Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i3.25283

# SEGURANÇA DA INFORMAÇÃO EM AMBIENTES DE INTERNET DAS COISAS (IOT): DESAFIOS, VULNERABILIDADES E ESTRATÉGIAS DE PROTEÇÃO

## INFORMATION SECURITY IN INTERNET OF THINGS (IoT) ENVIRONMENTS: CHALLENGES, VULNERABILITIES AND PROTECTION STRATEGIES

## SEGURIDAD DE LA INFORMACIÓN EN ENTORNOS DE INTERNET DE LAS COSAS (IoT): DESAFÍOS, VULNERABILIDADES Y ESTRATEGIAS DE PROTECCIÓN

**Bruno Soares Lopes**[1]

RESUMO: A Internet das Coisas (IoT) tem promovido avanços significativos na conectividade entre dispositivos e sistemas digitais, permitindo a automação de processos e a geração de grandes volumes de dados em diferentes áreas, como indústria, saúde, transporte e ambientes domésticos. Entretanto, o crescimento acelerado dessa tecnologia também tem ampliado os desafios relacionados à segurança da informação, uma vez que muitos dispositivos conectados apresentam vulnerabilidades que podem ser exploradas por ataques cibernéticos. Nesse contexto, o presente estudo tem como objetivo analisar os principais desafios, vulnerabilidades e estratégias de proteção relacionados à segurança da informação em ambientes de Internet das Coisas. A metodologia adotada baseia-se em uma revisão de literatura, realizada a partir da análise de livros, artigos científicos e trabalhos acadêmicos que abordam o tema da segurança em IoT. Os resultados evidenciam que falhas de autenticação, ausência de atualizações de segurança, uso inadequado de criptografia e limitações de hardware são fatores que contribuem para o aumento das vulnerabilidades nesses sistemas. Além disso, ataques cibernéticos podem comprometer a integridade, a confidencialidade e a disponibilidade das informações transmitidas em redes IoT. O estudo também destaca a importância da proteção de dados e da privacidade dos usuários, bem como a necessidade de desenvolvimento de novas abordagens de segurança capazes de lidar com as características específicas desses ambientes. Conclui-se que a implementação de mecanismos eficazes de segurança, aliada à adoção de boas práticas de gestão de riscos e ao desenvolvimento de tecnologias emergentes, é fundamental para garantir a utilização segura e confiável das aplicações baseadas em Internet das Coisas.

**Palavras-chave:** Internet das Coisas. Segurança da informação. Vulnerabilidades em IoT. Cibersegurança. Proteção de dados.

[1]Bacharel em Ciência da Computação, Universidade Veiga de Almeida (UVA)

ABSTRACT: The Internet of Things (IoT) has significantly advanced connectivity between devices and digital systems, enabling process automation and the generation of large volumes of data in various sectors such as industry, healthcare, transportation, and smart homes. However, the rapid growth of this technology has also increased challenges related to information security, since many connected devices present vulnerabilities that can be exploited by cyberattacks. In this context, this study aims to analyze the main challenges, vulnerabilities, and protection strategies related to information security in Internet of Things environments. The methodology adopted is based on a literature review, conducted through the analysis of books, scientific articles, and academic works addressing IoT security. The results indicate that authentication failures, lack of security updates, inadequate use of encryption, and hardware limitations are factors that contribute to increasing vulnerabilities in these systems. In addition, cyberattacks can compromise the integrity, confidentiality, and availability of information transmitted across IoT networks. The study also highlights the importance of data protection and user privacy, as well as the need to develop new security approaches capable of addressing the specific characteristics of IoT environments. It is concluded that the implementation of effective security mechanisms, combined with the adoption of risk management practices and the development of emerging technologies, is essential to ensure the safe and reliable use of Internet of Things applications.

**Keywords:** Internet of Things. Information security. IoT vulnerabilities. Cybersecurity. Data protection.

RESUMEN: La Internet de las Cosas (IoT) ha promovido avances significativos en la conectividad entre dispositivos y sistemas digitales, permitiendo la automatización de procesos y la generación de grandes volúmenes de datos en diferentes sectores, como la industria, la salud, el transporte y los entornos domésticos. Sin embargo, el crecimiento acelerado de esta tecnología también ha ampliado los desafíos relacionados con la seguridad de la información, ya que muchos dispositivos conectados presentan vulnerabilidades que pueden ser explotadas mediante ataques cibernéticos. En este contexto, el presente estudio tiene como objetivo analizar los principales desafíos, vulnerabilidades y estrategias de protección relacionadas con la seguridad de la información en entornos de Internet de las Cosas. La metodología adoptada se basa en una revisión de la literatura, realizada a partir del análisis de libros, artículos científicos y trabajos académicos que abordan el tema de la seguridad en IoT. Los resultados evidencian que las fallas de autenticación, la ausencia de actualizaciones de seguridad, el uso inadecuado de la criptografía y las limitaciones de hardware son factores que contribuyen al aumento de vulnerabilidades en estos sistemas. Además, los ataques cibernéticos pueden comprometer la integridad, la confidencialidad y la disponibilidad de la información transmitida en redes IoT. El estudio también destaca la importancia de la protección de datos y de la privacidad de los usuarios, así como la necesidad de desarrollar nuevos enfoques de seguridad capaces de enfrentar las características específicas de estos entornos. Se concluye que la implementación de mecanismos eficaces de seguridad, junto con la adopción de buenas prácticas de gestión de riesgos y el desarrollo de tecnologías emergentes, es fundamental para garantizar el uso seguro y confiable de las aplicaciones basadas en Internet de las Cosas.

**Palabras clave:** Internet de las Cosas. seguridad de la información. Vulnerabilidades en IoT. Ciberseguridad. Protección de datos.

## INTRODUÇÃO

A evolução das tecnologias digitais tem provocado profundas transformações na forma como pessoas, dispositivos e sistemas interagem no cotidiano. Nesse contexto, a Internet das Coisas (Internet of Things – IoT) surge como uma das principais inovações tecnológicas da atualidade, possibilitando a conexão de diversos dispositivos à internet, como sensores, eletrodomésticos inteligentes, sistemas industriais e equipamentos médicos. Essa interconectividade permite a coleta, transmissão e análise de grandes volumes de dados em tempo real, contribuindo para a automação de processos e para o desenvolvimento de cidades inteligentes, casas inteligentes e soluções tecnológicas em diferentes setores da sociedade (MORAES et al., 2022).

