SEGURANÇA NA INTERNET DAS COISAS (IoT): DESAFIOS, RISCOS E ESTRATÉGIAS DE MITIGAÇÃO

INTERNET OF THINGS (IOT) SECURITY: CHALLENGES, RISKS, AND MITIGATION STRATEGIES

SEGURIDAD EN EL INTERNET DE LAS COSAS (IOT): RETOS, RIESGOS Y ESTRATEGIAS DE MITIGACIÓN

Ygor Delfino da Silva
Mestrando em Redes Distribuídas
Universidade do Estado do Rio de Janeiro (UERJ)
https://orcid.org/0009-0005-9301-3613

Marco Antônio de Paula Dornel
Graduado em Sistemas de Informação
Instituto Federal do Espírito Santo (IFES)
https://orcid.org/0009-0004-8289-7284

Mauricio Lago Barros
Mestrando em Tecnologias Emergentes em Educação
Must University (MUST)
https://orcid.org/0009-0000-9231-5293

DOI: https://doi.org/10.46550/ilustracao.v7i9.795 Aceito em: 04.09.2026

Resumo: A Internet das Coisas (Internet of Things – IoT) refere-se ao ecossistema de objetos físicos conectados à internet, capazes de coletar, transmitir e processar dados de forma automatizada. Apesar de ampliar a eficiência e a inovação em áreas como saúde, indústria, segurança e cidades inteligentes, a IoT apresenta desafios significativos relacionados à segurança da informação, sobretudo devido à heterogeneidade de dispositivos, limitações computacionais, ausência de padrões consistentes e falhas recorrentes no firmware e na autenticação. Este artigo tem como objetivo discutir os principais riscos e vulnerabilidades presentes em ambientes IoT, além de apresentar estratégias técnicas e organizacionais de mitigação, incluindo boas práticas de governança, criptografia, autenticação robusta e monitoramento contínuo. Ademais, aborda-se a legislação aplicável no Brasil, com destaque para a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet, que impõem obrigações relativas à privacidade e à segurança no tratamento de dados pessoais. Conclui-se que a segurança em IoT demanda uma abordagem multidimensional, integrando tecnologia, conformidade legal e conscientização, sendo imprescindível para a confiabilidade e a continuidade dos serviços conectados.

Palavras-chave: Internet das Coisas. Segurança da informação. IoT. Vulnerabilidades. LGPD.

Abstract: The Internet of Things (IoT) refers to the ecosystem of physical objects connected to the internet that are capable of collecting, transmitting, and processing data automatically. Although it enhances efficiency and innovation in areas such as healthcare, industry, security, and smart cities, the IoT presents significant challenges related to information security, primarily due to the heterogeneity of devices, computational limitations, the absence of consistent standards, and recurring flaws in firmware and authentication. This article aims to discuss the main risks and vulnerabilities present in IoT environments, as well as to present technical and organizational mitigation strategies, including best practices for governance, encryption, robust authentication, and continuous monitoring. Furthermore, the article addresses the applicable legislation in Brazil, with an emphasis on the General Data Protection Law (LGPD) and the Brazilian Civil Rights Framework for the Internet, which impose obligations regarding privacy and security in the processing of personal data. It is concluded that IoT security requires a multidimensional approach, integrating technology, legal compliance, and awareness, and is essential for the reliability and continuity of connected services.

Keywords: Internet of Things. Information security. IoT. Vulnerabilities. LGPD.

