Revista ARACÊ
ISSN: 2358-2472

CIBERSEGURANÇA EM TEMPOS DE INTERNET DAS COISAS

CYBERSECURITY IN THE AGE OF THE INTERNET OF THINGS

CIBERSEGURIDAD EN LA ERA DEL INTERNET DE LAS COSAS

https://doi.org/10.56238/arev7n12-187

Data de submissão: 18/11/2025 **Data de publicação:** 18/12/2025

Pedro Soares Magalhães
Doutorando em Ciências da Educação
Instituição: Christian Business School (CBS)
E-mail: pedroletras26@gmail.com

Jucilene Aparecida Lima Prado
Mestranda em Tecnologia Emergentes em Educação
Instituição: MUST University
E-mail: Jucilenelprado@gmail.com

Miriam Mendonça de Jesus Fraga
Mestranda em Tecnologia Emergentes em Educação
Instituição: MUST University
E-mail: miriammendonca75@gmail.com

Elielza Barreto da Silva
Mestranda em Tecnologia Emergentes em Educação
Instituição: MUST University
E-mail: elielzabarreto@yahoo.com.br

Dayse Rodrigues dos Santos
Especialista em Psicopedagogia com ênfase em Educação Especial
Instituição: Faculdade de Educação São Luís
E-mail: profdayserodrigues@hotmail.com

Jaimy Paulo da Silva Rego
Mestrando em Ciências Contábeis e Administração
Instituição: Fundação Capixaba de Pesquisa (FUCAPE)
E-mail: jaimypaulo@gmail.com

José Rubens Rodrigues de Sousa
Doutor em Engenharia de Teleinformática (UFC)
Instituição: Universidade de Fortaleza (UNIFOR)
E-mail: telerubens@gmail.com

Iraci Braga Oliveira
Mestranda em Tecnologias Emergentes em Educação
Instituição: MUST University
E-mail: Iracibraga@hotmail.com.br

Revista ARACÊ
ISSN: 2358-2472

RESUMO
Este artigo tem como objetivo compreender os fundamentos da Teoria Histórico-Cultural de Vigotski e suas implicações para o ensino da matemática, com foco nas funções psicológicas superiores, na mediação pedagógica e na zona de desenvolvimento proximal. Trata-se de um ensaio teórico, baseado em pesquisa bibliográfica, que articula conceitos vigotskianos à prática docente na educação matemática. A análise evidencia que o desenvolvimento cognitivo dos estudantes ocorre por meio das interações sociais e da mediação do professor, que atua como facilitador do aprendizado. Assim, compreender as funções psicológicas superiores, como a memória lógica, a atenção voluntária e o pensamento abstrato, é essencial para a elaboração de estratégias pedagógicas que promovam aprendizagens significativas. Conclui-se que o ensino da matemática, quando pautado nos princípios da teoria histórico-cultural, contribui para o desenvolvimento integral do sujeito, valorizando a construção coletiva do conhecimento e a aprendizagem como processo social e cultural.

Palavras-chave: Teoria Histórico-Cultural. Ensino da Matemática. Mediação Pedagógica. Funções Psicológicas Superiores.

ABSTRACT
This article aims to understand the fundamentals of Vygotsky's Historical-Cultural Theory and its implications for mathematics teaching, focusing on higher psychological functions, pedagogical mediation, and the zone of proximal development. It is a theoretical essay, based on bibliographic research, which articulates Vygotskian concepts with teaching practice in mathematics education. The analysis shows that students' cognitive development occurs through social interactions and the mediation of the teacher, who acts as a facilitator of learning. Thus, understanding higher psychological functions, such as logical memory, voluntary attention, and abstract thinking, is essential for the development of pedagogical strategies that promote meaningful learning. It is concluded that mathematics teaching, when based on the principles of historical-cultural theory, contributes to the integral development of the subject, valuing the collective construction of knowledge and learning as a social and cultural process.

Keywords: Historical-Cultural Theory. Mathematics Education. Pedagogical Mediation. Higher Psychological Functions.