A expansão da IoT tem gerado inúmeras oportunidades de inovação, aumentando a eficiência operacional, a capacidade de monitoramento e a integração entre sistemas digitais. De acordo com Ahluwalia et al. (2024), o crescimento acelerado da Internet das Coisas está transformando diversos setores da economia, incluindo saúde, indústria, transporte e agricultura, criando novos modelos de negócios baseados em conectividade e análise de dados. Entretanto, ao mesmo tempo em que essa tecnologia amplia as possibilidades de integração digital, também aumenta significativamente os riscos relacionados à segurança da informação.



A grande quantidade de dispositivos conectados à rede amplia a superfície de ataque para ameaças cibernéticas, tornando os sistemas mais vulneráveis a invasões, vazamentos de dados e manipulação indevida de informações. Muitos dispositivos IoT apresentam limitações de processamento, armazenamento e recursos de segurança, o que dificulta a implementação de mecanismos avançados de proteção. Conforme destacam Alves, Peixoto e Rosa (2021), a crescente utilização de dispositivos conectados exige novas estratégias de segurança da informação capazes de proteger dados pessoais e garantir a privacidade dos usuários.

Outro fator que contribui para o aumento dos riscos de segurança é a heterogeneidade dos dispositivos e protocolos utilizados nos ambientes IoT. Segundo Laaroussi e Novo (2021), a diversidade de protocolos de comunicação e a limitação de recursos computacionais em dispositivos IoT representam desafios significativos para a implementação de mecanismos de autenticação, criptografia e controle de acesso. Essas limitações podem facilitar a exploração de vulnerabilidades por agentes mal-intencionados, comprometendo a integridade, a confidencialidade e a disponibilidade das informações.

Estudos recentes têm evidenciado que muitos dispositivos conectados apresentam falhas de segurança que podem ser exploradas por ataques cibernéticos. Rocha (2024) destaca que vulnerabilidades em dispositivos IoT podem permitir acesso não autorizado a redes corporativas ou residenciais, possibilitando desde o roubo de informações sensíveis até a utilização desses dispositivos em ataques distribuídos, como os ataques de negação de serviço (DDoS). Nesse sentido, compreender as principais vulnerabilidades presentes nos sistemas IoT torna-se essencial para o desenvolvimento de estratégias eficazes de proteção.

Além disso, a proteção de dados em ambientes IoT também envolve questões relacionadas à privacidade e à legislação de proteção de dados. A utilização massiva de dispositivos conectados pode resultar na coleta de grandes volumes de dados pessoais, exigindo mecanismos adequados de governança e segurança da informação. Nesse contexto, Oliveira e Rizo (2022) destacam que a segurança e a privacidade são elementos fundamentais para garantir a confiança dos usuários e a sustentabilidade das aplicações baseadas em Internet das Coisas.

Diante desse cenário, torna-se necessário desenvolver estratégias capazes de mitigar os riscos associados à segurança da informação em ambientes IoT. Pesquisas recentes têm explorado diferentes abordagens para fortalecer a proteção desses sistemas, incluindo o uso de blockchain, criptografia avançada, autenticação robusta e monitoramento inteligente de redes. Conforme apontam Cândido (2024) e Frogeri et al. (2022), tecnologias emergentes, como blockchain, podem contribuir para aumentar a segurança e a confiabilidade das redes IoT, permitindo a descentralização de processos e a proteção da integridade dos dados.



Apesar dos avanços tecnológicos, ainda existem lacunas significativas no que se refere à segurança da informação em ambientes de Internet das Coisas. A rápida expansão dessas tecnologias muitas vezes ocorre sem a implementação adequada de padrões de segurança, o que pode resultar em vulnerabilidades críticas nos sistemas conectados. Dessa forma, torna-se fundamental ampliar os estudos sobre os desafios, vulnerabilidades e estratégias de proteção em ambientes IoT, contribuindo para o desenvolvimento de soluções mais seguras e confiáveis para a sociedade digital.

Nesse contexto, o presente estudo aborda a segurança da informação em ambientes de Internet das Coisas, analisando os principais desafios, vulnerabilidades e estratégias de proteção relacionadas a esses sistemas. A pesquisa busca compreender os riscos associados à utilização de dispositivos conectados e identificar mecanismos capazes de fortalecer a

segurança das redes IoT, contribuindo para o avanço do conhecimento na área de segurança da informação.

## MÉTODOS

O presente estudo caracteriza-se como uma pesquisa de revisão de literatura, de natureza qualitativa e caráter exploratório, com o objetivo de analisar os principais desafios, vulnerabilidades e estratégias de proteção relacionados à segurança da informação em ambientes de Internet das Coisas (IoT). A revisão de literatura consiste em um método de investigação que permite reunir, analisar e sintetizar conhecimentos já publicados sobre determinado tema, possibilitando a compreensão do estado atual da pesquisa e a identificação de lacunas no conhecimento científico.

A coleta de dados foi realizada por meio de levantamento bibliográfico em fontes científicas e acadêmicas relevantes para a área de tecnologia da informação e segurança digital. Foram consultados livros, artigos científicos, dissertações, monografias e trabalhos publicados em periódicos e eventos acadêmicos. As bases de dados utilizadas para a busca das publicações incluíram bibliotecas digitais, repositórios institucionais e bases de dados científicas amplamente utilizadas na área de tecnologia, como Google Scholar, IEEE Xplore, Scopus e periódicos eletrônicos nacionais e internacionais.



Para a realização da busca bibliográfica foram utilizados descritores relacionados ao tema da pesquisa, tais como: Internet das Coisas (IoT), segurança da informação, vulnerabilidades em IoT, cibersegurança, dispositivos conectados, proteção de dados e redes inteligentes. A seleção dos estudos considerou publicações relevantes que abordassem aspectos relacionados à segurança, privacidade, vulnerabilidades e mecanismos de proteção em sistemas IoT.

Os critérios de inclusão adotados na pesquisa consideraram trabalhos publicados em português ou inglês, disponíveis em formato digital e que apresentassem contribuições relevantes para o estudo da segurança da informação em ambientes de Internet das Coisas. Foram priorizados artigos científicos, dissertações, livros e trabalhos acadêmicos publicados nos últimos anos, bem como estudos amplamente citados na literatura da área. Como critérios de exclusão, foram descartados materiais duplicados, trabalhos que não apresentavam relação direta com o tema proposto e publicações que não apresentavam rigor científico adequado.

