográfica foi realizada de forma sistemática nas bases Portal de Periódicos CAPES, Scopus, Web of Science (WoS), IEEE Xplore e ACM Digital Library, selecionadas por sua relevância e abrangência na área de Computação e Segurança da Informação. A Scopus e a Web of Science foram utilizadas devido à sua ampla cobertura multidisciplinar e elevado rigor de indexação. A IEEE Xplore e a ACM Digital Library concentram publicações especializadas em Computação, Engenharia, Redes de Computadores e Segurança Cibernética, enquanto o Portal de Periódicos CAPES possibilitou a recuperação da produção científica nacional, ampliando a representatividade do contexto brasileiro.

As buscas foram realizadas nos campos título (*Title*), resumo (*Abstract*) e palavras-chave (*Keywords*), utilizando descritores em português e inglês combinados por operadores booleanos (*AND* e *OR*). A utilização de descritores nos dois idiomas teve como objetivo minimizar o viés de idioma (*language bias*) e ampliar a recuperação de estudos relevantes publicados em periódicos nacionais e internacionais. As estratégias de busca foram estruturadas especificamente de acordo com o idioma utilizado, consistindo em: (a) no idioma inglês, a combinação dos termos *("Internet of Things" OR "IoT" OR "smart home") AND ("vulnerability" OR "security threat") AND ("mitigation" OR "countermeasure" OR "security solution")*; e (b) no idioma português, a combinação dos termos *("Internet das Coisas" OR "IoT doméstica") AND ("vulnerabilidade" OR "ameaça cibernética") AND ("mitigação" OR "solução de segurança")*.

O levantamento contemplou artigos publicados entre 2018 e 2024, nos idiomas português e inglês. Esse recorte temporal foi definido em função da rápida evolução da Internet das Coisas e do crescimento das pesquisas em segurança cibernética após a disseminação de ataques em larga escala, como o *botnet* Mirai, que evidenciou vulnerabilidades críticas em dispositivos IoT domésticos e impulsionou o desenvolvimento de novas abordagens de proteção.

Para assegurar a transparência, a rastreabilidade e a reprodutibilidade da revisão, as estratégias de busca foram aplicadas de forma padronizada em todas as bases consultadas, realizando-se apenas as adaptações sintáticas necessárias às especificidades de cada mecanismo de pesquisa, sem alterar a lógica dos descritores e dos operadores booleanos empregados. A seleção de cada uma das bases de dados consultadas justificou-se por suas contribuições acadêmicas específicas, sendo elas: (1) o Portal de Periódicos CAPES, selecionado pela recuperação da produção científica nacional e pelo amplo acesso a periódicos internacionais que proporciona; (2) a *Scopus*, por ser uma base de dados multidisciplinar que conta com uma ampla cobertura e elevado rigor de indexação; (3) a *Web of Science* (WoS), em virtude de ser uma base internacional caracterizada por seu alto rigor científico e pela indexação de periódicos de elevado impacto; (4) a IEEE *Xplore*, por concentrar publicações altamente especializadas nos campos de Engenharia, Computação, Redes de Computadores e Segurança Cibernética; e (5) a ACM *Digital Library*, por consistir em uma base especializada em Ciência da Computação, Sistemas de Informação, Internet das Coisas e Segurança Digital.

2.4 CRITÉRIOS DE ELEGIBILIDADE

Os critérios de elegibilidade foram definidos previamente à realização das buscas bibliográficas, com o objetivo de assegurar consistência, transparência e reprodutibilidade ao processo de seleção dos estudos. Foram estabelecidos critérios de inclusão e exclusão alinhados ao objetivo da pesquisa e à questão norteadora formulada por meio da estratégia PICo.

Os critérios de inclusão contemplaram estudos científicos diretamente relacionados à segurança da Internet das Coisas em ambientes domésticos, enquanto os critérios de exclusão tiveram como finalidade eliminar publicações que não apresentavam aderência temática, rigor metodológico ou informações suficientes para subsidiar a análise proposta.

Para a seleção das publicações, foram adotados cinco Critérios de Inclusão específicos: (CI1) Artigos científicos completos publicados em periódicos revisados por pares; (CI2) Estudos publicados nos idiomas português ou inglês; (CI3) Publicações disponibilizadas entre

os anos de 2018 e 2024; (CI4) Estudos que abordassem vulnerabilidades de segurança e/ou estratégias de mitigação em dispositivos IoT domésticos ou ambientes residenciais inteligentes; e (CI5) Trabalhos com metodologia e resultados claramente descritos, que permitissem a extração das informações necessárias à revisão.

Em contrapartida, os Critérios de Exclusão aplicados para descartar registros inadequados consistiram em: (CE1) Estudos duplicados recuperados em mais de uma base de dados; (CE2) Trabalhos indisponíveis na íntegra; (CE3) Artigos cujo foco estivesse exclusivamente em ambientes industriais, hospitalares, agrícolas ou cidades inteligentes, sem relação direta com a IoT doméstica; (CE4) Resumos de eventos, editoriais, notas técnicas, capítulos de livros sem revisão por pares, dissertações, teses e literatura cinzenta; e (CE5) Estudos que não apresentassem metodologia ou resultados suficientemente detalhados para subsidiar a análise proposta.

Após a aplicação desses critérios, os estudos considerados potencialmente relevantes foram encaminhados para a etapa de leitura dos títulos e resumos, seguida da avaliação do texto completo para confirmação da elegibilidade. Esse procedimento permitiu selecionar apenas publicações com aderência temática e qualidade metodológica compatíveis com os objetivos desta revisão.

2.5 PROCESSO DE SELEÇÃO DOS ESTUDOS

O processo de seleção dos estudos foi conduzido de acordo com as recomendações do *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA 2020), conforme proposto por Page et al. (2021), assegurando transparência, rastreabilidade e reprodutibilidade em todas as etapas da revisão.

Inicialmente, as estratégias de busca foram aplicadas nas cinco bases de dados selecionadas, resultando na identificação de 580 registros. Em seguida, todas as referências recuperadas foram exportadas para o software *Mendeley Reference Manager*, utilizado para organização das referências e identificação automática de registros duplicados.