RESUMEN
El objetivo de este artículo es comprender los fundamentos de la teoría histórico-cultural de Vigotski y sus implicaciones para la enseñanza de las matemáticas, centrándose en las funciones psicológicas superiores, la mediación pedagógica y la zona de desarrollo próximo. Se trata de un ensayo teórico, basado en la investigación bibliográfica, que articula los conceptos vigotskianos con la práctica docente en la educación matemática. El análisis evidencia que el desarrollo cognitivo de los estudiantes se produce a través de las interacciones sociales y la mediación del profesor, que actúa como facilitador del aprendizaje. Por lo tanto, comprender las funciones psicológicas superiores, como la memoria lógica, la atención voluntaria y el pensamiento abstracto, es esencial para la elaboración de estrategias pedagógicas que promuevan un aprendizaje significativo. Se concluye que la enseñanza de las matemáticas, cuando se basa en los principios de la teoría histórico-cultural, contribuye al desarrollo integral del sujeto, valorando la construcción colectiva del conocimiento y el aprendizaje como proceso social y cultural.

Palabras clave: Teoría Histórico-Cultural. Enseñanza de las Matemáticas. Mediación Pedagógica. Funciones Psicológicas Superiores.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

Internet das Coisas (IoT) foi considerada uma das inovações tecnológicas mais significativas da última década, tendo remodelado profundamente os padrões de conectividade e interação entre objetos, dados e pessoas. Seu avanço permitiu a integração de sensores, atuadores e dispositivos inteligentes a diversas infraestruturas físicas, tornando possível o monitoramento em tempo real de sistemas urbanos, industriais e domésticos. Contudo, paralelamente aos seus benefícios, esse ecossistema revelou-se vulnerável a múltiplos riscos de segurança, especialmente no que se refere à fragilidade dos dispositivos, à dificuldade de atualização de firmware e à exposição de redes sem proteção adequada. Diante disso, consolidou-se a necessidade de compreender os limites técnicos e sociais que envolvem a adoção segura de soluções baseadas em IoT.

A escolha pelo tema se justificou pela crescente centralidade que os dispositivos IoT passaram a ocupar em cidades inteligentes e serviços públicos digitais. A insegurança percebida pela população, somada à ausência de padronizações técnicas e à fragilidade na detecção de ameaças, passou a comprometer a confiabilidade desses sistemas, exigindo a revisão crítica de suas bases tecnológicas. Em razão disso, considerou-se essencial refletir, de modo fundamentado, sobre as limitações estruturais e os desafios na aplicação de inteligência artificial como suporte à segurança digital em ambientes conectados. Essa discussão revelou-se particularmente relevante diante do crescimento acelerado de redes IoT em contextos urbanos, nos quais a confiança do cidadão é fator determinante para o sucesso de políticas públicas.

A partir dessa motivação, formulou-se a seguinte questão norteadora: ‘Quais são os principais desafios técnicos e perceptivos relacionados à segurança e à confiabilidade da Internet das Coisas em contextos urbanos, e de que forma a inteligência artificial tem sido empregada para mitigar essas vulnerabilidades?’ Essa indagação permitiu direcionar o foco do estudo tanto para aspectos de natureza computacional e de engenharia, quanto para fatores sociais que influenciam a aceitação tecnológica. Assim, o objetivo geral da pesquisa consistiu em ‘analisar as limitações técnicas da segurança em dispositivos IoT, com ênfase na autenticação, atualização e infraestrutura de rede, investigando o papel da inteligência artificial na detecção de ameaças e a percepção de segurança na adoção dessas tecnologias em cidades inteligentes’. De forma específica, buscou-se: (1) identificar as fragilidades estruturais mais recorrentes em dispositivos IoT; (2) examinar as aplicações da inteligência artificial na resposta a incidentes e na prevenção de ataques; e (3) avaliar os fatores sociais que interferem na percepção de segurança tecnológica em contextos urbanos conectados.

A metodologia adotada teve como base uma pesquisa de caráter qualitativo e bibliográfico, com foco na revisão de estudos recentes publicados entre 2020 e 2025. As ideias de Santana, Narciso

Revista ARACÊ
ISSN: 2358-2472

e Fernandes (2025, p. 3) orientaram a condução do processo analítico, especialmente ao destacar que "a técnica de análise utilizada consistiu na leitura, seleção e organização dos materiais de acordo com sua relevância para o tema abordado". As buscas foram realizadas na base CAPES Periódicos, utilizando palavras-chave como 'segurança em IoT', 'inteligência artificial e IoT', 'confiança tecnológica' e 'percepção de risco urbano'. Os critérios de inclusão consideraram a atualidade, o acesso completo aos textos e a aderência temática. Os critérios de exclusão eliminaram estudos com foco exclusivamente técnico sem relação com contextos urbanos ou que não apresentassem fundamentação teórica consistente.