Após a etapa de seleção das fontes, foi realizada a leitura exploratória dos materiais identificados, seguida de leitura analítica e interpretativa das obras selecionadas. Nesse processo, buscou-se identificar os principais conceitos, desafios, vulnerabilidades e estratégias de proteção relacionados à segurança em ambientes IoT. As informações obtidas foram analisadas de forma comparativa, permitindo a construção de uma síntese teórica sobre o tema abordado.

Por tratar-se de uma pesquisa baseada exclusivamente em revisão de literatura e análise de documentos científicos, não houve envolvimento direto de seres humanos ou animais na coleta de dados. Dessa forma, o estudo não demandou submissão a comitê de ética em pesquisa, uma vez que todas as informações utilizadas são provenientes de fontes públicas e científicas previamente publicadas.

A partir da análise das publicações selecionadas, foi possível reunir e organizar os principais conhecimentos disponíveis na literatura sobre segurança da informação em ambientes de Internet das Coisas, contribuindo para a compreensão dos riscos associados a essas tecnologias e das estratégias utilizadas para mitigação de vulnerabilidades em sistemas conectados.



## RESULTADOS

A análise da literatura selecionada permitiu identificar diversos aspectos relevantes relacionados à segurança da informação em ambientes de Internet das Coisas (IoT). Um dos principais pontos observados refere-se às vulnerabilidades presentes nos dispositivos conectados, que frequentemente apresentam falhas em mecanismos de autenticação e controle de acesso. Essas falhas podem permitir que indivíduos não autorizados obtenham acesso aos dispositivos e às redes em que estão inseridos. Além disso, muitos equipamentos ainda utilizam senhas padrão ou senhas fracas definidas pelos fabricantes, o que facilita a exploração dessas falhas por agentes mal-intencionados.

Outro problema recorrente identificado nos estudos analisados é a ausência de atualizações regulares de segurança e correções de software, o que deixa os dispositivos expostos a vulnerabilidades já conhecidas. Soma-se a isso a comunicação de dados sem o uso adequado de criptografia, aumentando o risco de interceptação de informações sensíveis durante a transmissão. Também se observou que as limitações de processamento e

armazenamento presentes em muitos dispositivos IoT dificultam a implementação de mecanismos de segurança mais robustos.

No que se refere às ameaças cibernéticas, os estudos apontam que os dispositivos IoT podem ser utilizados como alvos ou instrumentos de diferentes tipos de ataques. Entre os ataques mais recorrentes estão os ataques de negação de serviço distribuído (DDoS), nos quais redes de dispositivos comprometidos são utilizadas para sobrecarregar sistemas e serviços online. Também foram identificados ataques de interceptação de dados, conhecidos como ataques man-in-the-middle, nos quais um invasor intercepta a comunicação entre dispositivos para obter acesso a informações transmitidas.

Outro risco significativo envolve o roubo de dados pessoais ou corporativos armazenados ou transmitidos pelos dispositivos conectados. Além disso, a exploração de falhas em protocolos de comunicação utilizados em redes IoT pode permitir o acesso indevido a sistemas e informações. Em muitos casos, dispositivos comprometidos também são utilizados para a formação de botnets, ampliando o alcance e o impacto de ataques cibernéticos em larga escala.

Os resultados da revisão de literatura também evidenciam diversos desafios para a implementação de segurança em ambientes IoT. Um dos principais desafios está relacionado à grande heterogeneidade de dispositivos, plataformas e tecnologias utilizadas nesses sistemas, o que dificulta a padronização de mecanismos de segurança. Outro fator relevante é o crescimento acelerado do número de dispositivos conectados à internet, ampliando significativamente a superfície de ataque disponível para criminosos digitais.



Além disso, muitos dispositivos apresentam limitações de hardware, como baixo poder de processamento e armazenamento reduzido, o que dificulta a aplicação de soluções avançadas de segurança. A falta de conscientização de usuários e organizações sobre boas práticas de segurança digital também foi identificada como um fator que contribui para o aumento das vulnerabilidades nesses ambientes. Soma-se a isso a necessidade de integração entre medidas de segurança da informação, políticas de privacidade e regulamentações relacionadas à proteção de dados.

Diante desses desafios, os estudos analisados apresentam diferentes estratégias e mecanismos de proteção que podem contribuir para o fortalecimento da segurança em redes IoT. Entre as principais estratégias identificadas está a implementação de criptografia na comunicação entre dispositivos, garantindo maior confidencialidade das informações

transmitidas. Também se destaca a utilização de mecanismos de autenticação forte e controle de acesso para restringir o uso dos dispositivos apenas a usuários autorizados.

A realização de atualizações periódicas de firmware e software é outra prática importante para corrigir vulnerabilidades e reduzir riscos de exploração por atacantes. Além disso, o monitoramento contínuo das redes permite a identificação de comportamentos suspeitos e possíveis tentativas de invasão. Alguns estudos também apontam o uso de tecnologias emergentes, como blockchain, como uma alternativa para aumentar a integridade e a rastreabilidade das informações em redes IoT. Paralelamente, destaca-se a importância do desenvolvimento de políticas de segurança e da adoção de boas práticas tanto por fabricantes quanto por usuários de dispositivos conectados.

De modo geral, os trabalhos analisados demonstram que a segurança da informação representa um dos principais desafios para a expansão segura da Internet das Coisas. As pesquisas indicam que a combinação entre tecnologias de proteção, gestão adequada de riscos e conscientização dos usuários é fundamental para reduzir vulnerabilidades e aumentar a confiabilidade dos sistemas.

Além disso, os estudos apontam para a necessidade de desenvolvimento de novos modelos de segurança adaptados às características específicas dos ambientes IoT, considerando as limitações técnicas dos dispositivos e a diversidade de tecnologias envolvidas. Nesse sentido, os resultados reforçam a importância da continuidade das pesquisas e do desenvolvimento de soluções capazes de fortalecer a segurança e garantir maior confiabilidade na utilização das tecnologias baseadas em Internet das Coisas.



## DISCUSSÃO

### Vulnerabilidades estruturais dos dispositivos IoT

A expansão da Internet das Coisas (IoT) tem proporcionado avanços significativos na conectividade entre dispositivos e sistemas digitais, permitindo a automação de processos e o desenvolvimento de soluções tecnológicas em diversos setores da sociedade. No entanto, juntamente com os benefícios trazidos por essa tecnologia, surgem também desafios relevantes relacionados à segurança da informação. As vulnerabilidades estruturais presentes em muitos dispositivos IoT representam um dos principais fatores de risco para a integridade, confidencialidade e disponibilidade dos dados que circulam nesses ambientes.