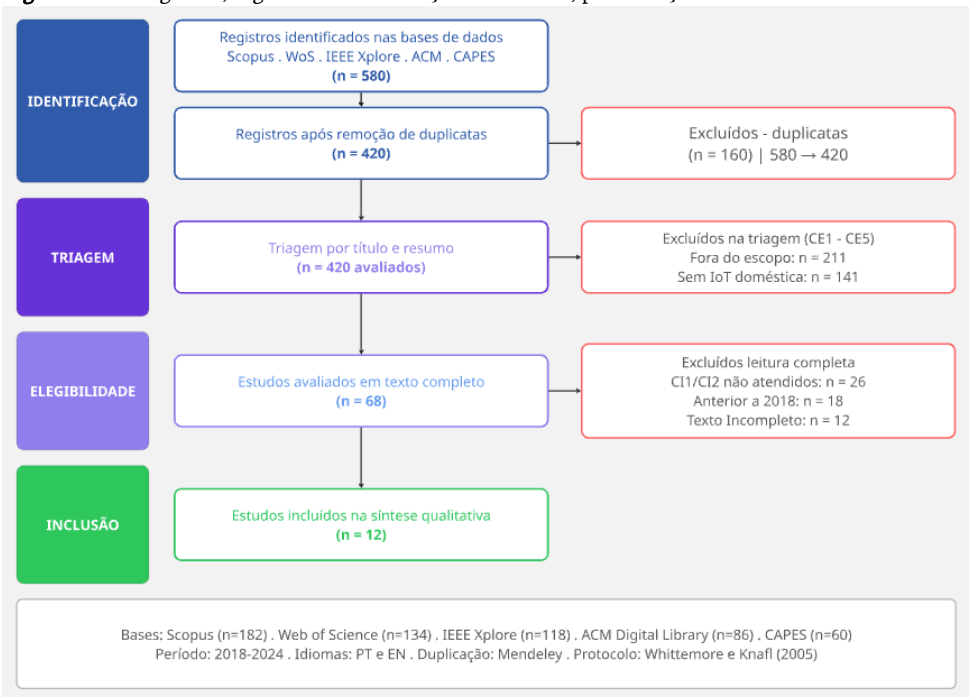
Após a remoção de 160 registros duplicados, permaneceram 420 estudos únicos, que foram submetidos à etapa de triagem por meio da leitura dos títulos e resumos. Nessa fase, foram excluídos os estudos que não atendiam aos critérios de elegibilidade previamente estabelecidos, especialmente aqueles sem relação direta com vulnerabilidades ou estratégias de mitigação em dispositivos IoT domésticos.

Como resultado da triagem inicial, 68 estudos foram considerados potencialmente elegíveis e submetidos à leitura integral. Durante essa etapa, realizou-se uma avaliação detalhada da aderência temática, da consistência metodológica e da disponibilidade das informações necessárias à extração dos dados. Ao final do processo de elegibilidade, 56 estudos foram excluídos pelos seguintes motivos:

> 26 estudos não atenderam aos critérios de inclusão CI4 e CI5, por não abordarem especificamente dispositivos IoT domésticos ou por apresentarem informações metodológicas insuficientes;
>
> 18 estudos estavam fora do recorte temporal estabelecido (CI3);
>
> 12 estudos não estavam disponíveis na íntegra (CE2).
>
> Dessa forma, a amostra final da revisão foi composta por 12 artigos científicos, que subsidiaram a análise crítica das evidências e o desenvolvimento do Framework de Segurança IoT Doméstica.

O fluxo completo das etapas de identificação, triagem, elegibilidade e inclusão dos estudos é apresentado na Figura 1, elaborada conforme as recomendações do protocolo PRISMA 2020.

Figura 1 – Fluxograma, segundo recomendações PRISMA, para seleção dos estudos encontrados.



Fonte: Elaborado pelos autores (2026).

2.6 EXTRAÇÃO E ORGANIZAÇÃO DOS DADOS

Após a definição da amostra final, composta por 12 estudos, realizou-se a leitura integral de todos os artigos selecionados. A extração dos dados foi conduzida de forma sistemática e

padronizada, com o objetivo de garantir uniformidade na coleta das informações e facilitar a comparação entre os estudos incluídos na revisão.

Para cada artigo foram extraídas informações bibliográficas, metodológicas e analíticas consideradas relevantes para responder à questão norteadora da pesquisa. Os dados coletados contemplaram: autoria, ano de publicação, país de origem, base de dados de recuperação, objetivo do estudo, características da população ou contexto investigado, principais vulnerabilidades identificadas, estratégias de mitigação propostas e os resultados mais relevantes relacionados à segurança em ambientes IoT domésticos.

As informações extraídas foram organizadas em uma matriz de análise desenvolvida pelos autores, permitindo a sistematização dos dados e a identificação de convergências, divergências e lacunas entre os estudos analisados. Essa organização também subsidiou a elaboração dos quadros síntese apresentados na seção de resultados, facilitando a comparação das evidências encontradas na literatura. O processo de extração e mapeamento dos dados considerou as seguintes categorias de informações: (1) Identificação, englobando o código atribuído ao estudo, seus respectivos autores, o ano em que foi publicado e o país de origem; (2) Caracterização, abrangendo o periódico científico de publicação, a base de dados de onde foi recuperado e o idioma original do estudo; (3) Aspectos metodológicos, compreendendo a definição do objetivo do estudo e a população ou contexto investigado; (4) Vulnerabilidades, identificando as principais vulnerabilidades de segurança apontadas pela literatura; (5) Estratégias de mitigação, levantando soluções, técnicas ou mecanismos de proteção recomendados nos artigos; e (6) Principais resultados, agrupando as evidências empíricas e teóricas relacionadas de forma geral à segurança em dispositivos IoT domésticos.

As informações sistematizadas constituíram a base para a etapa seguinte de análise e síntese das evidências, possibilitando identificar padrões recorrentes entre os estudos e construir categorias analíticas que fundamentaram a proposição do Framework de Segurança IoT Doméstica.

2.7 PROCEDIMENTOS DE ANÁLISE E SÍNTESE DAS EVIDÊNCIAS

Após a extração e organização dos dados, realizou-se a análise comparativa das evidências provenientes dos estudos selecionados, com o objetivo de identificar padrões recorrentes, convergências, divergências e lacunas relacionadas às vulnerabilidades de segurança e às estratégias de mitigação em dispositivos IoT domésticos.

A síntese das evidências foi conduzida por meio de uma análise temática de caráter indutivo, na qual os resultados dos estudos foram comparados quanto às vulnerabilidades identificadas, às estratégias de proteção propostas e aos contextos de aplicação. Inicialmente, as informações extraídas foram examinadas individualmente e, posteriormente, agrupadas conforme suas similaridades conceituais.