Foram escolhidos como principais referenciais os estudos de Sahu e Mazumdar (2024), que discutem detalhadamente os riscos de segurança técnica na IoT e as contribuições da inteligência artificial; Kołaczek (2025), cuja análise técnica envolve os limites operacionais e computacionais dos dispositivos; Tariq *et al*. (2023), que abordam a fragmentação do ecossistema IoT e suas implicações para a segurança em larga escala; e Romani *et al*. (2023), que contribuem com a perspectiva sociotécnica da confiança pública em tecnologias urbanas.

A estrutura deste artigo está dividida em três capítulos centrais. O primeiro, intitulado 'Fragilidades técnicas na segurança de dispositivos IoT: autenticação, atualização e infraestrutura de rede', discute as limitações estruturais e operacionais que tornam os dispositivos vulneráveis a ameaças cibernéticas. O segundo capítulo, denominado 'Aplicações de inteligência artificial na detecção de ameaças em ambientes IoT', examina as estratégias baseadas em aprendizado de máquina e outras formas de inteligência computacional utilizadas para detectar e responder a ataques em redes distribuídas. Por fim, o terceiro capítulo, 'Confiabilidade tecnológica e percepção de segurança na adoção de soluções IoT em contextos urbanos', analisa os fatores sociais, institucionais e técnicos que afetam a aceitação das tecnologias de IoT pela população, enfatizando o papel da confiança como elemento-chave para o sucesso de políticas públicas digitais.

2 METODOLOGIA

A presente pesquisa caracteriza-se como uma investigação de natureza qualitativa, fundamentada em revisão bibliográfica, com o objetivo de analisar criticamente as fragilidades técnicas da segurança em dispositivos IoT, o uso da inteligência artificial na detecção de ameaças e a relação entre confiabilidade tecnológica e percepção de segurança em contextos urbanos. Segundo Gil (2010), a pesquisa bibliográfica consiste no exame de materiais já publicados, sendo adequada quando se pretende compreender, discutir ou problematizar determinado tema a partir do que já foi produzido

Revista ARACÊ
ISSN: 2358-2472

pela comunidade científica. Nesse sentido, a escolha por esse tipo de abordagem permitiu acessar diferentes perspectivas teóricas e identificar as contribuições mais atuais e relevantes sobre a temática.

Para alcançar os objetivos propostos, a metodologia foi estruturada em etapas. Inicialmente, realizou-se o levantamento das produções acadêmicas em bases científicas reconhecidas, seguido pela seleção dos textos com base em critérios de relevância e atualidade, e, por fim, procedeu-se à análise crítica dos conteúdos selecionados. A técnica de análise utilizada consistiu na leitura, seleção e organização dos materiais de acordo com sua relevância para o tema abordado (Santana; Narciso; Fernandes, 2025). Esse processo garantiu que o corpus da pesquisa refletisse uma visão ampla e atualizada sobre os principais desafios e soluções relacionados à segurança em ambientes IoT.

A coleta dos materiais foi realizada exclusivamente na base de dados CAPES Periódicos, um portal mantido pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, que oferece acesso a milhares de publicações científicas nacionais e internacionais, cobrindo diversas áreas do conhecimento. Essa base é amplamente reconhecida por sua credibilidade e por disponibilizar artigos revisados por pares, fator que assegura a qualidade das fontes utilizadas na pesquisa.

Na busca pelos textos, foram utilizadas palavras-chave simples, selecionadas a partir de termos recorrentes na literatura sobre o tema, combinadas de forma estratégica para ampliar a abrangência dos resultados. As expressões aplicadas incluíram: ‘segurança em IoT’, ‘inteligência artificial e IoT’, ‘percepção de risco urbano’, ‘cibersegurança em dispositivos inteligentes’ e ‘tecnologia e confiança social’. As combinações desses termos possibilitaram o refinamento da busca e o encontro de estudos que abordam as três dimensões centrais deste trabalho.

Como critérios de inclusão, consideraram-se materiais publicados entre 2020 e 2025, por representarem as discussões mais recentes sobre a temática. Também foram priorizados artigos disponíveis em texto completo, com abordagem analítica e foco em segurança digital, cidades inteligentes e inteligência artificial aplicada à IoT. Por outro lado, foram excluídas publicações que tratavam de aplicações industriais isoladas sem relação com o contexto urbano, estudos de natureza exclusivamente técnica sem interface com a segurança, e textos que não apresentavam fundamentação teórica sólida. Os critérios de inclusão e exclusão dos materiais seguiram parâmetros claros e objetivos (Santana; Narciso; Fernandes, 2025).