Resumen: El Internet de las cosas (Internet of Things, IoT) hace referencia al ecosistema de objetos físicos conectados a Internet, capaces de recopilar, transmitir y procesar datos de forma automatizada. Aunque aumenta la eficiencia y la innovación en ámbitos como la sanidad, la industria, la seguridad y las ciudades inteligentes, el IoT plantea retos importantes relacionados con la seguridad de la información, sobre todo debido a la heterogeneidad de los dispositivos, las limitaciones informáticas, la ausencia de estándares coherentes y los fallos recurrentes en el firmware y la autenticación. El objetivo de este artículo es analizar los principales riesgos y vulnerabilidades presentes en los entornos de IoT, además de presentar estrategias técnicas y organizativas de mitigación, incluidas las buenas prácticas de gobernanza, cifrado, autenticación robusta y supervisión continua. Además, se aborda la legislación aplicable en Brasil, destacando la Ley General de Protección de Datos (LGPD) y el Marco Civil de Internet, que imponen obligaciones relativas a la privacidad y la seguridad en el tratamiento de datos personales. Se concluye que la seguridad en el IoT exige un enfoque multidimensional que integre tecnología, cumplimiento normativo y sensibilización, lo cual resulta imprescindible para la fiabilidad y la continuidad de los servicios conectados.

Palabras clave: Internet de las cosas. Seguridad de la información. IoT. Vulnerabilidades. LGPD.

1 Introdução

A Internet das Coisas (Internet of Things – IoT) constitui uma das principais transformações tecnológicas contemporâneas, caracterizada pela conexão de objetos físicos à internet com capacidade de sensoriamento, processamento e troca de informações. Esse paradigma tecnológico permite que equipamentos e sistemas coletem dados do ambiente, tomem decisões e se comuniquem automaticamente com outros dispositivos e plataformas, reduzindo a intervenção humana e potencializando a automação em larga escala.

Diante desse contexto, o artigo discute os principais desafios e riscos à segurança na IoT e apresenta soluções e boas práticas, considerando aspectos técnicos, operacionais e legais. O objetivo geral é analisar riscos e medidas de mitigação voltadas à segurança em IoT, considerando aspectos técnicos e normativos. Como objetivos específicos: a) conceituar IoT e sua arquitetura; b) identificar vulnerabilidades recorrentes; c) propor medidas e soluções; e d) apresentar legislação aplicável no Brasil.

O presente trabalho utiliza a metodologia de revisão bibliográfica, com abordagem qualitativa e caráter exploratório. Foram analisadas publicações acadêmicas, documentos de entidades técnicas e a legislação brasileira relacionados à segurança da informação e à proteção de dados em ambientes conectados.

2 Fundamentação teórica

2.1 Conceito de Internet das Coisas e a arquitetura em camadas

A IoT pode ser definida como um ecossistema composto por dispositivos físicos conectados à internet ou a redes privadas, capazes de se comunicar e executar ações com base em dados coletados por sensores. Esses dispositivos vão de equipamentos domésticos a sistemas industriais complexos. A essência da IoT reside na capacidade de integrar o mundo físico ao digital, criando ambientes inteligentes e automatizados.

A IoT normalmente é representada por uma arquitetura em camadas, sendo comuns as seguintes camadas: de percepção, de rede e de aplicação. Cada camada apresenta vulnerabilidades específicas: sensores podem ser adulterados fisicamente; redes podem sofrer ataques de interceptação; e aplicações podem apresentar falhas de autenticação e vazamentos de dados.

2.2 Segurança da informação aplicada à IoT

A segurança da informação tem como base o tripé CIA (Confidencialidade, Integridade e Disponibilidade). Em IoT, esses princípios ganham relevância ampliada: a) Confidencialidade: dados pessoais e operacionais devem ser protegidos contra acesso não autorizado; b) Integridade: leituras e comandos não podem ser adulterados sem detecção; e c) Disponibilidade: sistemas conectados devem permanecer operacionais, sobretudo em ambientes críticos. Entretanto, a aplicação desses princípios na IoT é dificultada por restrições de processamento, de memória e de energia em diversos dispositivos.

Além das vulnerabilidades técnicas, a segurança de IoT deve considerar fatores organizacionais. Dispositivos adquiridos sem critérios de segurança, instalados sem documentação ou mantidos sem responsável definido tendem a permanecer fora dos processos formais de gestão. Esse cenário dificulta a identificação de ativos, a atualização do *firmware* e a resposta a incidentes, aumentando a exposição ao longo de todo o ciclo de vida.