Os dispositivos IoT são frequentemente projetados com foco na funcionalidade, baixo custo de produção e rápida inserção no mercado, o que muitas vezes resulta na negligência de aspectos fundamentais de segurança. De acordo com Ahluwalia et al. (2024), a rápida evolução e disseminação das tecnologias de Internet das Coisas têm ampliado a conectividade global, porém também têm aumentado significativamente os riscos relacionados a falhas de segurança, especialmente em dispositivos que não foram desenvolvidos com mecanismos robustos de proteção.

Entre as principais vulnerabilidades estruturais observadas nesses dispositivos estão falhas nos sistemas de autenticação e controle de acesso. Muitos equipamentos ainda utilizam credenciais padrão definidas pelos fabricantes ou sistemas de autenticação simplificados, o que facilita o acesso indevido por usuários não autorizados. Conforme destacam Alves, Peixoto e Rosa (2021), a utilização de senhas fracas ou padrões de autenticação inadequados pode permitir que dispositivos conectados sejam facilmente explorados por agentes mal-intencionados, comprometendo não apenas o equipamento individual, mas também toda a rede à qual ele está conectado.

Outro fator que contribui para a existência de vulnerabilidades estruturais em dispositivos IoT está relacionado à ausência de atualizações regulares de software e firmware. Muitos fabricantes deixam de fornecer atualizações de segurança após o lançamento dos dispositivos, o que mantém falhas conhecidas ativas nos sistemas. Nesse contexto, Rocha (2024) ressalta que a falta de manutenção e atualização de sistemas IoT amplia significativamente o risco de exploração de vulnerabilidades por cibercriminosos, permitindo ataques que podem comprometer dados sensíveis e a infraestrutura digital.



Além disso, a comunicação entre dispositivos IoT nem sempre utiliza mecanismos adequados de criptografia. A transmissão de dados sem proteção adequada pode facilitar a interceptação de informações durante o processo de comunicação entre dispositivos e servidores. Laaroussi e Novo (2021) destacam que muitos protocolos utilizados em redes IoT foram inicialmente desenvolvidos para ambientes com recursos computacionais limitados, o que resultou em soluções de comunicação que nem sempre priorizam a segurança da informação.

Outro aspecto importante refere-se às limitações de hardware presentes em muitos dispositivos conectados. Sensores, câmeras inteligentes e outros equipamentos IoT frequentemente possuem capacidade reduzida de processamento e armazenamento, o que

dificulta a implementação de mecanismos avançados de segurança, como sistemas robustos de criptografia e autenticação multifator. Segundo Lohiya e Thakkar (2021), essas limitações tecnológicas representam um desafio significativo para o desenvolvimento de arquiteturas de segurança eficientes em ambientes IoT.

A diversidade de dispositivos e plataformas também contribui para o aumento das vulnerabilidades estruturais. A IoT é composta por equipamentos de diferentes fabricantes, que utilizam variados sistemas operacionais, protocolos de comunicação e padrões tecnológicos. Essa heterogeneidade dificulta a padronização de medidas de segurança e pode resultar em lacunas de proteção dentro das redes conectadas. Moraes et al. (2022) destacam que a integração de múltiplos dispositivos e tecnologias em ambientes IoT exige o desenvolvimento de estratégias de segurança capazes de lidar com essa diversidade tecnológica.

Além das vulnerabilidades técnicas, também existem desafios relacionados à proteção de dados e à privacidade dos usuários. Muitos dispositivos IoT coletam e armazenam informações pessoais, como dados de localização, hábitos de consumo e registros de atividades domésticas ou corporativas. Nesse sentido, Oliveira e Rizo (2022) ressaltam que a segurança e a privacidade devem ser consideradas elementos centrais no desenvolvimento de soluções baseadas em Internet das Coisas, especialmente diante do crescimento do volume de dados gerados por esses dispositivos.



Diante desse cenário, pesquisadores têm investigado diferentes estratégias para mitigar os riscos associados às vulnerabilidades estruturais da IoT. Entre essas estratégias destacam-se o uso de tecnologias emergentes, como blockchain, que podem contribuir para aumentar a integridade e a rastreabilidade das informações em redes distribuídas. Estudos como os de Cândido (2024) e Frogeri et al. (2022) apontam que a integração entre tecnologias de segurança e novas arquiteturas de rede pode fortalecer significativamente a proteção dos sistemas IoT.

Portanto, a análise das vulnerabilidades estruturais presentes nos dispositivos IoT evidencia a necessidade de adoção de práticas mais rigorosas de segurança desde a fase de desenvolvimento dessas tecnologias. A implementação de mecanismos robustos de autenticação, criptografia, atualização de software e gestão de riscos torna-se essencial para reduzir a exposição a ameaças cibernéticas e garantir maior confiabilidade na utilização das soluções baseadas em Internet das Coisas.

## Impacto dos ataques cibernéticos em ambientes IoT

A crescente utilização da Internet das Coisas (IoT) tem ampliado significativamente a conectividade entre dispositivos, sistemas e redes digitais, possibilitando avanços em diversos setores como indústria, saúde, transporte e ambientes domésticos. Entretanto, essa expansão tecnológica também tem aumentado os riscos relacionados à segurança da informação, uma vez que a grande quantidade de dispositivos conectados pode se tornar alvo de ataques cibernéticos. Nesse contexto, os impactos desses ataques em ambientes IoT podem ser amplos, afetando desde usuários individuais até infraestruturas críticas e organizações de grande porte.

Os ataques cibernéticos direcionados a dispositivos IoT podem comprometer a confidencialidade, a integridade e a disponibilidade das informações transmitidas e armazenadas nesses sistemas. Conforme destacam Alves, Peixoto e Rosa (2021), a segurança e a privacidade dos dados representam desafios fundamentais no contexto da Internet das Coisas, especialmente devido à quantidade crescente de dispositivos conectados que coletam e compartilham informações continuamente. Quando esses dispositivos apresentam falhas de segurança, tornam-se vulneráveis à exploração por atacantes, que podem acessar dados sensíveis ou manipular sistemas conectados.