O fluxo desse processo analítico estruturou-se de forma sequencial ao longo de sete fases lógicas fundamentais, iniciando com (1) a definição dos artigos selecionados, que compuseram o corpus de análise inicial de 12 estudos; seguido pela (2) extração dos dados relevantes de cada artigo de forma isolada; (3) a comparação das evidências por meio do exame pormenorizado das semelhanças e diferenças nos resultados obtidos; e (4) o agrupamento por similaridade de descobertas e sugestões em blocos conceituais comuns. A partir disso, alcançou-se a fase de (5) categorias temáticas, em que emergiram três níveis específicos decorrentes da consolidação das similaridades, sendo eles a Camada de Dispositivo (que investiga vulnerabilidades e estratégias diretamente ligadas a dispositivos, hardware, firmware, autenticação e configurações de segurança), a Camada de Rede (que se concentra em vulnerabilidades e estratégias focadas na comunicação, nos protocolos, na infraestrutura de rede e na transmissão de dados) e a Camada de Usuário (que compreende vulnerabilidades e estratégias pertinentes ao comportamento dos indivíduos, à conscientização, à privacidade, à governança e aos aspectos regulatórios). O processo seguiu com (6) a síntese crítica, que envolveu a integração e interpretação detalhada das evidências consolidadas, culminando no (7) desenvolvimento do Framework, com a estruturação final e proposição do modelo explicativo.

Essas categorias foram definidas de forma iterativa, buscando representar as convergências observadas entre os estudos analisados e permitindo organizar os resultados de maneira sistemática e coerente com a questão norteadora da pesquisa. Posteriormente, cada categoria foi submetida à análise crítica, estabelecendo relações entre as diferentes abordagens encontradas na literatura, identificando consensos, divergências e oportunidades de investigação.

Foi realizada uma análise interpretativa das evidências, permitindo compreender não apenas a frequência das vulnerabilidades relatadas, mas também as relações existentes entre fatores tecnológicos, humanos e regulatórios envolvidos na segurança dos ambientes IoT domésticos. Essa abordagem favoreceu uma compreensão integrada do fenômeno investigado e subsidiou a construção do modelo conceitual proposto nesta pesquisa.

2.8 DESENVOLVIMENTO DO FRAMEWORK DE SEGURANÇA IOT DOMÉSTICA

O Framework de Segurança IoT Doméstica foi desenvolvido a partir da síntese integrativa das evidências identificadas nos estudos selecionados, buscando consolidar, em um modelo conceitual único, as principais vulnerabilidades de segurança e as estratégias de mitigação descritas na literatura.

A construção do framework fundamentou-se nos resultados obtidos durante a análise temática, na qual foram identificadas convergências entre os estudos quanto às vulnerabilidades recorrentes, aos mecanismos de proteção empregados e aos diferentes atores envolvidos na segurança dos ambientes IoT domésticos. A organização dessas evidências possibilitou estruturar uma proposta integrada capaz de representar, de forma sistemática, os principais elements que influenciam a segurança desses ambientes.

O processo de desenvolvimento ocorreu por meio de três etapas sequenciais e interligadas, gerando resultados complementares que fundamentaram a síntese de evidências e deram origem à estrutura final. Na Etapa 1, correspondente à consolidação das vulnerabilidades, realizou-se o levantamento exaustivo e a síntese das fraquezas recorrentes apontadas nos 12 estudos selecionados, gerando como resultado a Taxonomia de Vulnerabilidades, responsável por categorizar as falhas detectadas conforme a sua natureza intrínseca e organizá-las hierarquicamente pelo seu nível específico de ocorrência. Na Etapa 2, voltada ao relacionamento com estratégias de mitigação, envolveu-se a associação direta das estratégias de segurança sugeridas na literatura com as respectivas vulnerabilidades mapeadas anteriormente, determinando também quais são os agentes responsáveis pela sua implementação prática, o que resultou na Matriz de Mitigação, a qual cruza vulnerabilidades com mecanismos de proteção e indica o nível de aplicação de cada ação, seja no nível do dispositivo, da rede ou do usuário. Por fim, na Etapa 3, caracterizada pela integração em um modelo conceitual, realizou-se a convergência entre as vulnerabilidades consolidadas, as estratégias mapeadas e os diferentes atores envolvidos, construindo um elo interpretativo de interdependência mútua entre as

dimensões tecnológicas, humanas e normativas, cujo resultado foi a elaboração de um Modelo Conceitual Integrado, que estabelece as relações entre as camadas do ambiente e oferece uma visão sistêmica sobre a proteção integrada da IoT doméstica.

Esse encadeamento analítico permitiu cruzar as convergências e as lacunas da literatura para compor a proposta definitiva do Framework de Segurança IoT Doméstica, o qual foi estruturado a partir de três pilares centrais interdependentes: (a) a Camada de Dispositivo, focando na proteção voltada a hardware, firmware, mecanismos de autenticação e configurações locais de segurança dos aparelhos; (b) a Camada de Rede, tratando do gerenciamento de protocolos de rede, comunicação segura, infraestrutura e fluxos saudáveis de transmissão de dados; e (c) a Camada de Usuário, voltando-se para o comportamento humano, a promoção da conscientização em segurança digital, a proteção da privacidade, a governança dos dados e a adoção de boas práticas regulatórias.

O framework proposto possui natureza conceitual e tem como finalidade sintetizar o conhecimento produzido pela literatura analisada, oferecendo uma estrutura de referência para pesquisadores, fabricantes, desenvolvedores, órgãos reguladores e usuários na compreensão das vulnerabilidades e na definição de estratégias de proteção em dispositivos IoT domésticos.

Ressalta-se que esta proposta não constitui um modelo validado experimentalmente, mas uma construção teórica fundamentada nas evidências identificadas nesta revisão integrativa, cuja validação empírica poderá ser realizada em pesquisas futuras.

3. RESULTADOS E DISCUSSÃO

Após a aplicação dos critérios de inclusão e exclusão, foram selecionados 12 estudos publicados entre 2018 e 2024, que abordam vulnerabilidades e estratégias de mitigação em dispositivos IoT domésticos. Os estudos estão identificados no Quadro 1, com informações de procedência, e analisados no Quadro 2, com síntese do conteúdo.