2.3 Perigos dos dispositivos IoT sem segurança adequada

A expansão da Internet das Coisas trouxe dispositivos conectados a ambientes residenciais, corporativos, industriais e públicos. Entretanto, a simples conexão à internet não significa que esses equipamentos possuam mecanismos de proteção suficientes. O NIST alerta que muitos dispositivos IoT, incluindo câmeras de segurança e sistemas de automação, podem possuir software sem correções, limitações de processamento e mecanismos de controle de acesso insuficientes. Em determinadas condições, um dispositivo vulnerável pode ser identificado e atacado pouco tempo após ser conectado à internet.

A gravidade decorre do fato de que o dispositivo comprometido pode deixar de ser apenas uma vítima e passar a funcionar como instrumento de novas ações maliciosas. Um equipamento vulnerável pode ser utilizado para acesso não autorizado, coleta de informações, comprometimento da privacidade ou integração a uma *botnet*. O problema, portanto, deixa de ser individual e adquire caráter sistêmico.

2.4 Câmeras, webcams e o risco de espionagem nas webcams e interfaces web expostas

Câmeras e webcams conectadas constituem um dos exemplos mais sensíveis de dispositivos IoT, pois combinam conectividade, captação de imagens e, em determinados equipamentos, áudio e mecanismos de controle remoto. Quando uma câmera apresenta autenticação fraca, interface web insegura, firmware vulnerável ou configuração inadequada, há risco de acesso não autorizado. A consequência pode ir além da indisponibilidade do equipamento, comprometendo diretamente a privacidade das pessoas captadas pelo dispositivo.

O risco de espionagem também precisa ser analisado sob a perspectiva da proteção de dados. Quando as imagens ou informações captadas permitem identificar pessoas, o tratamento pode envolver dados pessoais, o que torna a segurança do dispositivo parte integrante da governança de privacidade.

Outro problema relevante diz respeito à exposição das interfaces administrativas dos dispositivos. Muitos equipamentos IoT possuem uma interface web para configuração, monitoramento ou gerenciamento remoto. Quando essa interface é disponibilizada diretamente na internet sem mecanismos adequados de autenticação, autorização e proteção, torna-se uma superfície de ataque.

Uma “webcam sem proteção” pode estar exposta devido a credenciais fracas, serviços desnecessários, firmware vulnerável, interfaces administrativas expostas, ausência de criptografia, falhas de autorização ou falta de atualizações.

2.5 Dispositivos IoT como componentes de botnets e DDoS e o efeito coletivo da insegurança

Um dos perigos mais relevantes da IoT é a utilização de dispositivos comprometidos para formação de botnets. Uma botnet pode ser entendida como um conjunto de dispositivos comprometidos que passam a ser controlados remotamente por um atacante. No contexto da IoT, câmeras, roteadores, DVRs e outros equipamentos podem ser incorporados a essas redes quando apresentam vulnerabilidades exploráveis.

O NIST reconhece expressamente esse cenário e afirma que vulnerabilidades em dispositivos IoT podem permitir que atacantes controlem conjuntos de equipamentos para realizar ataques distribuídos de negação de serviço. O documento utiliza a Mirai como exemplo de botnet baseada em dispositivos IoT comprometidos.

Os ataques de *Distributed Denial of Service* (DDoS) constituem uma consequência importante da exploração de dispositivos IoT. Em termos gerais, o objetivo de um ataque DDoS é utilizar uma grande quantidade de tráfego ou de requisições para comprometer a disponibilidade de um determinado serviço. Quando dispositivos IoT vulneráveis são agrupados em uma botnet, milhares ou até milhões de equipamentos podem participar simultaneamente da geração desse tráfego.

O NIST possui uma publicação específica sobre mitigação de DDoS baseada em IoT e destaca que mecanismos de segurança de rede podem aumentar significativamente o esforço necessário para comprometer dispositivos e reduzir a utilidade desses dispositivos para agentes maliciosos. Entre os mecanismos considerados estão gateways, controles de rede, servidores de atualização e *Manufacturer Usage Description* (MUD).

