Revista ft

www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 159, 2026 | DOI: 10.69849/n00pe748

Segurança em IoT de baixo custo: vulnerabilidades, matriz de riscos e diretrizes de hardening para sistemas embarcados

Low-cost IoT security: vulnerabilities, risk matrix and hardening guidelines for embedded systems

Gleibson da Silva Lima[1]
Paulino Wagner Palheta Viana[2]

Resumo. A expansão da Internet das Coisas (IoT) inseriu dispositivos embarcados de baixo custo em residências, indústrias, cidades inteligentes e infraestruturas críticas, mas também ampliou a superfície de ataque de sistemas com processamento, memória e energia limitados. Este artigo analisa vulnerabilidades recorrentes em dispositivos IoT de entrada e propõe diretrizes de proteção compatíveis com sistemas embarcados restritos. Metodologicamente, a pesquisa é qualitativa, exploratória e bibliográfica, apoiada em revisão de literatura sobre segurança embarcada, criptografia leve e incidentes de larga escala, além do mapeamento de normativas e guias técnicos como NISTIR 8259A, RFC 8576 e OWASP IoT Project. Como resultados, são sistematizados os vetores de ataque físicos e lógicos, uma matriz de riscos com impactos e controles compensatórios, e um conjunto de recomendações baseadas em security by design, com ênfase em identidade única, atualização segura, criptografia proporcional, raiz de confiança, hardening de serviços e governança do ciclo de vida. Conclui-se que a elevação da segurança em IoT de baixo custo não exige necessariamente a substituição integral do hardware, mas a adoção planejada de controles mínimos, verificáveis e adequados ao contexto de Engenharia da Computação.

Palavras-chave: Internet das Coisas. Cibersegurança. Sistemas Embarcados. Criptografia Leve. Vulnerabilidades. Security by Design.

Abstract. The expansion of the Internet of Things (IoT) has introduced low-cost embedded devices into homes, industries, smart cities and critical infrastructures, while also increasing the attack surface of systems constrained by processing power, memory and energy. This article analyzes recurrent vulnerabilities in entry-level IoT devices and proposes protection guidelines compatible with resource-constrained embedded systems. Methodologically, the research is qualitative, exploratory and bibliographic, based on a literature review about embedded security, lightweight cryptography and large-scale incidents, as well as on the mapping of technical standards and guidelines such as NISTIR 8259A, RFC 8576 and the OWASP IoT Project. As results, the study systematizes physical and logical attack vectors, a risk matrix with impacts and compensating controls, and recommendations based on security by design, emphasizing unique identity, secure updates, proportional cryptography, root of trust, service hardening and life-cycle governance. It concludes that improving security in

[1] Graduando do Curso de Engenharia da Computação da Faculdade FUCAPI.
[2] Orientador: Dr. Paulino Wagner Palheta Viana. Faculdade FUCAPI

low-cost IoT does not necessarily require complete hardware replacement, but rather the planned adoption of minimum, verifiable controls suitable for Computer Engineering practice.

Keywords: Internet of Things. Cybersecurity. Embedded Systems. Lightweight Cryptography. Vulnerabilities. Security by Design.

1. INTRODUÇÃO

A Internet das Coisas (IoT) consolidou-se como uma das bases técnicas da conectividade contemporânea, permitindo que sensores, atuadores, eletrodomésticos, medidores e equipamentos industriais passem a operar como nós computacionais capazes de coletar dados, comunicar eventos e executar ações automatizadas. A literatura clássica define esse ecossistema pela presença de objetos heterogêneos com endereçamento, conectividade e capacidade de cooperação entre si (ATZORI; IERA; MORABITO, 2010). Em perspectiva socioeconômica, essa conectividade desloca objetos antes analógicos para o centro de novos modelos de mercado e de serviços digitais (LARA; REIS; MOURA, 2021).

A popularização da IoT, entretanto, ocorreu de modo fortemente condicionado pelo custo. Para atingir escala comercial, fabricantes passaram a empregar microcontroladores e SoCs de entrada, frequentemente dotados de pouca memória, baixo clock, comunicação sem fio integrada e alimentação energética restrita. Esses recursos viabilizam produtos acessíveis, mas dificultam a aplicação direta de mecanismos tradicionais de proteção, como pilhas criptográficas densas, gestão robusta de memória e atualizações seguras complexas (RANA; MAMUN; ISLAM, 2022).