Quadro 1 – Identificação dos estudos selecionados

Código	Título do artigo	Autores	País/Idioma	Periódico (ano)	Procedência
A01	Desafios e soluções em segurança de IoT: conscientização e prevenção de ataques	Oliveira et al.	Brasil / PT	Revista Contemporânea (2024)	CAPES
A02	Secure smart home IoT ecosystem for public safety and privacy protection	Hassan et al.	Nigéria / EN	Int. J. Multidisciplinary Research (2024)	Scopus

A03	Cybersecurity in a scalable smart city framework using blockchain and federated learning for IoT	Sefati et al.	Irã / EN	Smart Cities (2024)	Web of Science
A04	Nudging purchase intention towards more secure domestic IoT: label features and psychological mechanisms	Walterscheid; Huijts; Van Sintemaartensdijk	Holanda / EN	Computers in Human Behavior Reports (2024)	Scopus
A05	Ethics in Internet of Things security: challenges and opportunities	Szymoniak; Kubanek	Polônia / EN	Smart Ethics in the Digital World (2024)	Scopus
A06	Internet das Coisas: a vulnerabilidade do consumidor no compartilhamento de dados	Paz et al.	Brasil / PT	Rev. de Tecnologia Aplicada (2023)	CAPES
A07	Security standards for low-end IoT devices: a comparative review	Tertulino da Silva; Antunes	Brasil / EN	RECIMA21 (2023)	CAPES
A08	Análise de segurança em dispositivos Internet das Coisas	Moura; Neves	Brasil / PT	Rev. Interface Tecnológica (2021)	CAPES
A09	Utilização de ontologias na avaliação de segurança cibernética na Internet das Coisas	Rezende; Marques; Parreiras	Brasil / PT	Ciência da Informação (2021)	Scopus
A10	Estudo sobre segurança e privacidade na Internet das Coisas (IoT)	Della Rovere; Florian	Brasil / PT	RECIMA21 (2022)	CAPES
A11	A survey of machine and deep learning methods for Internet of Things (IoT) security	Al-Garadi et al.	Catar–EUA / EN	IEEE Comm. Surveys & Tutorials (2020)	IEEE Xplore
A12	A taxonomy of cyber-physical threats and impact in the smart home	Heartfield et al.	Reino Unido / EN	Computers & Security (2018)	Web of Science

Fonte: Elaborado pelos autores (2026).

Quadro 2 – Síntese analítica dos estudos selecionados

Código	Objetivo do estudo	Intervenção (I)	População (P)	Principais resultados / Vulnerabilidades
A01	Identificar desafios e soluções em segurança IoT doméstica	Análise de práticas de segurança e conscientização	Usuários de IoT doméstica	Baixa conscientização; senhas padrão; ausência de atualização de firmware
A02	Analisar segurança e privacidade em casas inteligentes	Criptografia, MFA e controles de privacidade	Ecossistemas IoT residenciais	Falhas de autenticação; exposição de dados pessoais; ataques remotos
A03	Propor framework com blockchain e aprendizado federado para IoT	Blockchain e federated learning	Redes IoT conectadas	Ataques distribuídos; falta de rastreabilidade; blockchain como contramedida eficaz
A04	Investigar influência da rotulagem de segurança na intenção de compra	Rotulagem e conscientização do consumidor	Consumidores de dispositivos IoT	Consumidores optam por dispositivos mais seguros quando informados; falta de transparência
A05	Analisar desafios éticos na segurança de IoT	Frameworks éticos e tríade CIA	Fabricantes, desenvolvedores e usuários	Desafios éticos na coleta de dados; necessidade de governança responsável

A06	Investigar vulnerabilidade do consumidor no compartilhamento de dados	Educação digital e transparência	Usuários de IoT doméstica	Compartilhamento excessivo de dados; desconhecimento dos direitos e riscos
A07	Comparar padrões de segurança para dispositivos IoT de baixo custo	Normas e frameworks internacionais de segurança	Fabricantes de dispositivos IoT entry-level	Ausência de padrões mínimos; inconsistência entre fabricantes; necessidade de certificação
A08	Analisar segurança em dispositivos IoT domésticos	Avaliação de configurações e práticas de atualização	Dispositivos IoT residenciais	Configurações inseguras de fábrica; ausência de atualizações periódicas de firmware
A09	Revisar abordagens de avaliação de segurança cibernética em IoT	Modelos de avaliação e ontologias de segurança	Ambientes IoT heterogêneos	Falhas estruturais; ausência de padrões; necessidade de modelos formais de avaliação
A10	Analisar segurança e privacidade em dispositivos IoT	Revisão de práticas e políticas de segurança	Dispositivos IoT domésticos e urbanos	Senhas padrão; ausência de criptografia; protocolos inseguros; riscos à privacidade
A11	Revisar métodos ML/DL para segurança IoT	Técnicas ML/DL para detecção de intrusões e ataques	Sistemas e dispositivos IoT em geral	DDoS via botnets (Mirai); ataques MitM; eavesdropping; ML/DL como contramedida eficaz
A12	Propor taxonomia de ameaças cyber-físicas em casas inteligentes	Taxonomia de vetores de ataque e impacto doméstico	Residências inteligentes com IoT	25 tipos de ataques classificados: WiFi, ZigBee, Bluetooth, firmware, cadeia suprimentos; impactos físicos e emocionais

Nota: I = Intervenção/estratégia analisada; P = População/contexto do estudo.
Fonte: Elaborado pelos autores (2026).

Os estudos selecionados foram organizados em três eixos temáticos correspondentes às camadas do framework proposto: vulnerabilidades na camada de dispositivo, ameaças na camada de rede e fatores humanos e regulatórios na camada de usuário. Essa estrutura permite superar a descrição isolada dos achados e promover o diálogo crítico entre os estudos, revelando convergências, tensões e lacunas relevantes para o contexto brasileiro.

3.1 CAMADA DE DISPOSITIVO: O PROBLEMA ESTRUTURAL DO DESIGN INSEGURO

A análise dos estudos A07, A08, A10 e A12 revela um padrão estrutural preocupante: as vulnerabilidades mais recorrentes em dispositivos IoT domésticos não decorrem de falhas acidentais ou de ataques sofisticados, mas de decisões deliberadas de projeto que priorizam custo e velocidade de lançamento em detrimento da segurança. Tertulino da Silva e Antunes (A07) demonstram que dispositivos de baixo custo, que representam a maior fatia do mercado doméstico, sistematicamente descumprem padrões mínimos de segurança, como o NIST SP 800-213 e o ETSI EN 303 645, sem que haja qualquer mecanismo coercitivo que impeça sua

comercialização. Essa constatação confronta diretamente o argumento de Hassan et al. (A02), que propõem soluções baseadas em criptografia TLS e autenticação multifatorial como se fossem de implementação trivial: se os próprios fabricantes não adotam nem mesmo a substituição de senhas padrão, a distância entre o que a literatura técnica prescreve e o que chega ao mercado permanece abismal.