2.6 Espionagem, privacidade, coleta indevida de dados e risco para redes corporativas

Além da participação em botnets, dispositivos IoT podem representar riscos relacionados à coleta e à utilização indevidas de informações. Câmeras, microfones, sensores, dispositivos vestíveis e sistemas de automação podem coletar informações sobre comportamento, localização, presença, rotina e preferências. Consequentemente, a segurança deve acompanhar todo o fluxo de informação: coleta → transmissão → processamento → armazenamento → compartilhamento → descarte.

O comprometimento de um dispositivo IoT também pode representar um risco para toda a rede corporativa. Quando equipamentos IoT são instalados em redes sem segmentação adequada, um dispositivo comprometido pode servir de ponto de apoio para novas tentativas de acesso.

2.7 Dispositivos sem atualização: consequências para pessoas e organizações

Outro problema crítico é a permanência de equipamentos conectados após o término do suporte do fabricante. Um dispositivo pode ter sido considerado seguro no momento da aquisição e, posteriormente, tornar-se vulnerável devido à descoberta de novas falhas.

A OWASP identifica a ausência de mecanismos seguros de atualização e de gerenciamento do dispositivo entre os principais riscos da IoT. “Por quanto tempo esse equipamento receberá atualizações de segurança?” Essa pergunta deveria fazer parte dos processos de aquisição de qualquer organização que utilize IoT.

O comprometimento de um dispositivo IoT pode gerar impactos que vão além do equipamento afetado, alcançando usuários, organizações, redes corporativas e terceiros. Os principais impactos envolvem privacidade, segurança da informação, disponibilidade, perdas financeiras, reputação e questões jurídicas relacionadas ao tratamento de dados.

A privacidade é especialmente afetada quando câmeras, microfones e sensores capturam informações de pessoas. Na dimensão da segurança da informação, o comprometimento pode permitir acesso indevido a serviços, credenciais ou recursos da infraestrutura. Em relação à disponibilidade, dispositivos comprometidos podem participar de botnets destinadas a ataques DDoS. Também podem ocorrer custos associados à recuperação de sistemas, à substituição de equipamentos e à investigação de incidentes.

No aspecto reputacional e jurídico, incidentes podem comprometer a confiança dos usuários e exigir investigação, medidas corretivas e avaliação das responsabilidades aplicáveis. A avaliação de risco deve, portanto, considerar a relação entre dispositivo, dados, redes, pessoas e processos.

2.8 Como reduzir esses perigos e síntese dos perigos

A solução não consiste em simplesmente impedir o uso da IoT. O caminho adequado é estabelecer segurança desde a concepção e ao longo de todo o ciclo de vida. Entre as principais medidas estão inventário, substituição de credenciais padrão, autenticação forte, atualização de firmware, desativação de serviços desnecessários, proteção das interfaces administrativas, criptografia, segmentação, monitoramento, registros, resposta a incidentes e retirada de equipamentos sem suporte.

Os perigos associados a dispositivos IoT sem segurança adequada demonstram que conectividade e segurança precisam caminhar juntas. A segurança da IoT deve ser compreendida como uma responsabilidade compartilhada entre fabricantes, fornecedores, integradores, organizações e usuários. A vulnerabilidade de um único equipamento pode exceder seus limites físicos e acarretar consequências para outras pessoas, organizações e serviços.

3 Soluções e boas práticas de segurança em IoT

A segurança da Internet das Coisas deve ser estruturada com base em uma abordagem de defesa em profundidade, considerando que nenhum mecanismo isolado é capaz de eliminar todos os riscos associados aos dispositivos conectados. A proteção deve abranger desde a seleção e aquisição do equipamento até sua implantação, operação, atualização, monitoramento e descomissionamento.

Nesse contexto, boas práticas devem combinar controles técnicos, administrativos e organizacionais capazes de reduzir a exploração e limitar os impactos. Referenciais como o OWASP IoT Top 10, o NIST *Cybersecurity Framework* e as publicações específicas do NIST para dispositivos IoT fornecem bases importantes para a identificação de riscos, a definição de controles, o gerenciamento de vulnerabilidades e a resposta a incidentes (OWASP FOUNDATION, 2018; NIST, 2018).