Um dos impactos mais comuns dos ataques cibernéticos em ambientes IoT é a interrupção de serviços digitais por meio de ataques de negação de serviço distribuído (DDoS). Nesse tipo de ataque, dispositivos comprometidos são utilizados para gerar grandes volumes de tráfego direcionados a servidores ou sistemas específicos, sobrecarregando a infraestrutura e tornando os serviços indisponíveis. Segundo Rocha Neto et al. (2025), dispositivos IoT vulneráveis podem ser facilmente integrados a redes de computadores infectados, conhecidas como botnets, que são utilizadas para realizar ataques em larga escala contra organizações e sistemas digitais.

Além da interrupção de serviços, os ataques cibernéticos também podem resultar no roubo de dados pessoais e corporativos. Muitos dispositivos IoT coletam e armazenam informações sensíveis, como dados de localização, registros de comportamento dos usuários e informações relacionadas a ambientes residenciais ou empresariais. De acordo com Oliveira e Rizo (2022), a falta de mecanismos adequados de segurança nesses dispositivos pode facilitar o acesso não autorizado a dados confidenciais, comprometendo a privacidade dos usuários e gerando riscos legais e financeiros para organizações.

Outro impacto relevante refere-se à possibilidade de manipulação ou controle indevido de dispositivos conectados. Em ambientes industriais ou em sistemas de automação residencial, por exemplo, um ataque cibernético pode permitir que invasores alterem o funcionamento de equipamentos, causando falhas operacionais ou danos materiais. Laaroussi e Novo (2021) destacam que vulnerabilidades em protocolos de comunicação utilizados em redes IoT podem ser exploradas para interceptar ou modificar dados transmitidos entre dispositivos, ampliando os riscos associados à segurança dessas tecnologias.

Além dos impactos técnicos, os ataques cibernéticos também podem gerar consequências econômicas e sociais significativas. Empresas que sofrem incidentes de segurança podem enfrentar prejuízos financeiros decorrentes da interrupção de operações, perda de dados e danos à reputação institucional. Segundo Belfante Neto (2024), a gestão de riscos em redes IoT torna-se fundamental para minimizar os impactos de ataques cibernéticos, sendo necessário adotar estratégias de segurança capazes de identificar e mitigar vulnerabilidades antes que elas sejam exploradas.

Outro aspecto relevante está relacionado à utilização de dispositivos IoT em infraestruturas críticas, como sistemas de saúde, redes elétricas e sistemas de transporte. Conforme destacam Camara et al. (2021), a integração de tecnologias digitais em setores estratégicos exige mecanismos robustos de segurança, uma vez que ataques cibernéticos nesses ambientes podem comprometer serviços essenciais e afetar diretamente a sociedade. Nesse sentido, a proteção desses sistemas torna-se uma prioridade para governos, organizações e pesquisadores da área de segurança da informação.



Diante desse cenário, torna-se evidente que os ataques cibernéticos representam uma ameaça significativa para os ambientes baseados em Internet das Coisas. A análise da literatura demonstra que a expansão dessas tecnologias deve ser acompanhada pelo desenvolvimento de estratégias de segurança mais eficazes, capazes de proteger os dispositivos conectados e reduzir os riscos associados às ameaças digitais. Dessa forma, a adoção de políticas de segurança, a implementação de tecnologias de proteção e o investimento em pesquisas voltadas à segurança da informação são elementos essenciais para garantir a confiabilidade e a sustentabilidade dos sistemas IoT.

## Desafios para implementação de segurança em IoT

A implementação de mecanismos eficazes de segurança em ambientes de Internet das Coisas (IoT) representa um dos principais desafios para a expansão segura dessa tecnologia. A IoT é caracterizada pela interconexão de diversos dispositivos, sensores e sistemas que coletam, processam e compartilham informações continuamente. Essa ampla conectividade traz benefícios significativos em termos de automação, eficiência e monitoramento, porém também amplia as vulnerabilidades e os riscos relacionados à segurança da informação.

Um dos principais desafios para a implementação de segurança em ambientes IoT está relacionado à grande diversidade de dispositivos e tecnologias utilizadas. A IoT é composta por equipamentos de diferentes fabricantes, com variados sistemas operacionais, protocolos de comunicação e padrões tecnológicos. Essa heterogeneidade dificulta a criação de padrões universais de segurança, tornando mais complexa a proteção das redes e sistemas conectados. De acordo com Lohiya e Thakkar (2021), a diversidade de plataformas e aplicações presentes na Internet das Coisas exige soluções de segurança capazes de se adaptar a diferentes contextos e arquiteturas tecnológicas.

Outro fator relevante refere-se ao crescimento acelerado da quantidade de dispositivos conectados à internet. Com o avanço das tecnologias digitais e a popularização de dispositivos inteligentes, milhões de novos equipamentos são integrados às redes diariamente. Esse crescimento amplia significativamente a superfície de ataque disponível para cibercriminosos, tornando mais difícil o monitoramento e a proteção desses sistemas. Ahluwalia et al. (2024) destacam que o rápido desenvolvimento da IoT tem gerado desafios importantes para a segurança da informação, uma vez que muitos dispositivos são incorporados às redes sem a implementação adequada de mecanismos de proteção.



As limitações técnicas presentes em muitos dispositivos IoT também representam um obstáculo significativo para a implementação de soluções de segurança robustas. Sensores, câmeras inteligentes e outros dispositivos conectados frequentemente possuem capacidade limitada de processamento, memória e armazenamento. Essas restrições dificultam a aplicação de mecanismos avançados de segurança, como criptografia complexa, autenticação multifator e sistemas sofisticados de monitoramento. Segundo Laaroussi e Novo (2021), os protocolos de comunicação utilizados em ambientes IoT muitas vezes precisam ser adaptados para funcionar em dispositivos com recursos reduzidos, o que pode comprometer o nível de segurança oferecido.

Além das limitações tecnológicas, a falta de atualização e manutenção dos dispositivos também representa um desafio relevante. Muitos equipamentos IoT permanecem em uso por longos períodos sem receber atualizações de segurança ou correções de software, o que mantém vulnerabilidades conhecidas ativas nos sistemas. Rocha (2024) ressalta que a ausência de políticas eficazes de atualização e gerenciamento de dispositivos pode aumentar significativamente o risco de exploração de falhas por atacantes.

Outro aspecto importante refere-se à conscientização dos usuários e das organizações quanto à importância da segurança digital. Em muitos casos, dispositivos IoT são utilizados sem a configuração adequada de mecanismos de proteção, como alteração de senhas padrão, ativação de autenticação segura ou implementação de políticas de controle de acesso. Conforme destacam Alves, Peixoto e Rosa (2021), a segurança da informação em ambientes IoT depende não apenas de soluções tecnológicas, mas também da adoção de boas práticas por parte de usuários, fabricantes e organizações.