Essa tensão entre custo e proteção tornou-se crítica após incidentes como a botnet Mirai, que comprometeu câmeras IP e roteadores domésticos por meio de credenciais padrão e falhas de configuração, demonstrando que vulnerabilidades simples em dispositivos de massa podem ser exploradas em escala global (ANTONAKAKIS et al., 2017). Em dispositivos IoT, o comprometimento não ameaça apenas a confidencialidade da informação, mas pode afetar disponibilidade, privacidade, integridade operacional e até segurança física, especialmente quando equipamentos conectados interagem com ambientes reais.

O problema central investigado neste artigo pode ser sintetizado na seguinte pergunta: como proteger dispositivos IoT e sistemas embarcados de baixo custo contra vulnerabilidades físicas e lógicas recorrentes, conciliando controles de segurança com limitações severas de processamento, memória, energia e custo de fabricação? Para responder a essa questão, o estudo parte da análise da arquitetura típica desses dispositivos, classifica vulnerabilidades frequentes, estrutura uma matriz de riscos e propõe diretrizes práticas de hardening sob o paradigma de security by design.

O objetivo geral consiste em analisar as principais vulnerabilidades cibernéticas de dispositivos IoT de baixo custo e propor diretrizes de proteção adequadas à realidade dos sistemas embarcados. Como objetivos específicos, busca-se mapear a arquitetura e o ciclo de vida desses equipamentos; identificar falhas de segurança recorrentes; cruzar vetores de ataque com impactos e controles compensatórios; sintetizar recomendações de normativas internacionais; e oferecer um roteiro operacional aplicável à prática da Engenharia da Computação.

2. MÉTODOS

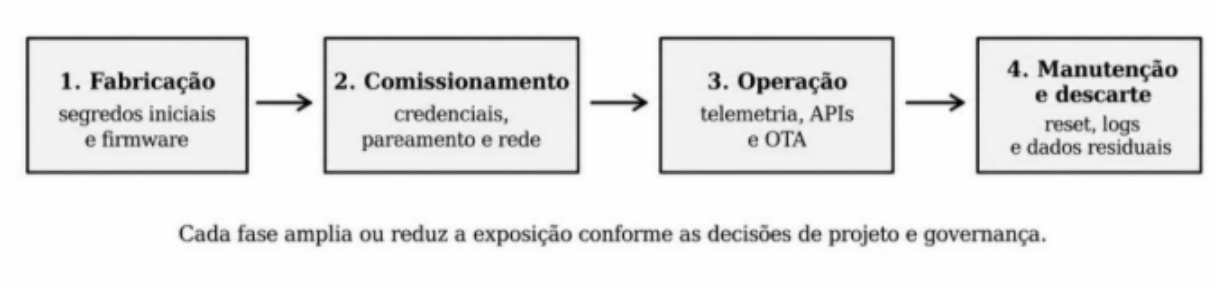
O estudo foi desenvolvido como pesquisa qualitativa, exploratória e bibliográfica, adequada à interpretação e organização crítica de fenômenos técnicos a partir de literatura científica e documentação normativa (LAKATOS; MARCONI, 2003; GIL, 2017). Não se buscou realizar ensaio laboratorial com placas físicas, mas consolidar conhecimento técnico disperso em um conjunto estruturado de diretrizes aplicáveis ao projeto de firmware e hardware embarcado.

A primeira etapa consistiu no levantamento de trabalhos relacionados à segurança em IoT, sistemas embarcados, criptografia leve, botnets e protocolos de comunicação. Foram priorizados estudos acadêmicos em bases como IEEE Xplore, ScienceDirect, Google Scholar e SciELO, com atenção a publicações que discutem restrições computacionais e energéticas em dispositivos de borda.

A segunda etapa envolveu análise documental de guias técnicos e normativos, especialmente o NISTIR 8259A, a RFC 8576 da IETF e o OWASP IoT Project. Esses documentos foram utilizados para extrair requisitos mínimos de segurança, categorias de vulnerabilidade, controles esperados e princípios de governança aplicáveis ao ciclo de vida de produtos conectados.

Na terceira etapa, os achados foram organizados em quatro produtos analíticos: mapeamento do ciclo de vida do dispositivo; identificação da superfície de ataque; matriz de vulnerabilidades, impactos e controles; e diretrizes de mitigação. A Figura 1 sintetiza o ciclo de vida observado, destacando que decisões inseguras tomadas na fabricação e no comissionamento tendem a permanecer ativas durante toda a operação do equipamento.