3.1 Boas práticas e padrões técnicos

A adoção de padrões técnicos constitui uma das principais estratégias para organizar a segurança dos ambientes IoT. O OWASP IoT Top 10 apresenta categorias de riscos recorrentes, como senhas fracas, serviços de rede inseguros, interfaces inseguras, ausência de mecanismos seguros de atualização, componentes vulneráveis, proteção insuficiente da privacidade e configurações inseguras (OWASP FOUNDATION, 2018). Assim, a organização deve transformar a segurança em requisitos verificáveis, estabelecendo as capacidades exigidas antes da aquisição e da conexão do dispositivo.

3.2 Criptografia e proteção de dados

Na comunicação entre dispositivos, servidores, aplicações e serviços de nuvem, recomenda-se o uso de mecanismos criptográficos adequados, como TLS (*Transport Layer Security*), certificados digitais e, quando aplicável, autenticação baseada em certificados.

A criptografia deve ser acompanhada de gerenciamento de chaves, controle de acesso, armazenamento seguro e gestão do ciclo de vida das credenciais. Quando dispositivos IoT tratam dados pessoais, a proteção criptográfica deve ser integrada às demais medidas técnicas e administrativas previstas na legislação de proteção de dados.

3.3 Autenticação forte e controle de acesso

A autenticação constitui uma das primeiras barreiras contra o acesso não autorizado aos dispositivos IoT. Equipamentos que permanecem com credenciais padrão de fábrica, senhas fracas ou mecanismos de autenticação inadequados apresentam elevado risco de comprometimento. Uma medida básica consiste em substituir imediatamente as credenciais

padrão durante a implantação. Também devem ser utilizados senhas fortes, individualizadas e, quando tecnicamente possível, mecanismos de autenticação multifator.

Nesse sentido, deve ser aplicado o princípio do menor privilégio, segundo o qual usuários, dispositivos e aplicações devem possuir apenas as permissões necessárias para desempenhar suas funções. Esse modelo reduz o impacto de um eventual comprometimento ao limitar as permissões disponíveis ao atacante. Identidades individuais também ampliam a rastreabilidade, facilitando a auditoria e a resposta a incidentes.

3.4 Segmentação de rede e Zero Trust

A segmentação de rede constitui uma importante medida de contenção de incidentes em ambientes IoT. Dispositivos conectados não devem, como regra geral, ter acesso irrestrito aos demais componentes da infraestrutura.

A segmentação permite separar dispositivos IoT de servidores, de estações de trabalho, de sistemas administrativos e de outros ativos críticos. Conforme o ambiente, podem ser utilizadas VLANs, firewalls, ACLs, redes específicas para IoT, gateways, controles de comunicação, políticas de filtragem e microsegmentação.

Nesse modelo, cada tentativa de acesso deve ser avaliada com base na identidade, no dispositivo, no recurso, no contexto e na política de segurança. Dessa forma, mesmo que um equipamento IoT seja comprometido, sua capacidade de alcançar outros ativos pode ficar significativamente limitada.

3.5 Monitoramento e resposta a incidentes

A prevenção não elimina a possibilidade de comprometimento. Por isso, os ambientes IoT precisam dispor de mecanismos de detecção, monitoramento e resposta a incidentes. O monitoramento permite identificar comportamentos anômalos, como aumento inesperado do tráfego, tentativas repetidas de autenticação, comunicação com destinos desconhecidos e alterações não autorizadas na configuração ou no *firmware*. A resposta deve prever o isolamento do dispositivo, a preservação de evidências, a análise, a comunicação, a correção e o retorno controlado à operação.

3.6 Governança, ciclo de vida e gestão de fornecedores

A segurança de IoT deve integrar a aquisição, a implantação, a operação, a atualização e o descomissionamento. A escolha de um dispositivo não deve considerar apenas o preço, a funcionalidade ou a capacidade de conectividade.