Portanto, a metodologia adotada nesta pesquisa possibilitou a construção de um panorama crítico e fundamentado sobre os desafios e potenciais das soluções IoT, articulando a literatura técnica com questões sociais, políticas e tecnológicas, o que contribuiu diretamente para o alcance dos objetivos propostos.

Revista ARACÊ
ISSN: 2358-2472

3 FRAGILIDADES TÉCNICAS NA SEGURANÇA DE DISPOSITIVOS IOT: AUTENTICAÇÃO, ATUALIZAÇÃO E INFRAESTRUTURA DE REDE

A segurança de dispositivos conectados à Internet das Coisas (IoT) enfrenta entraves decorrentes da arquitetura técnica desses sistemas. A fragmentação do ecossistema, marcada pela diversidade de plataformas, capacidades computacionais e protocolos de rede, impede a uniformização de práticas de autenticação. Segundo Sahu e Mazumdar (2024), a ausência de padrões amplamente aplicáveis permite que agentes mal-intencionados explorem lacunas básicas de segurança utilizando técnicas como *spoofing* e ataques de força bruta. Essa dificuldade é reiterada por Kołaczek (2025), ao observar que a interoperabilidade entre dispositivos e a inexistência de padrões universais de segurança tornam a superfície de ataque consideravelmente mais extensa. Tariq *et al.* (2023) complementam essa perspectiva ao ressaltar que, mesmo em sistemas com maior capacidade, a multiplicidade de fabricantes e a ausência de diretrizes comuns perpetuam um cenário de vulnerabilidade estrutural.

Além da diversidade técnica, o problema da autenticação é agravado pelas limitações dos dispositivos em termos de memória, energia e capacidade de processamento. Kołaczek (2025) indica que tais restrições inviabilizam a adoção de algoritmos criptográficos convencionais, comprometendo a verificação de identidade e a integridade das comunicações. Tariq *et al.* (2023) corroboram essa visão ao afirmar que dispositivos com suporte limitado frequentemente não conseguem operar com autenticação baseada em certificados, permanecendo expostos. Ainda conforme Sahu e Mazumdar (2024), a fragilidade da autenticação é particularmente crítica em redes mesh, nas quais a vulnerabilidade de um único nó compromete toda a estrutura.

Outra dimensão sensível refere-se à impossibilidade de garantir atualizações seguras e contínuas aos dispositivos. Muitos desses sistemas operam por anos com *firmware* obsoleto, mantendo falhas conhecidas que já dispõem de exploração automatizada. Para Sahu e Mazumdar (2024), a ausência de mecanismos criptograficamente validados para atualização representa um risco persistente em larga escala. Nesse sentido, Tariq *et al.* (2023) destacam a inviabilidade de coordenar atualizações em redes compostas por dispositivos heterogêneos e distribuídos, dado que os fabricantes nem sempre oferecem suporte pós-implantação. Kołaczek (2025) acrescenta que essa lacuna não se limita ao *software*, mas inclui também a inexistência de estratégias para distribuição segura de pacotes de correção.

Esse conjunto de limitações técnicas é amplificado por uma infraestrutura de rede frequentemente insegura. A conectividade baseada em redes domésticas ou tecnologias de baixo consumo energético, como *LoRaWAN*, opera sem criptografia robusta ou segmentação lógica. De acordo com Sahu e Mazumdar (2024), a ausência de *firewalls* embutidos facilita a interceptação e

Revista ARACÊ
ISSN: 2358-2472

modificação de pacotes, sobretudo em aplicações que envolvem dados sensíveis. Tariq *et al.* (2023) argumentam que, ao depender excessivamente da nuvem para o processamento, os dispositivos criam pontos únicos de falha que podem comprometer a disponibilidade da rede. Essa centralização dificulta, ainda, a implementação de políticas de mitigação distribuída.

Tais fatores estruturais comprometem também a resiliência dos dispositivos frente a ataques de negação de serviço. Os sistemas baseados em IoT possuem baixa tolerância a picos de tráfego e, em muitos casos, não dispõem de mecanismos de mitigação incorporados. Sahu e Mazumdar (2024) apontam que a inexistência de filtragem na camada de transporte permite que requisições mínimas causem instabilidade ou paralisação completa. Tariq *et al.* (2023) observam que, mesmo em contextos industriais, a falta de previsibilidade no tráfego e a ausência de segmentação dificultam a detecção de padrões anômalos que poderiam antecipar ataques.