Figura 1 – Ciclo de vida de um dispositivo IoT de baixo custo e suas fases de exposição



Fonte: Elaborado pelo autor (2026).

3. REFERENCIAL TEÓRICO E TRABALHOS RELACIONADOS

A segurança da informação é tradicionalmente sustentada pela tríade confidencialidade, integridade e disponibilidade, mas, em sistemas ciberfísicos, esses princípios precisam ser expandidos para incluir autenticação, autorização, privacidade, resiliência de comunicação, segurança física e continuidade operacional (STALLINGS, 2023; KUROSE; ROSS, 2021). Em IoT, a falha de um nó não se limita ao dispositivo isolado: pode servir como ponto de entrada para redes maiores, compor botnets ou comprometer processos físicos.

O conceito de security by design recomenda que a proteção seja incorporada desde a concepção do produto, em vez de ser adicionada tardiamente após o firmware já estar funcional. Essa abordagem sustenta mecanismos como root of trust, secure boot, assinatura de firmware, identidade única, gestão segura de chaves, redução de serviços expostos e atualização segura (PAL et al., 2020; MEGAS; SCARFONE; SMITH, 2020).

No campo da criptografia, os estudos sobre Lightweight Cryptography (LWC) respondem ao desafio de proteger dispositivos com restrições de memória, clock e energia. Algoritmos leves e implementações otimizadas podem reduzir o custo computacional de operações criptográficas, embora sua eficácia dependa também da configuração correta de protocolos, chaves e autenticação de mensagens (HATZIVASILIS et al., 2016; DHANDA; SINGH; JINDAL, 2020; THAKOR; RAZZAQUE; KHANDAKER, 2021).

O OWASP IoT Project reúne vulnerabilidades recorrentes em produtos conectados, como senhas fracas ou universais, serviços inseguros, ausência de atualização segura, transmissão em texto claro e interfaces físicas expostas. Já a RFC 8576 destaca que a insegurança em IoT pode gerar efeitos em escala, pois dispositivos comprometidos podem ser utilizados contra terceiros, além de expor dados e energia do próprio usuário (GARCIA-MORCHON et al., 2019; OWASP FOUNDATION, [s. d.]).

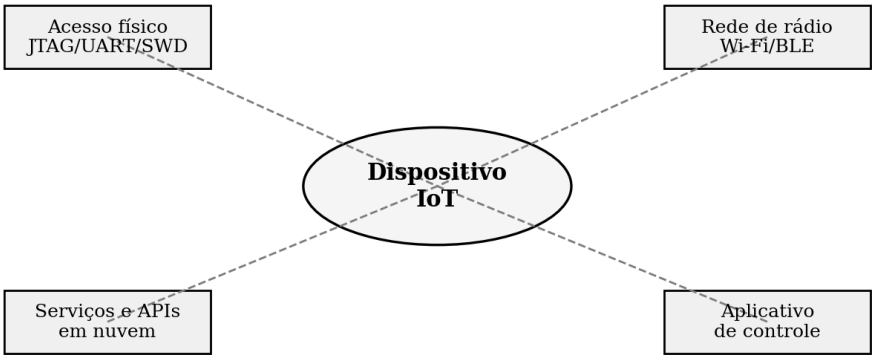
4. RESULTADOS

4.1 Arquitetura típica e superfície de ataque

Os dispositivos IoT de baixo custo costumam empregar microcontroladores ARM Cortex-M, RISC-V, ESP ou SoCs equivalentes, com memória flash reduzida, RAM limitada e arquitetura orientada a baixo consumo. A ausência de MMU e a execução sobre RTOS ou ambiente bare-metal reduzem o isolamento entre componentes, de modo que falhas em periféricos, pilhas de rede ou bibliotecas podem afetar diretamente a lógica principal do firmware.

A superfície de ataque não se limita ao acesso físico à placa. Ela inclui conectividade Wi-Fi, Bluetooth Low Energy, Zigbee ou protocolos semelhantes; APIs de nuvem; aplicativos móveis de controle; processos de provisionamento; interfaces de depuração; armazenamento local de segredos; e mecanismos OTA. A Figura 2 apresenta esse mapeamento de forma simplificada.