Heartfield et al. (A12) oferecem a perspectiva analítica mais abrangente sobre essa camada ao demonstrarem que o firmware vulnerável não é apenas uma porta de entrada técnica, mas um vetor que permite ao atacante escalar privilégios e comprometer outros dispositivos na rede doméstica em efeito cascata. Esse achado tensiona a abordagem de Moura e Neves (A08), que tratam a ausência de atualizações como problema de comportamento do usuário: a análise de Heartfield et al. (A12) evidencia que a responsabilidade primária é do fabricante, que não implementa mecanismos de atualização automática seguros. No contexto brasileiro, essa tensão tem implicações práticas severas: a LGPD responsabiliza os controladores de dados, entre eles os fabricantes, pela segurança dos sistemas, mas o Decreto nº 9.854/2019, que institui o Plano Nacional de IoT, não estabelece requisitos técnicos mínimos de segurança para dispositivos comercializados no país, criando um vácuo regulatório que favorece a proliferação de equipamentos inseguros.

Rezende, Marques e Parreiras (A09) apontam para outra dimensão crítica: a ausência de modelos formais de avaliação de segurança que possam ser aplicados de maneira independente do fabricante. Enquanto os países europeus avançam na implementação do Cyber Resilience Act, que exigirá certificação de segurança para dispositivos IoT comercializados na União Europeia a partir de 2027, o Brasil não dispõe de instrumento equivalente. Essa lacuna regulatória nacional representa, na avaliação desta revisão, o principal fator que perpetua o ciclo de design inseguro identificado pelos estudos analisados, pois sem obrigação regulatória, a pressão competitiva de mercado sempre favorecerá o dispositivo mais barato em detrimento do mais seguro.

3.2 CAMADA DE REDE: SOFISTICAÇÃO DOS ATAQUES VERSUS MATURIDADE DAS DEFESAS

Os estudos A03, A11 e A12 convergem na identificação de um paradoxo inquietante: enquanto os vetores de ataque na camada de rede evoluem rapidamente em sofisticação e escala, as defesas disponíveis para o usuário doméstico permaneceram praticamente inalteradas na

última década. Al-Garadi et al. (A11) documentam que o botnet Mirai, que explorou credenciais padrão em câmeras IP e roteadores domésticos para orquestrar ataques DDoS de terabits por segundo, foi lançado em 2016, e seus descendentes ainda circulam ativamente, explorando as mesmas vulnerabilidades. Esse dado é analiticamente revelador: não se trata de ameaças novas, mas da persistência de vulnerabilidades antigas em dispositivos que continuam sendo vendidos. A sofisticação não está no ataque, mas na incapacidade estrutural do ecossistema de responder.

Heartfield et al. (A12) ampliam significativamente essa análise ao demonstrarem que os ataques em redes domésticas inteligentes raramente exploram um único vetor: a cadeia típica envolve a combinação de vulnerabilidades no meio de comunicação (WiFi, ZigBee, Bluetooth), no software de controle e no canal sensorial dos dispositivos. Essa natureza composta dos ataques contrasta com a abordagem fragmentada das defesas propostas na literatura. Sefati et al. (A03) propõem blockchain e aprendizado federado como soluções de grande elegância técnica, mas a proposta pressupõe infraestrutura computacional e capacidade de gestão que estão completamente fora do alcance do usuário residencial médio. Há aqui uma tensão não resolvida na literatura: as soluções tecnologicamente mais avançadas são, precisamente, as menos acessíveis para a população que mais necessita de proteção.

Al-Garadi et al. (A11) oferecem uma resposta parcial a essa tensão ao demonstrarem que algoritmos de machine learning embarcados, como redes neurais convolucionais leves (lightweight CNN), podem ser implementados diretamente nos dispositivos de borda (edge computing), reduzindo a dependência de infraestrutura centralizada e permitindo detecção de anomalias em tempo real mesmo em ambientes domésticos com conectividade limitada. Essa perspectiva é particularmente relevante para o Brasil, onde a desigualdade de acesso à internet de alta velocidade ainda é expressiva: segundo dados do IBGE (2022), aproximadamente 17 milhões de domicílios brasileiros não possuíam acesso à internet, e aqueles que possuem enfrentam conexões frequentemente instáveis. Soluções de segurança que dependem de conectividade contínua com servidores em nuvem são, portanto, intrinsecamente inadequadas para uma parcela significativa do território nacional.

3.3 CAMADA DE USUÁRIO: A ARMADILHA DA RESPONSABILIZAÇÃO INDIVIDUAL

A análise dos estudos A01, A04, A05 e A06 revela o que pode ser identificado como a principal contradição da literatura sobre segurança IoT doméstica: a tendência de transferir para

o usuário final a responsabilidade por vulnerabilidades que são, em sua origem, estruturais e sistêmicas. Oliveira et al. (A01) e Paz et al. (A06) documentam com precisão o baixo nível de conscientização dos usuários brasileiros sobre riscos digitais e práticas seguras. Szymoniak e Kubanek (A05) acrescentam a dimensão ética, argumentando que a governança de dados IoT deve partir de princípios de responsabilidade compartilhada. Tomados em conjunto, esses estudos sustentam um argumento educativo legítimo. O problema surge quando esse argumento é desconectado da análise estrutural: se dispositivos são vendidos sem segurança mínima por padrão, exigir que o usuário domine configurações técnicas complexas equivale a responsabilizá-lo por uma falha que não está em seu poder corrigir.

Walterscheid, Huijts e Van Sintemaartensdijk (A04) oferecem a contribuição mais original e analiticamente produtiva nessa camada ao demonstrarem, por meio de experimentos controlados, que a simples presença de rótulos de segurança no ponto de venda aumenta significativamente a probabilidade de o consumidor optar por dispositivos mais protegidos. Esse achado é relevante porque desloca o problema: em vez de exigir que o consumidor adquira conhecimento técnico especializado, o que é irrealista para a maioria da população, a rotulagem transfere a comunicação para o fabricante e para o regulador, que são os atores com capacidade real de produzir e atestar esse conhecimento. Trata-se, em síntese, de uma solução que opera no mercado sem depender da transformação cognitiva do usuário.

No entanto, a proposta de Walterscheid et al. (A04) apresenta uma limitação importante quando transportada para o contexto brasileiro: o estudo foi conduzido na Holanda, em um ambiente de alta literacia digital e com histórico robusto de regulação de consumo. No Brasil, a pesquisa de Paz et al. (A06) indica que os consumidores sequer reconhecem com clareza o que constitui um dispositivo IoT, o que sugere que a eficácia de rótulos de segurança dependeria de um trabalho educativo prévio que ainda está ausente. Essa contradição aponta para uma lacuna empírica relevante: não há estudos que tenham testado a eficácia de estratégias de rotulagem de segurança em populações brasileiras, o que representa uma oportunidade concreta para pesquisas futuras com impacto direto na formulação de políticas públicas.