Antes da contratação, devem ser avaliados o período de suporte, a política de atualização de firmware, os mecanismos de atualização segura, o gerenciamento de credenciais, a autenticação,

a criptografia, a documentação, a gestão de vulnerabilidades, a comunicação de incidentes, as dependências na nuvem, a proteção de dados e o procedimento de encerramento. Portanto, a segurança não deve terminar no momento em que o dispositivo é instalado.

Ela deve acompanhar todo o ciclo: aquisição → implantação → configuração → operação → monitoramento → atualização → manutenção → descomissionamento.

3.7 Atualização segura e gestão de vulnerabilidades

A capacidade de atualização é um requisito essencial para dispositivos IoT. Vulnerabilidades podem ser descobertas depois que o equipamento já está instalado, o que torna necessário um mecanismo confiável para a distribuição e a instalação de correções.

Entretanto, não basta permitir qualquer atualização. O processo deve garantir a autenticidade e a integridade do firmware, evitando que um atacante substitua o software legítimo por código malicioso. A organização deve manter controle das versões instaladas, das datas de atualização e dos dispositivos que não receberam determinada correção.

O processo de gestão de vulnerabilidades deve identificar os dispositivos afetados, verificar as versões de firmware, avaliar a criticidade, obter as correções, testar, implantar, validar e registrar as atualizações. Quando determinado equipamento deixa de receber suporte, deve-se avaliar a substituição ou a retirada da rede.

3.8 Segurança física, Security by Design e integração dos controles

A segurança física deve acompanhar os controles lógicos em dispositivos instalados em locais públicos, industriais ou técnicos. Da mesma forma, o princípio de Security by Design exige que identidade, autenticação, criptografia, atualização, privacidade e monitoramento sejam considerados desde o desenvolvimento e a aquisição. A integração desses controles produz uma defesa em profundidade capaz de limitar o impacto quando um mecanismo isolado falhar.

4 Legislação aplicável à IoT no Brasil

Em ambientes IoT, também devem ser observados os princípios da necessidade e da transparência, evitando a coleta excessiva e assegurando informações adequadas sobre a finalidade e o tratamento dos dados.

4.1 Lei Geral de Proteção de Dados (LGPD)

A LGPD (Lei nº 13.709/2018) estabelece regras para a coleta e o tratamento de dados pessoais. Em IoT, dados de geolocalização, hábitos de consumo e informações biométricas podem ser classificados como pessoais e até sensíveis, o que exige rigor jurídico. A legislação prevê princípios como finalidade, adequação, necessidade e segurança. (BRASIL, 2018).

4.2 Marco Civil da Internet

O Marco Civil assegura direitos e deveres no uso da internet, reforçando a importância da privacidade e da proteção de registros. (BRASIL, 2014). A responsabilização também exige considerar a capacidade de demonstrar que os controles foram efetivamente implementados. Políticas documentadas, inventário de ativos, registros de atualização, avaliações de risco e evidências de monitoramento contribuem para demonstrar a adoção de medidas de segurança e para identificar lacunas de proteção. Em ambientes sujeitos à LGPD, essa documentação também auxilia na governança e na prestação de contas do tratamento de dados pessoais.

4.3 Responsabilização e dever de segurança

A responsabilização deve ser analisada conforme o contexto, considerando as obrigações legais aplicáveis, os controles adotados, a natureza dos dados tratados e as consequências de eventual incidente. A segurança deve, portanto, fazer parte dos processos de governança da organização e não ser tratada apenas após a ocorrência de falhas.

A adoção de mecanismos como inventário de ativos, avaliação de riscos, gestão de vulnerabilidades, controle de acesso, registros de eventos, políticas de atualização e planos de resposta contribui para reduzir a exposição dos dispositivos e para demonstrar a adoção de medidas de segurança compatíveis com o ambiente.

Além da implementação dos controles, é importante manter a documentação e as evidências de sua aplicação. Políticas internas, registros de atualização, avaliações de risco, relatórios de monitoramento e procedimentos de resposta a incidentes podem auxiliar na identificação de lacunas de proteção e na demonstração das medidas adotadas, especialmente em ambientes sujeitos à legislação de proteção de dados.