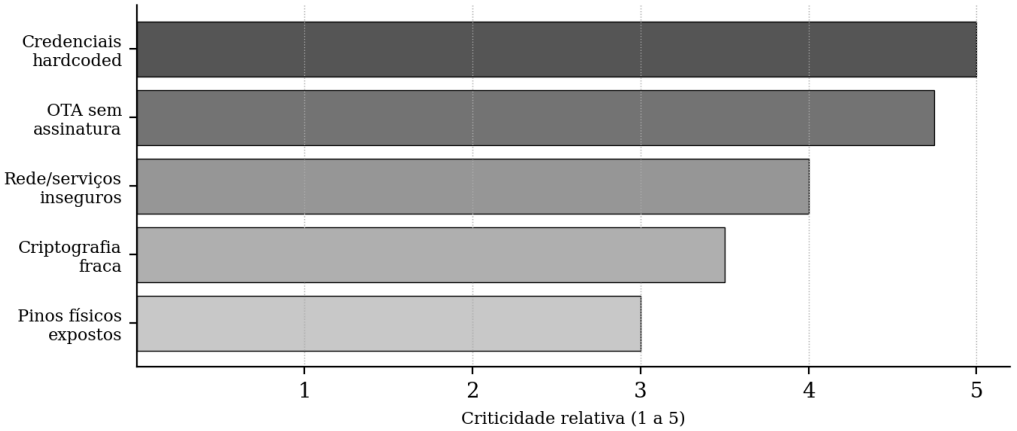
Figura 2 – Mapeamento da superfície de ataque em ecossistemas de sistemas embarcados conectados



Fonte: Elaborado pelo autor (2026).

Entre as fragilidades identificadas, destacam-se credenciais hardcoded, serviços de rede inseguros, atualizações sem assinatura digital, criptografia ausente ou fraca e exposição de pinos de depuração. O Gráfico 1 apresenta uma avaliação relativa de criticidade, considerando frequência de ocorrência, facilidade de exploração e impacto sistêmico reportado na literatura e em guias técnicos.

Gráfico 1 – Avaliação de criticidade relativa das principais categorias de vulnerabilidade do projeto OWASP IoT



Fonte: Elaborado pelo autor com base nas categorias do projeto OWASP IoT (2026).

4.2 Matriz de riscos

A consolidação dos vetores de ataque resultou na matriz apresentada no Quadro 1. O objetivo da matriz é conectar, de forma operacional, a vulnerabilidade observada, seu impacto provável e a ação de controle prioritária para equipes de desenvolvimento, qualidade e homologação.

Quadro 1 – Matriz de vulnerabilidades, impactos e controles compensatórios propostos

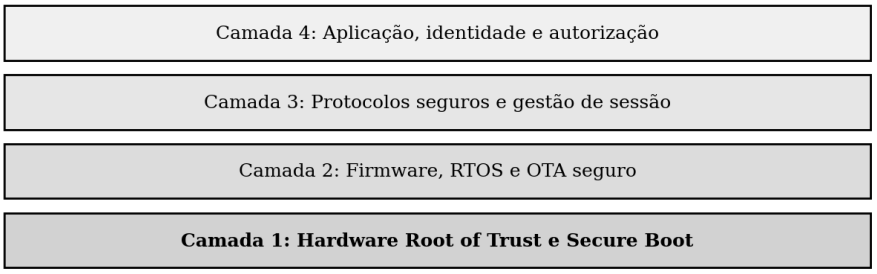
Vulnerabilidade	Impacto sistêmico	Controle compensatório
Senhas hardcoded e universais em lote	Tomada remota de dispositivos por botnets, fraude de provisionamento e violação de contas.	Credencial única por equipamento, troca obrigatória no primeiro uso e bloqueio de senhas fracas.
Transporte em texto claro ou criptografia insuficiente	Espionagem passiva, sequestro de sessão, extração de telemetria sensível e injeção de comandos.	Adoção de TLS/DTLS quando viável, chaves protegidas e primitivas compatíveis com o hardware.
OTA sem assinatura e sem verificação de integridade	Instalação de firmware malicioso, persistência do atacante e perda de recuperação confiável.	Secure boot, assinatura digital de imagens, partições A/B e política anti-rollback.
Interfaces físicas expostas (JTAG/UART/SWD)	Leitura de memória, engenharia reversa, extração de segredos e clonagem de dispositivos.	Desativação ou restrição das interfaces, proteção de leitura e controle físico no layout.
Dependências desatualizadas e sem inventário	Exploração de CVEs conhecidas e comprometimento da cadeia de suprimentos.	Gestão de versões, SBOM, rastreabilidade de bibliotecas e política formal de atualização.
Configuração padrão insegura e serviços desnecessários	Exposição de portas e APIs indevidas, ampliando a superfície de varredura remota.	Hardening de fábrica, princípio do menor privilégio e desativação de serviços não essenciais.