Além disso, a crescente coleta e processamento de dados pessoais por dispositivos IoT levanta preocupações relacionadas à privacidade e à proteção de dados. Muitos dispositivos conectados registram informações sensíveis sobre hábitos, localização e comportamento dos usuários, o que exige mecanismos adequados de proteção dessas informações. Oliveira e Rizo (2022) destacam que a integração entre segurança da informação e políticas de privacidade é essencial para garantir a confiança dos usuários nas tecnologias baseadas em Internet das Coisas.



## Importância da proteção de dados e da privacidade

A crescente expansão da Internet das Coisas (IoT) tem transformado significativamente a forma como dados são coletados, processados e compartilhados em ambientes digitais. Dispositivos conectados, como sensores, câmeras inteligentes, assistentes virtuais e equipamentos de automação residencial ou industrial, possuem a capacidade de gerar e transmitir grandes volumes de informações em tempo real. Embora essa conectividade traga inúmeros benefícios para a automação e otimização de processos, ela também levanta preocupações relevantes relacionadas à proteção de dados e à privacidade dos usuários.

Os dispositivos IoT frequentemente coletam dados sensíveis, incluindo informações pessoais, padrões de comportamento, localização geográfica, preferências de consumo e registros de atividades domésticas ou profissionais. Esses dados podem ser utilizados para

melhorar serviços, automatizar tarefas e gerar análises inteligentes, porém, quando não são adequadamente protegidos, podem representar um risco significativo para a privacidade dos indivíduos. Nesse contexto, Alves, Peixoto e Rosa (2021) destacam que a segurança e a privacidade dos dados são elementos fundamentais para o desenvolvimento sustentável das tecnologias baseadas em Internet das Coisas, uma vez que a exposição inadequada dessas informações pode resultar em violações de privacidade e uso indevido dos dados coletados.

Outro aspecto importante refere-se ao fato de que muitos dispositivos IoT operam de forma contínua e silenciosa, coletando informações sem que os usuários tenham plena consciência da quantidade e do tipo de dados que estão sendo armazenados ou compartilhados. Essa característica aumenta a necessidade de implementação de mecanismos de segurança capazes de garantir a confidencialidade e o controle sobre essas informações. De acordo com Oliveira e Rizo (2022), a proteção da privacidade em ambientes IoT deve envolver não apenas mecanismos tecnológicos de segurança, mas também políticas claras de gerenciamento e utilização dos dados coletados.

Além disso, a proteção de dados em sistemas IoT também está diretamente relacionada à conformidade com legislações de proteção de dados pessoais. Em diversos países, leis e regulamentações foram criadas para garantir que informações pessoais sejam tratadas de forma responsável e segura. No contexto brasileiro, por exemplo, a Lei Geral de Proteção de Dados (LGPD) estabelece princípios e diretrizes para o tratamento de dados pessoais, exigindo que organizações adotem medidas adequadas para garantir a segurança das informações coletadas. Camara et al. (2021) ressaltam que a aplicação de tecnologias digitais em setores sensíveis, como saúde e serviços públicos, exige especial atenção à proteção de dados, pois a exposição dessas informações pode causar impactos significativos para indivíduos e instituições.



Outro fator relevante está relacionado ao aumento das ameaças cibernéticas que podem comprometer a privacidade dos usuários. Dispositivos IoT vulneráveis podem ser explorados por atacantes para acessar dados pessoais ou monitorar atividades de indivíduos e organizações. Rocha (2024) destaca que vulnerabilidades presentes em dispositivos conectados podem permitir o acesso indevido a sistemas e informações sensíveis, ampliando os riscos associados à segurança digital.

Diante desse cenário, a implementação de mecanismos robustos de proteção de dados torna-se essencial para garantir a confiança dos usuários nas tecnologias baseadas em Internet das Coisas. Medidas como criptografia de dados, autenticação segura, controle de acesso e

monitoramento contínuo das redes são estratégias importantes para reduzir riscos e fortalecer a segurança dos sistemas. Além disso, a adoção de boas práticas de segurança por fabricantes e usuários contribui para minimizar vulnerabilidades e proteger informações sensíveis.

## Tecnologias emergentes como apoio à segurança em IoT

O avanço da Internet das Coisas (IoT) tem impulsionado o desenvolvimento de novas soluções tecnológicas voltadas à segurança da informação. À medida que aumenta o número de dispositivos conectados, também cresce a necessidade de mecanismos mais sofisticados capazes de proteger redes, dados e sistemas contra ameaças cibernéticas. Nesse contexto, diversas tecnologias emergentes vêm sendo estudadas e aplicadas como ferramentas de apoio à segurança em ambientes IoT, contribuindo para o fortalecimento da proteção das informações e para a redução das vulnerabilidades presentes nesses sistemas.

Uma das tecnologias que tem recebido destaque nesse cenário é o blockchain, que pode ser utilizado como uma alternativa para aumentar a integridade, a transparência e a confiabilidade das transações realizadas entre dispositivos conectados. O blockchain funciona como um sistema descentralizado de registro de informações, no qual os dados são armazenados em blocos interligados e protegidos por mecanismos criptográficos. De acordo com Cândido (2024), a aplicação de blockchain em redes IoT pode contribuir para a criação de ambientes mais seguros, pois permite registrar transações de forma imutável, dificultando a alteração ou manipulação indevida das informações. Da mesma forma, Frogeri et al. (2022) destacam que a integração entre blockchain e Internet das Coisas pode ampliar a segurança dos sistemas conectados, promovendo maior confiabilidade na comunicação entre dispositivos e na gestão de dados.



Outra tecnologia emergente que tem sido utilizada como apoio à segurança em ambientes IoT é a inteligência artificial (IA), especialmente em sistemas de detecção de intrusões e monitoramento de redes. A inteligência artificial possibilita a análise de grandes volumes de dados gerados pelos dispositivos conectados, permitindo identificar padrões de comportamento e detectar atividades suspeitas em tempo real. Segundo Belfante Neto (2024), a utilização de técnicas de aprendizado de máquina e análise comportamental pode auxiliar na identificação precoce de ameaças cibernéticas, contribuindo para a prevenção de ataques e para o fortalecimento da segurança em redes IoT.