3.4 SÍNTESE CRÍTICA: CONVERGÊNCIAS, LACUNAS E O CENÁRIO BRASILEIRO

A leitura transversal dos 12 estudos evidencia três convergências centrais que respondem às questões secundárias desta revisão. Em relação a QS1, todos os estudos que analisaram dispositivos reais identificaram as mesmas três categorias de vulnerabilidade: credenciais padrão

não alteradas, firmware desatualizado e protocolos de comunicação inseguros. Essa convergência, longe de ser trivial, é analiticamente significativa: indica que o problema não é de complexidade técnica, mas de incentivos econômicos. Os fabricantes sabem como produzir dispositivos seguros; optam por não fazê-lo porque o mercado não pune essa escolha.

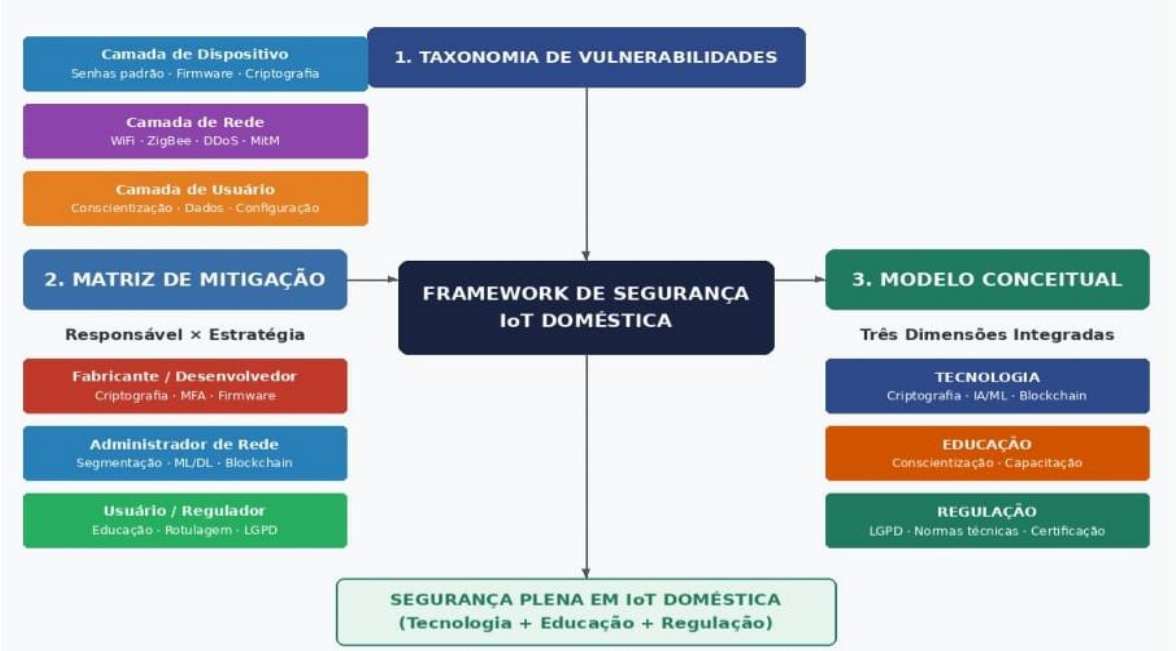
Em relação a QS2, a taxonomia de Heartfield et al. (A12) e o mapeamento de Al-Garadi et al. (A11) convergem ao demonstrar que os vetores de ataque mais explorados operam na combinação de vulnerabilidades de rede com falhas de software de controle. Isso contradiz a narrativa simplificadora de que proteger uma rede doméstica é questão de configurar o roteador corretamente: o escopo real dos ataques documentados cobre desde o protocolo ZigBee da lâmpada inteligente até o aplicativo de terceiros instalado no smartphone que controla a fechadura eletrônica. A superfície de ataque é sistêmica, e as defesas pontuais são, portanto, insuficientes.

Em relação a QS3, a principal lacuna identificada é a ausência de estudos que avaliem a eficácia das estratégias de mitigação em contextos de baixa renda e baixa literacia digital — justamente o perfil de grande parte dos novos usuários de IoT doméstica no Brasil. Os estudos internacionais propõem soluções sofisticadas (blockchain, federated learning, ML embarcado) sem problematizar o pressuposto de infraestrutura que sustentam. Os estudos brasileiros identificam corretamente o problema da baixa conscientização, mas não avançam em direção a intervenções testadas empiricamente. Essa dupla lacuna — soluções técnicas sem contexto e diagnósticos sem intervenção — define o espaço de contribuição original desta revisão e fundamenta o framework proposto na seção seguinte, que articula explicitamente responsabilidades distribuídas entre fabricantes, reguladores e usuários, reconhecendo as assimetrias estruturais do cenário nacional.

4. CONTRIBUIÇÃO: FRAMEWORK DE SEGURANÇA IoT DOMÉSTICA

Com base na síntese dos estudos analisados, esta revisão integrativa propõe um Framework de Segurança IoT Doméstica estruturado em três componentes complementares: (1) Taxonomia de Vulnerabilidades; (2) Matriz de Mitigação; e (3) Modelo Conceitual Integrado. Conforme apresentado na Figura 2, esses componentes articulam-se para oferecer uma estrutura prática e aplicável por fabricantes, desenvolvedores, reguladores e usuários finais.

Figura 2 – Framework de Segurança IoT Doméstica proposto.



Fonte: Elaborado pelos autores (2026), com base em Heartfield et al. (2018), Al-Garadi et al. (2020), Hassan et al. (2024) e Walterscheid et al. (2024).

4.1 TAXONOMIA DE VULNERABILIDADES

A Taxonomia de Vulnerabilidades organiza as falhas de segurança identificadas nos estudos em três camadas hierárquicas, expandindo e adaptando a classificação de Heartfield et al. (2018) para o contexto brasileiro. A Camada de Dispositivo abrange senhas padrão, firmware desatualizado, ausência de criptografia e configurações inseguras de fábrica (MOURA; NEVES, 2021; AL-GARADI et al., 2020). A Camada de Rede engloba protocolos de comunicação inseguros (WiFi, ZigBee, Bluetooth), ausência de segmentação de rede e vulnerabilidade a ataques man-in-the-middle, DDoS e replay (HEARTFIELD et al., 2018; SEFATI et al., 2024). A Camada de Usuário compreende baixa conscientização sobre práticas seguras, compartilhamento excessivo de dados e ausência de configuração adequada dos dispositivos (PAZ et al., 2023; OLIVEIRA et al., 2024).