Fonte: Elaborado pelo autor (2026).

4.3 Diretrizes de proteção e mitigação

Os resultados indicam que a proteção viável para a IoT de baixo custo depende da composição de controles complementares, e não de uma única solução isolada. A defesa em profundidade precisa ser ajustada ao orçamento computacional do dispositivo, priorizando controles de alto impacto e baixo custo de execução. A Figura 3 sintetiza essa lógica em camadas.

Figura 3 – Arquitetura em camadas para proteção de dispositivos IoT



Defesa em profundidade: controles complementares reduzem o impacto de falhas isoladas.

Fonte: Elaborado pelo autor (2026).

A primeira diretriz é estabelecer uma raiz de confiança baseada em hardware ou em recursos imutáveis do chip. O bootloader deve validar a integridade e a procedência do firmware antes da execução, utilizando assinatura digital, hash autenticado ou cadeia de confiança proporcional ao dispositivo. Esse controle reduz a chance de execução persistente de firmware adulterado.

A segunda diretriz é adotar criptografia adaptativa e gerenciamento seguro de segredos. A escolha de primitivas deve considerar robustez, tempo de processamento, consumo energético e memória disponível. Quando o hardware não comportar pilhas densas, recomenda-se o uso de alternativas leves, armazenamento seguro de chaves, rotação planejada e eliminação de credenciais universais.

A terceira diretriz é garantir atualização e recuperação segura. Todo dispositivo conectado deve nascer com capacidade de receber firmware autenticado, verificar integridade antes da ativação, impedir rollback indevido e manter uma imagem confiável de recuperação. Sem atualização segura, vulnerabilidades descobertas após a venda tornam-se passivos permanentes.

A quarta diretriz é implantar governança de ciclo de vida e cadeia de suprimentos. Isso inclui inventário de componentes, SBOM, rastreabilidade de bibliotecas, política de

descontinuação, descarte seguro e documentação mínima para auditoria. A proteção, portanto, deve acompanhar o produto desde a fabricação até sua retirada de operação.

Quadro 2 – Mapeamento entre normativas e diretrizes propostas

Normativa/guia	Requisito ou princípio	Aplicação prática no projeto embarcado
NISTIR 8259A	Capacidade de atualização lógica segura	Partições A/B com validação criptográfica antes da ativação da nova imagem.
NISTIR 8259A	Identificação única e configuração segura	Provisionamento inicial com credencial exclusiva por unidade e redefinição controlada.
OWASP IoT Top 10	Eliminar senhas fixas previsíveis	Geração de segredo inicial aleatório ou derivado de identidade única em manufatura.
OWASP IoT Top 10	Mecanismo seguro de atualização	Assinatura digital de firmware, verificação de integridade e bloqueio de rollback.
OWASP IoT Top 10	Endurecimento físico	Desabilitação de JTAG/UART em campo e proteção de leitura da memória flash.
RFC 8576	Mitigação contra exaustão de recursos	Rate limiting, descarte precoce de pacotes inválidos e política de despertar controlado.
Cadeia de suprimentos	Inventário de componentes de software	Manutenção de SBOM para bibliotecas, drivers e dependências de terceiros.

Fonte: Elaborado pelo autor (2026).

4.4 Aplicação em cenário de referência

Para exemplificar a transposição das diretrizes, considere-se o projeto de um sensor ambiental residencial com conectividade Wi-Fi, aplicativo móvel e integração em nuvem. Em uma configuração insegura, esse sensor poderia sair de fábrica com senha idêntica em todo o lote, comunicação HTTP, provisionamento aberto, OTA sem assinatura e interface UART acessível no produto final. Embora tal desenho reduza o custo inicial, ele cria uma superfície de ataque incompatível com a escala de implantação.