5 Resultados e discussão

A principal contribuição do estudo é reforçar que a segurança não deve ser tratada como uma característica isolada do dispositivo, mas como um requisito de arquitetura, aquisição, governança e operação. Os resultados também mostram que os controles são interdependentes: autenticação reduz acessos indevidos, segmentação limita a movimentação lateral, atualização reduz vulnerabilidades e monitoramento amplia a capacidade de detecção.

Assim, NIST e OWASP convergem quanto à necessidade de controles ao longo de todo o ciclo de vida, enquanto a LGPD acrescenta requisitos de segurança e privacidade desde a concepção. *Frameworks* gerais precisam, portanto, ser complementados por requisitos específicos para IoT. A análise demonstra que a segurança de IoT é um problema de ecossistema. Interfaces, APIs, serviços de nuvem, mecanismos de atualização e redes integram a cadeia de risco.

Considerações finais

A Internet das Coisas amplia a automação e a integração entre o mundo físico e o digital, proporcionando ganhos de eficiência em diferentes setores. Entretanto, a expansão da conectividade também amplia a superfície de ataque e intensifica os desafios relacionados à segurança da informação, à privacidade e à continuidade dos serviços.

Os resultados da análise demonstram que vulnerabilidades como credenciais fracas, interfaces inseguras, firmware desatualizado e falhas de configuração podem comprometer não apenas o dispositivo, mas também as redes, os sistemas e os dados associados. Câmeras, webcams e outros dispositivos conectados exigem atenção especial, pois podem representar riscos à privacidade, acesso não autorizado, a formação de botnets e a participação em ataques distribuídos de negação de serviço.

A mitigação desses riscos depende da combinação de diferentes controles de segurança, incluindo autenticação forte, criptografia, atualização segura, segmentação de redes, monitoramento, gestão de vulnerabilidades e governança. Nenhuma dessas medidas, isoladamente, é suficiente para eliminar completamente os riscos existentes em ambientes IoT. A proteção deve acompanhar todo o ciclo de vida do dispositivo, desde a aquisição e configuração até a atualização, manutenção e descomissionamento.

No contexto brasileiro, a Lei Geral de Proteção de Dados Pessoais reforça a necessidade de adoção de medidas técnicas e administrativas de segurança e aproxima os conceitos de proteção de dados, de segurança da informação e de governança. Dessa forma, a segurança deve ser considerada desde a concepção dos produtos e serviços que realizam tratamento de dados pessoais.

Conclui-se que a segurança da Internet das Coisas deve ser tratada como um processo contínuo e uma responsabilidade compartilhada entre fabricantes, fornecedores, organizações, profissionais de tecnologia e usuários. A utilização segura de dispositivos conectados depende da integração entre tecnologia, processos, pessoas, governança e requisitos legais.

Como possibilidade para pesquisas futuras, recomenda-se o aprofundamento de estudos de caso em ambientes corporativos, industriais e de infraestrutura crítica, bem como a realização de avaliações experimentais de mecanismos de autenticação, atualização, segmentação, monitoramento e resposta a incidentes aplicados a diferentes categorias de dispositivos IoT.

Referências

OWASP FOUNDATION. **OWASP Internet of Things Top 10**. [S. l.]: OWASP Foundation, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Foundational Cybersecurity Activities for IoT Product Manufacturers**. Gaithersburg, MD: NIST, 2026. (NISTIR 8259 Rev. 1).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **IoT Device Cybersecurity Capability Core Baseline**. Gaithersburg, MD: NIST, 2020. (NISTIR 8259A).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for Improving Critical Infrastructure Cybersecurity**. Gaithersburg, MD: NIST, 2018.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet**. Diário Oficial da União: Brasília, DF, 24 abr. 2014. (BRASIL, 2014).

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: Brasília, DF, 15 ago. 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001**: **Information security management systems**. Geneva: ISO, 2022.