4.2 MATRIZ DE MITIGAÇÃO

A Matriz de Mitigação cruza cada camada de vulnerabilidade com as estratégias recomendadas e os responsáveis pela implementação. Para a Camada de Dispositivo, as estratégias indicadas são autenticação multifatorial, criptografia TLS/DTLS e atualizações

automáticas de firmware, responsabilidade de fabricantes e desenvolvedores (HASSAN et al., 2024; TERTULINO DA SILVA; ANTUNES, 2023). Para a Camada de Rede, recomenda-se segmentação de rede, monitoramento contínuo por algoritmos de machine learning e blockchain para rastreabilidade, responsabilidade de desenvolvedores e administradores de rede (AL-GARADI et al., 2020; SEFATI et al., 2024; DELLA ROVERE; FLORIAN, 2022). Para a Camada de Usuário, destacam-se educação digital, rotulagem de segurança e conformidade com a LGPD, envolvendo fabricantes, órgãos reguladores e os próprios usuários (WALTERSCHEID; HUIJTS; VAN SINTEMAARTENSDIJK, 2024; PAZ et al., 2023).

4.3 MODELO CONCEITUAL INTEGRADO

O Modelo Conceitual Integrado evidencia que a segurança plena em ambientes IoT domésticos não pode ser alcançada por ações isoladas. Vulnerabilidades técnicas exigem respostas tecnológicas; vulnerabilidades comportamentais exigem respostas educativas; e a ausência de padrões exige respostas regulatórias (BOECKL et al., 2019; SZYMONIAK; KUBANEK, 2024). Heartfield et al. (2018) reforçam essa perspectiva ao demonstrar que os impactos dos ataques em casas inteligentes estendem-se às dimensões física, psicológica e emocional dos ocupantes, exigindo estratégias de proteção que considerem não apenas a segurança técnica, mas também o suporte humano às vítimas. A combinação das três dimensões, tecnologia, educação e regulação, constitui o núcleo do framework proposto.

5. CONSIDERAÇÕES FINAIS

A presente revisão integrativa da literatura investigou as principais vulnerabilidades em dispositivos IoT domésticos e as estratégias de mitigação propostas na literatura entre 2018 e 2024. A análise crítica dos 12 estudos selecionados evidenciou que as vulnerabilidades mais recorrentes, senhas padrão não alteradas, firmware desatualizado e protocolos de comunicação inseguros, não são falhas acidentais, mas consequências previsíveis de um modelo de mercado que não penaliza o design inseguro. A taxonomia de Heartfield et al. (2018) demonstrou que os vetores de ataque em casas inteligentes abrangem desde o protocolo ZigBee da lâmpada inteligente até a cadeia de suprimentos do firmware, com impactos que afetam a privacidade física, a segurança e o bem-estar psicológico dos ocupantes, dimensões ainda sistematicamente ausentes na literatura brasileira sobre o tema.

A principal contribuição original deste estudo é o Framework de Segurança IoT

Doméstica, que se diferencia dos trabalhos anteriores em três aspectos centrais. Primeiro, articula explicitamente responsabilidades distribuídas entre fabricantes, desenvolvedores e usuários, em vez de concentrar o ônus da proteção no usuário final, abordagem dominante na literatura brasileira identificada nesta revisão, mas analyticamente insustentável diante das assimetrias técnicas e informacionais do mercado.

Segundo, integra em um único modelo conceitual os três eixos de intervenção, tecnológico, educativo e regulatório, reconhecendo que ações isoladas em qualquer um desses eixos são insuficientes: criptografia sem educação do usuário não evita engenharia social; educação sem regulação não corrige o design inseguro dos fabricantes; regulação sem soluções técnicas acessíveis não alcança populações de baixa literacia digital.

Terceiro, o framework incorpora a dimensão emocional e comportamental dos impactos identificada por Heartfield et al. (2018), propondo suporte às vítimas como componente legítimo de qualquer estratégia de segurança doméstica, aspecto completamente ausente nos frameworks existentes na literatura nacional. Al-Garadi et al. (2020) fornecem a sustentação técnica da camada de rede do framework ao demonstrarem que algoritmos de machine learning embarcados em dispositivos de borda são viáveis para detecção de anomalias em tempo real mesmo em ambientes domésticos com conectividade limitada, condição prevalente em grande parte do território brasileiro.

Conclui-se que a segurança em ambientes IoT domésticos é um problema sistêmico que não pode ser resolvido por nenhum ator isoladamente. Do ponto de vista das aplicações práticas, o framework proposto oferece três contribuições imediatas: para fabricantes, uma taxonomia de vulnerabilidades que pode orientar processos de desenvolvimento seguro (security by design) alinhados às exigências regulatórias emergentes; para reguladores, uma matriz de mitigação que distribui responsabilidades de forma rastreável e auditável, subsidiando a formulação de requisitos técnicos mínimos para dispositivos IoT comercializados no Brasil; para usuários e educadores, um modelo conceitual que traduz a complexidade técnica da segurança IoT em três dimensões de ação compreensíveis e acionáveis.

Em relação à agenda de pesquisas futuras, três lacunas empíricas identificadas nesta revisão merecem prioridade: (1) testar a eficácia de estratégias de rotulagem de segurança em consumidores brasileiros, dada a evidência de Walterscheid et al. (2024) produzida em contexto europeu incompatível com o perfil nacional; (2) avaliar a implementação de algoritmos de ML embarcado em dispositivos de baixo custo prevalentes no mercado doméstico brasileiro,

verificando se a promessa técnica de Al-Garadi et al. (2020) se confirma em hardware restrito; e (3) conduzir estudos sobre o impacto emocional e comportamental de incidentes de segurança em moradores de residências inteligentes no Brasil, dimensão documentada por Heartfield et al. (2018) em contexto britânico e ainda completamente inexplorada na literatura nacional.

Por fim, reconhece-se que o corpus de 12 estudos, o recorte temporal de 2018 a 2024 e o caráter conceitual do framework, não submetido a validação empírica, constituem limitações desta revisão que devem ser consideradas na interpretação dos resultados e que definem, em si mesmas, parte da agenda de pesquisa aqui proposta.

REFERÊNCIAS

AL-GARADI, Mohammed Ali et al. A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys and Tutorials, v. 22, n. 3, p. 1646-1685, 2020. DOI: 10.1109/COMST.2020.2988293. Disponível em: https://ieeexplore.ieee.org/document/9023234.