Ao incorporar os requisitos derivados do NISTIR 8259A, do OWASP IoT Project e da RFC 8576, o mesmo equipamento passa a operar com identidade única, autenticação inicial controlada, comunicação protegida, limitação de taxa contra requisições abusivas, firmware assinado, logs mínimos e procedimento de reset seguro. A elevação de segurança ocorre sem exigir, necessariamente, a troca da plataforma de hardware, desde que a arquitetura seja planejada desde o início.

O produto aplicado deste estudo é um checklist de hardening a ser usado antes da liberação para teste de campo, homologação ou produção. O Quadro 3 resume os itens essenciais, reduzindo a matriz técnica a uma ferramenta de verificação rápida para equipes de firmware, testes, qualidade e integração.

Quadro 3 – Checklist sintético de hardening para IoT de baixo custo

Categoria	Item de verificação	Status
Identidade	Identificador único e segredo inicial não reutilizado em lote.	[ ] Sim [ ] Não [ ] Parcial
Credenciais	Troca de senha ou provisionamento seguro no primeiro uso.	[ ] Sim [ ] Não [ ] Parcial
Inicialização segura	Verificação de assinatura, hash ou cadeia de confiança antes da execução.	[ ] Sim [ ] Não [ ] Parcial
Atualização	OTA valida autenticidade, integridade e impede rollback indevido.	[ ] Sim [ ] Não [ ] Parcial
Criptografia	Canais de telemetria e comando protegidos conforme o hardware disponível.	[ ] Sim [ ] Não [ ] Parcial
Interfaces físicas	JTAG, UART ou SWD desabilitados, protegidos ou controlados.	[ ] Sim [ ] Não [ ] Parcial
SBOM	Inventário de bibliotecas, drivers e dependências com rastreabilidade.	[ ] Sim [ ] Não [ ] Parcial
Descomissionamento	Reset seguro remove chaves, dados e parâmetros sensíveis.	[ ] Sim [ ] Não [ ] Parcial

Fonte: Elaborado pelo autor (2026).

5. DISCUSSÃO

A análise demonstra que a insegurança em IoT de baixo custo decorre menos de uma impossibilidade técnica absoluta e mais de decisões de projeto orientadas por pressões comerciais, prazo curto e desconhecimento dos riscos. A limitação do chip é real, mas não justifica credenciais universais, serviços desnecessários expostos, ausência de assinatura em firmware ou falta de inventário de componentes.

É provável que a incorporação de controles mínimos aumente o esforço de desenvolvimento e exija maior qualificação das equipes. Ainda assim, os custos decorrentes da insegurança - perda reputacional, recall, violação de dados, exploração por botnets e interrupção de serviços - tendem a ser superiores ao investimento incremental em hardening. Em produtos de massa, pequenas negligências replicadas em milhares de unidades podem produzir efeitos sistêmicos.

Outro ponto relevante é que segurança em IoT não pode ser tratada apenas como atributo de firmware. Ela depende de arquitetura de hardware, decisões de manufatura, gestão de chaves, protocolos de rede, APIs de nuvem, aplicativo móvel, suporte pós-venda e descarte seguro. Portanto, a proteção de dispositivos embarcados conectados deve ser vista como disciplina interdisciplinar, envolvendo Engenharia da Computação, segurança da informação, qualidade, produto e conformidade regulatória.

6. CONCLUSÃO

Este artigo analisou vulnerabilidades recorrentes em dispositivos IoT de baixo custo e consolidou diretrizes de proteção adequadas à realidade de sistemas embarcados com recursos restritos. O estudo mostrou que falhas como credenciais hardcoded, canais sem criptografia, ausência de OTA seguro, exposição de interfaces físicas e dependências sem inventário continuam presentes porque frequentemente são toleradas como atalhos de desenvolvimento.

Os objetivos propostos foram alcançados ao mapear a arquitetura típica desses equipamentos, classificar sua superfície de ataque, estruturar uma matriz de riscos e traduzir recomendações de NIST, IETF e OWASP em controles aplicáveis. A principal contribuição reside na organização de um caminho pragmático: segurança por projeto, identidade única, raiz de confiança, criptografia proporcional, atualização verificável, hardening de serviços, SBOM e governança do ciclo de vida.