Além disso, tecnologias de criptografia avançada desempenham um papel fundamental na proteção das comunicações entre dispositivos conectados. A criptografia permite garantir a confidencialidade e a integridade dos dados transmitidos nas redes IoT, dificultando a interceptação ou manipulação das informações por agentes mal-intencionados. Laaroussi e Novo (2021) ressaltam que a implementação de protocolos de comunicação seguros e mecanismos criptográficos adequados é essencial para reduzir os riscos de ataques em ambientes IoT, especialmente em dispositivos que operam em redes abertas ou distribuídas.

Outra abordagem relevante envolve o desenvolvimento de sistemas de autenticação mais robustos, capazes de garantir que apenas usuários ou dispositivos autorizados tenham acesso às redes e aos sistemas conectados. Técnicas como autenticação multifator, certificação digital e gerenciamento seguro de identidades podem contribuir para reduzir o risco de acessos não autorizados. Nesse sentido, Alves, Peixoto e Rosa (2021) destacam que o fortalecimento dos mecanismos de autenticação é um dos pilares fundamentais para a proteção da segurança da informação em ambientes baseados em Internet das Coisas.

Adicionalmente, o uso de arquiteturas de segurança baseadas em computação em nuvem e edge computing tem sido explorado como uma forma de melhorar o gerenciamento e a proteção das redes IoT. Essas tecnologias permitem processar e analisar dados em diferentes níveis da infraestrutura digital, possibilitando respostas mais rápidas a incidentes de segurança e melhor controle sobre o fluxo de informações. Lohiya e Thakkar (2021) ressaltam que o desenvolvimento de arquiteturas distribuídas pode contribuir para melhorar a eficiência e a segurança das aplicações baseadas em IoT.



## Necessidade de desenvolvimento de novas abordagens de segurança

O crescimento acelerado da Internet das Coisas (IoT) tem ampliado significativamente o número de dispositivos conectados à internet, criando um ambiente digital cada vez mais complexo e interconectado. Embora essa expansão traga inúmeros benefícios em termos de automação, eficiência e inovação tecnológica, ela também evidencia a necessidade de desenvolver novas abordagens de segurança capazes de lidar com os desafios específicos desses ambientes. A segurança tradicional de redes e sistemas computacionais muitas vezes não é suficiente para proteger a diversidade de dispositivos e aplicações presentes na IoT, tornando essencial a criação de modelos de proteção mais adaptados às características dessa tecnologia.

Um dos principais fatores que justificam a necessidade de novas abordagens de segurança é a própria natureza distribuída e heterogênea da Internet das Coisas. Diferentemente das redes tradicionais, os ambientes IoT são compostos por dispositivos com diferentes capacidades de processamento, variados sistemas operacionais e múltiplos protocolos de comunicação. Essa diversidade dificulta a aplicação de soluções padronizadas de segurança e exige o desenvolvimento de mecanismos mais flexíveis e adaptáveis. Lohiya e Thakkar (2021) ressaltam que os ambientes IoT apresentam desafios específicos de segurança devido à ampla variedade de aplicações e dispositivos conectados, o que demanda novas estratégias de proteção voltadas para esse contexto tecnológico.

Outro aspecto relevante está relacionado às limitações de hardware presentes em muitos dispositivos IoT. Sensores, atuadores e outros equipamentos conectados geralmente possuem recursos computacionais reduzidos, como baixa capacidade de processamento, memória limitada e restrições energéticas. Essas limitações dificultam a implementação de mecanismos de segurança mais complexos, como algoritmos criptográficos avançados ou sistemas sofisticados de autenticação. Nesse sentido, pesquisadores têm destacado a necessidade de desenvolver soluções de segurança leves e eficientes, capazes de oferecer proteção adequada sem comprometer o desempenho dos dispositivos. Laaroussi e Novo (2021) destacam que o desenvolvimento de protocolos seguros adaptados a dispositivos com recursos limitados é um dos principais desafios atuais da segurança em redes IoT.



Além das limitações tecnológicas, o aumento das ameaças cibernéticas também reforça a necessidade de novas abordagens de segurança. À medida que cresce o número de dispositivos conectados, aumenta também a superfície de ataque disponível para cibercriminosos. Dispositivos IoT vulneráveis podem ser explorados para realizar ataques de grande escala, como ataques distribuídos de negação de serviço (DDoS), roubo de dados e invasões de redes corporativas ou residenciais. Rocha (2024) destaca que muitas vulnerabilidades presentes em dispositivos IoT decorrem da ausência de práticas adequadas de segurança durante o desenvolvimento e a implementação dessas tecnologias.

Outro ponto importante refere-se à integração entre segurança da informação, privacidade de dados e regulamentações legais. Com o aumento da coleta e do processamento de dados pessoais por dispositivos IoT, torna-se fundamental garantir que essas informações sejam protegidas de acordo com normas e legislações vigentes. Oliveira e Rizo (2022) ressaltam que a proteção da privacidade e a segurança dos dados devem ser consideradas elementos

centrais no desenvolvimento de soluções baseadas em Internet das Coisas, exigindo a criação de políticas e mecanismos de segurança adequados para o tratamento dessas informações.

Nesse contexto, diversas pesquisas têm explorado novas abordagens para fortalecer a segurança em ambientes IoT, incluindo o uso de tecnologias emergentes, modelos de segurança distribuída, arquiteturas baseadas em blockchain e sistemas inteligentes de detecção de intrusões. Estudos como os de Cândido (2024) e Frogeri et al. (2022) indicam que a integração entre tecnologias inovadoras e estratégias avançadas de proteção pode contribuir significativamente para reduzir vulnerabilidades e aumentar a confiabilidade das redes IoT.

## CONSIDERAÇÕES FINAIS

A Internet das Coisas (IoT) representa uma das principais inovações tecnológicas da atualidade, promovendo a integração entre dispositivos, sistemas e redes digitais em diferentes contextos, como ambientes domésticos, industriais, comerciais e institucionais. Essa conectividade tem proporcionado avanços significativos na automação de processos, no monitoramento de atividades e na geração de dados em tempo real, contribuindo para o desenvolvimento de soluções tecnológicas capazes de melhorar a eficiência e a qualidade dos serviços oferecidos à sociedade.



Entretanto, juntamente com os benefícios proporcionados pela expansão da IoT, surgem também desafios relevantes relacionados à segurança da informação. A grande quantidade de dispositivos conectados, a diversidade de tecnologias utilizadas e as limitações técnicas presentes em muitos equipamentos ampliam os riscos de vulnerabilidades e ataques cibernéticos. Dessa forma, garantir a proteção das informações e a confiabilidade dos sistemas torna-se uma preocupação central para pesquisadores, organizações e desenvolvedores de tecnologias digitais.