BOECKL, Katie et al. Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks. Gaithersburg: NIST Interagency Report 8228, 2019. DOI: 10.6028/NIST.IR.8228. Disponível em: https://doi.org/10.6028/NIST.IR.8228

CARRION, Patrícia et al. Internet das Coisas (IoT): definições e aplicabilidade aos usuários finais. Human Factors in Design, v. 8, n. 15, p. 49-66, jan. 2019. DOI: 10.5965/2316796308152019049. Disponível em: https://revistas.udesc.br/index.php/hfd/article/view/14613

CHENG, Long; LIU, Fang; YAO, Danfeng. Enterprise data breach: causes, challenges, prevention, and future directions. WIREs Data Mining and Knowledge Discovery, v. 7, n. 5, e1211, 2017. DOI: 10.1002/widm.1211

DE JESUS JUNIOR, Airton A.; MORENO, Edward David. Segurança em infraestrutura para Internet das Coisas. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 33.,
2015, Vitória. Anais [...]. Vitória: SBC, 2015.

OLIVEIRA, Bruno Vieira et al. Desafios e soluções em segurança de IoT: conscientização e prevenção de ataques. Revista Contemporânea, v. 4, n. 5, e4235, 2024. DOI: 10.56083/RCV4N5-122. Disponível em: https://ojs.revistacontemporanea.com/ojs/index.php/home/article/view/4235

DE OLIVEIRA, N.; GOMES, M.; LOPES, R.; NOBRE, J. Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). Revista Eletrônica de Iniciação Científica em Computação, [S. l.], v. 17, n. 4, 2019. DOI: 10.5753/reic.2019.1704. Disponível em: https://journals-sol.sbc.org.br/index.php/reic/article/view/1704. Acesso em: 10 jun. 2026.

REZENDE, Mauricio Vianna; MARQUES, Rodrigo Moreno; PARREIRAS, Fernando Silva. Utilização de ontologias na avaliação de segurança cibernética na Internet das Coisas: uma revisão sistemática de literatura. Ciência da Informação, v. 50, n. 3, 2021. DOI: 10.18225/ci.inf.v50i3.5659

DELLA ROVERE, L.; FLORIAN, F. Estudo sobre segurança e privacidade na Internet das Coisas (IoT). RECIMA21 - Revista Científica Multidisciplinar, v. 3, n. 6, e361601, 2022. DOI: 10.47820/recima21.v3i6.1601. Disponível em: https://recima21.com.br/index.php/recima21/article/view/1601

ERCOLE, Flávia Falci; MELO, Laís Samara de; ALCOFORADO, Carla Lúcia Goulart Constant. Revisão integrativa versus revisão sistemática. REME – Revista Mineira de Enfermagem, v. 18, n. 1, p. 9-11, jan./mar. 2014. DOI: 10.5935/1415-2762.20140001. Disponível em: https://www.reme.org.br/artigo/detalhes/904

HASSAN, Yewande Goodness et al. Secure smart home IoT ecosystem for public safety and privacy protection. International Journal of Multidisciplinary Research and Growth Evaluation,
v. 5, n. 1, p. 1151-1157, 2024.

HEARTFIELD, Ryan et al. A taxonomy of cyber-physical threats and impact in the smart home. Computers & Security, v. 78, p. 398-428, 2018. DOI: 10.1016/j.cose.2018.07.011. IDC. The growth in connected IoT devices is expected to generate 79.4ZB of data in 2025. International Data Corporation, 2023. Disponível em:
https://www.idc.com/getdoc.jsp?containerId=prUS45213219

KADOW, André; CAMARGO, C. Internet das Coisas: vulnerabilidade, privacidade e pontos de segurança. Revista Competência, v. 9, n. 1, p. 153-161, 2016. Disponível em: https://seer.senacrs.com.br/index.php/RC/article/view/346

MOURA, Thiago Martiusi; NEVES, João Emmanuel D'Alkmin. Análise de segurança em dispositivos Internet das Coisas. Revista Interface Tecnológica, v. 18, n. 2, p. 15-27, 2021. DOI: 10.31510/infa.v18i2.1123

PAZ, Herlane Chaves et al. Internet das Coisas: a vulnerabilidade do consumidor no compartilhamento de dados. Revista de Tecnologia Aplicada, v. 12, n. 1, p. 68-85, 2023. DOI: 10.21714/2237-3713rta2023v12n1p68-85.

SANTAELLA, Lucia et al. Desvelando a Internet das Coisas. Revista GEMInIS, v. 4, n. 2, p. 19-32, 2013. Disponível em: https://www.revistageminis.ufscar.br/index.php/geminis/article/view/148

SANTOS, Cleide Maria da Rocha; PIMENTA, Cibele Andrucioli de Mattos; NOBRE, Moacyr Roberto Cuce. A estratégia PICO para a construção da pergunta de pesquisa e busca de evidências. Revista Latino-Americana de Enfermagem, v. 15, n. 3, p. 508-511, 2007. DOI: 10.1590/S0104-11692007000300023.

SANTOS, Paulo et al. Análise de riscos e segurança em IoT. Revista Brasileira de Computação Aplicada, v. 6, n. 1, p. 15-28, 2016. DOI: 10.5335/rbca.v6i1.3433.

SEFATI, Seyed Salar et al. Cybersecurity in a scalable smart city framework using blockchain and federated learning for Internet of Things (IoT). Smart Cities, v. 7, n. 5, p. 2802-2841, 2024. DOI: 10.3390/smartcities7050109.

SOUZA, Marcela Tavares de; SILVA, Michelly Dias da; CARVALHO, Rachel de. Revisão integrativa: o que é e como fazer. Einstein (São Paulo), v. 8, n. 1, p. 102-106, 2010. DOI: 10.1590/S1679-45082010RW1134. Disponível em: https://journal.einstein.br/article/integrative-review-what-is-it-how-to-do-it/

SZYMONIAK, Sabina; KUBANEK, Mariusz. Ethics in Internet of Things security: challenges and opportunities. In: FERRARI, Filippo; CARAMIAUX, Baptiste (Eds.). The Leading Role of Smart Ethics in the Digital World. Cham: Springer, 2024. p. 123-133. DOI: 10.1007/978-3-031-57851-6_9

TERTULINO DA SILVA, R. R.; ANTUNES, N. Security standards for low-end IoT devices: a comparative review. RECIMA21 – Revista Científica Multidisciplinar, v. 4, n. 1, e412437, 2023. DOI: 10.47820/recima21.v4i1.2437.

WALTERSCHEID, Michelle; HUIJTS, Nicole; VAN SINTEMAARTENSDIJK, Iris. Nudging purchase intention towards more secure domestic IoT: the effect of label features and psychological mechanisms. Computers in Human Behavior Reports, v. 14, p. 100386, 2024. DOI: 10.1016/j.chbr.2024.100386.

WHITTEMORE, Robin; KNAFL, Kathleen. The integrative review: updated methodology. Journal of Advanced Nursing, v. 52, n. 5, p. 546-553, dez. 2005. DOI: 10.1111/j.1365-2648.2005.03621.x.