Conclui-se que a mitigação de vulnerabilidades em IoT de entrada não depende exclusivamente de hardware caro ou de soluções corporativas complexas. O ganho mais imediato está na adoção diligente de práticas mínimas, planejadas desde a concepção e verificadas antes da produção. Como trabalhos futuros, recomendam-se testes laboratoriais com placas reais, medição de consumo energético de primitivas leves, avaliação comparativa de estratégias OTA e análise de requisitos regulatórios emergentes para produtos conectados de consumo.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 10520: informação e documentação: citações em documentos: apresentação. Rio de Janeiro: ABNT, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14724: informação e documentação: trabalhos acadêmicos: apresentação. Rio de Janeiro: ABNT, 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023: informação e documentação: referências: elaboração. Rio de Janeiro: ABNT, 2018.

ANTONAKAKIS, Manos et al. Understanding the Mirai Botnet. In: USENIX SECURITY SYMPOSIUM, 26., 2017, Vancouver. Proceedings [...]. Berkeley: USENIX Association, 2017. p. 1093-1110.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The Internet of Things: a survey. Computer Networks, [s. l.], v. 54, n. 15, p. 2787-2805, 2010.

DHANDA, Sumit Singh; SINGH, Brahmjit; JINDAL, Poonam. Lightweight cryptography: a solution to secure IoT. Wireless Personal Communications, [s. l.], v. 112, n. 3, p. 1947-1980, 2020. DOI: https://doi.org/10.1007/s11277-020-07134-3.

GARCIA-MORCHON, Oscar et al. Internet of Things (IoT) Security: State of the Art and Challenges. RFC 8576. Fremont: RFC Editor, 2019. Disponível em: https://datatracker.ietf.org/doc/html/rfc8576. Acesso em: 20 abr. 2026.

GIL, Antonio Carlos. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2017.

HATZIVASILIS, George et al. A survey of lightweight stream ciphers for embedded systems. Security and Communication Networks, [s. l.], v. 9, n. 10, p. 1226-1246, 2016.

JING, Qi et al. Security of the Internet of Things: perspectives and challenges. Wireless Networks, [s. l.], v. 20, p. 2481-2501, 2014.

KUROSE, James F.; ROSS, Keith W. Computer networking: a top-down approach. 8. ed. Hoboken: Pearson, 2021.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 5. ed. São Paulo: Atlas, 2003.

LARA, Lívia; REIS, Luciano José; MOURA, Maria Aparecida. Admirável mundo novo na perspectiva da tríade: Internet das Coisas, pessoas e mercados. Perspectivas em Ciência da Informação, Belo Horizonte, v. 26, n. 2, 2021. Disponível em: https://www.scielo.br/j/pci/. Acesso em: 20 abr. 2026.

MEGAS, Katerina; SCARFONE, Karen; SMITH, Matthew. IoT Device Cybersecurity Capability Core Baseline. Gaithersburg: National Institute of Standards and Technology, 2020. (NISTIR 8259A). DOI: https://doi.org/10.6028/NIST.IR.8259A.

OWASP FOUNDATION. OWASP Internet of Things Project. [S. l.], [s. d.]. Disponível em: https://owasp.org/www-project-internet-of-things/. Acesso em: 20 abr. 2026.

PAL, Shantanu; HITCHENS, Michael; RABEHAJA, Tahiry; MUKHOPADHYAY, Subhas. Security requirements for the Internet of Things: a systematic approach. Sensors, Basel, v. 20, n. 20, art. 5897, 2020. DOI: https://doi.org/10.3390/s20205897.

RANA, Muhammad; MAMUN, Quazi; ISLAM, Rafiqul. Lightweight cryptography in IoT networks: a survey. Future Generation Computer Systems, [s. l.], v. 129, p. 77-89, 2022. DOI: https://doi.org/10.1016/j.future.2021.11.011.

SICARI, Sabrina et al. Security, privacy and trust in Internet of Things: the road ahead. Computer Networks, [s. l.], v. 76, p. 146-164, 2015.

STALLINGS, William. Cryptography and network security: principles and practice. 8. ed. Harlow: Pearson, 2023.

TANENBAUM, Andrew S.; WETHERALL, David J. Computer networks. 5. ed. Boston: Pearson, 2011.

THAKOR, Vishal A.; RAZZAQUE, M. A.; KHANDAKER, M. R. A. Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities. IEEE Access, [s. l.], v. 9, p. 28177-28193, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3052867.