A análise realizada ao longo deste estudo evidenciou que os ambientes baseados em Internet das Coisas apresentam diferentes tipos de vulnerabilidades estruturais que podem comprometer a segurança das redes e dos dados transmitidos. Falhas em mecanismos de autenticação, ausência de atualizações de segurança, uso inadequado de criptografia e limitações de hardware são alguns dos fatores que contribuem para a exposição dos dispositivos a ameaças cibernéticas. Além disso, os ataques realizados por meio de dispositivos comprometidos podem gerar impactos significativos, incluindo interrupção de serviços, acesso indevido a informações sensíveis e prejuízos operacionais para organizações.

Outro aspecto importante identificado na pesquisa refere-se aos desafios enfrentados na implementação de mecanismos eficazes de segurança em ambientes IoT. A heterogeneidade dos dispositivos, a rápida expansão das redes conectadas e a falta de padronização de soluções de segurança dificultam o desenvolvimento de estratégias capazes de proteger adequadamente esses sistemas. Nesse contexto, torna-se fundamental investir no desenvolvimento de tecnologias, políticas e práticas de segurança que sejam capazes de acompanhar a evolução das aplicações baseadas em Internet das Coisas.

Além disso, a proteção de dados e da privacidade dos usuários destaca-se como um elemento essencial para o uso responsável dessas tecnologias. A grande quantidade de informações coletadas por dispositivos IoT exige mecanismos adequados de proteção e gerenciamento de dados, garantindo que essas informações sejam utilizadas de forma segura e ética. A adoção de políticas de segurança da informação, aliada à conscientização de usuários e organizações, pode contribuir para reduzir riscos e fortalecer a confiança nas tecnologias conectadas.

Por fim, destaca-se a importância do desenvolvimento contínuo de novas abordagens de segurança capazes de lidar com as características específicas dos ambientes IoT. A integração entre tecnologias emergentes, boas práticas de segurança e gestão de riscos representa um caminho promissor para aumentar a proteção dos dispositivos e das redes conectadas. Dessa forma, o avanço das pesquisas e o investimento em soluções inovadoras são fundamentais para garantir que a Internet das Coisas continue evoluindo de forma segura, confiável e sustentável no cenário tecnológico contemporâneo.



## REFERÊNCIAS

AHLUWALIA, A.; GARG, D. V.; KAPOOR, D. S.; GUPTA, D. L. The Internet of Things (IoT): Transformations and Challenges in the Modern World. *African Journal of Biological Sciences*, 2024.

ALVES, D.; PEIXOTO, M.; ROSA, T. Internet das Coisas (IoT): segurança e privacidade dos dados pessoais. Rio de Janeiro: Alta Books, 2021.

BELFANTE NETO, J. Estratégias de mitigação de riscos em redes IoT. *Revista de Engenharia e Tecnologia Aplicada*, v. 9, n. 2, p. 88–101, 2024.

CAMARA, M. A. A. et al. Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados. *Cadernos Ibero-Americanos de Direito Sanitário*, v. 10, n. 1, p. 93-112, 2021.

CÂNDIDO, R. Blockchain aplicado à segurança em redes IoT. *Revista de Computação Aplicada*, v. 12, n. 1, p. 33–47, 2024.

CARVALHO, A. F. A.; SANTOS, C. M. L.; GONÇALVES, L. V. Segurança em IoT. 2021. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Centro Universitário do Planalto Central Apparecido dos Santos, 2021.

FROGERI, R. F. et al. Blockchain e Internet das Coisas. *Textos para Discussão*, v. 1, n. 1, p. 813-835, 2022.

LAAROUSSI, A.; NOVO, O. Security analysis of CoAP protocol in constrained IoT environments. *Journal of Network and Computer Applications*, v. 174, p. 102887, 2021.

LOHIYA, R.; THAKKAR, A. Application domains, evaluation data sets, and research challenges of IoT: a systematic review. *IEEE Internet of Things Journal*, v. 8, p. 8774-8798, 2021.

MORAES, J. M.; QUIRINO, C.; ALMEIDA, R. M.; D'ALKMIN NEVES, J. E. Internet das Coisas (IoT): casa inteligente, definições e aplicações. *Revista Brasileira em Tecnologia da Informação*, v. 4, n. 2, p. 1-48, 2022.

OLIVEIRA, L.; RIZO, A. C. Segurança e privacidade no contexto da Internet das Coisas. *Revista Interface Tecnológica*, v. 19, n. 2, p. 201-212, 2022.

PESSOA, C. H. M. Catálogo de vulnerabilidades de segurança em sistemas de software IoT. Rio de Janeiro: UFRJ/COPPE, 2025.



PESSOA, C.; TRAVASSOS, G. Categorizing IoT Software Systems Security Vulnerabilities Through Literature Studies. In: SIMPÓSIO BRASILEIRO DE ENGENHARIA DE SOFTWARE, 38., 2024, Curitiba. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 169-180.

REGGIO, G. et al. What are IoT systems for real? An experts' survey on software engineering aspects. *Internet of Things*, v. 12, 2020.

ROCHA, M. A. Vulnerabilidades em dispositivos IoT: uma análise crítica. *Revista Brasileira de Segurança da Informação*, v. 13, n. 1, p. 45-62, 2024.

ROCHA NETO, C. M. S. et al. Segurança na Internet das Coisas: um estudo avaliativo sobre vulnerabilidades e estratégias de mitigação. Aurum Editora, p. 36-49, 2025.

SAKAMOTO, S. G. Security, privacy and blockchain in Internet of Everything context. 2020. Monografia (Especialização em Internet das Coisas) – Universidade Tecnológica Federal do Paraná, Curitiba, 2020.

SANTOS, M. M. IoT Tunnel – uma proposta para mitigar vulnerabilidades na comunicação de elementos IoT. 2020. Dissertação (Mestrado em Computação) – Universidade Federal do Rio Grande, Rio Grande, 2020.

SILVA, C. D. O. O desafio da segurança das informações digitais na Internet das Coisas. *Revista Científica Multidisciplinar Núcleo do Conhecimento*, v. 4, p. 137-157, 2018.

STORK, E. Smart voice control: um sistema IoT para casas inteligentes controlado por voz. 2019. Trabalho de Conclusão de Curso – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2019.