É relevante considerar, ainda, a negligência com que a segurança é tratada nas fases iniciais do desenvolvimento de dispositivos IoT. Devido a restrições comerciais, como redução de custos e pressa no lançamento, os fabricantes frequentemente omitem camadas de proteção essenciais. Como exemplificam Tariq *et al.* (2023), é comum que dispositivos sejam implantados com senhas padrão ou interfaces expostas. Sahu e Mazumdar (2024) destacam que essa negligência é amplificada pela inexistência de auditoria regulatória no ciclo de vida do produto. A ausência de mecanismos de verificação pós-implantação perpetua vulnerabilidades mesmo em ambientes sensíveis, como os de controle urbano ou de saúde.

Nesse cenário, a falta de padronização dificulta não apenas a prevenção de incidentes, mas também a resposta coordenada a violações. Segundo Kołaczek (2025), mesmo em contextos que requerem monitoramento em tempo real, como redes descentralizadas, não há soluções adequadas para detecção rápida de anomalias sem comprometer a eficiência energética dos dispositivos. Essa limitação inviabiliza a adoção de modelos preditivos que demandam processamento contínuo. Além disso, a carência de dados rotulados e a ausência de integração entre sistemas de diferentes fornecedores dificultam a formação de ecossistemas de defesa automatizada.

Dessa forma, observa-se que o problema da segurança em dispositivos IoT não reside apenas na fragilidade isolada de componentes, mas na ausência de uma arquitetura segura desde o projeto até a operação. A seguir, Sahu e Mazumdar destacam:

> O ecossistema da IoT é altamente fragmentado, com dispositivos variados em termos de capacidade computacional, arquitetura de firmware e conectividade de rede. Essa heterogeneidade dificulta a aplicação uniforme de padrões de autenticação e cria lacunas exploráveis por invasores com técnicas simples, como spoofing ou brute-force attacks. (Sahu; Mazumdar, 2024, p. 2)

Revista ARACÊ
ISSN: 2358-2472

Portanto, torna-se evidente que a superação dessas limitações requer o estabelecimento de políticas técnicas integradas, que contemplem desde requisitos mínimos de segurança na fase de fabricação até mecanismos automatizados de atualização e mitigação. Contudo, enquanto persistirem incentivos econômicos que favorecem a negligência e a fragmentação, a segurança dos sistemas baseados em IoT permanecerá estruturalmente comprometida.

4 APLICAÇÕES DE INTELIGÊNCIA ARTIFICIAL NA DETECÇÃO DE AMEAÇAS EM AMBIENTES IOT

A crescente complexidade dos ambientes baseados em Internet das Coisas (IoT) tem demandado abordagens mais adaptativas e inteligentes para a detecção de ameaças cibernéticas. Nesse contexto, a aplicação de técnicas de inteligência artificial (IA) tem se consolidado como uma estratégia promissora, sobretudo em razão da capacidade de aprendizado e adaptação a padrões dinâmicos de tráfego de dados. Conforme destacado por Sahu e Mazumdar (2024), modelos como máquinas de vetores de suporte (SVM), redes neurais convolucionais e algoritmos baseados em árvores têm sido aplicados com êxito em ambientes de IoT, mesmo diante de dados ruidosos e desbalanceados. Kołaczek (2025) complementa essa análise ao observar que o volume contínuo de dados gerado pelos dispositivos oferece subsídios para o desenvolvimento de sistemas automáticos de detecção com base em aprendizado de máquina, o que amplia a capacidade de resposta a ataques.

Além disso, a IA tem demonstrado eficiência na antecipação de comportamentos maliciosos, superando as limitações de métodos baseados em assinaturas. Sahu e Mazumdar (2024) argumentam que algoritmos preditivos podem detectar variações sutis no comportamento dos dispositivos, emitindo alertas antes mesmo de que a ameaça seja consumada. Tariq *et al.* (2023) reforçam essa perspectiva ao salientar a capacidade dos modelos de IA de aprender com dados históricos para identificar ameaças futuras, o que é essencial em ecossistemas altamente voláteis. Entretanto, Kołaczek (2025) adverte que a eficácia desses sistemas depende, em grande parte, da disponibilidade de conjuntos de dados representativos e bem rotulados, os quais são escassos em muitas aplicações industriais.

Outro ponto discutido na literatura refere-se à arquitetura distribuída de detecção baseada em IA. Conforme observado por Sahu e Mazumdar (2024), a incorporação de modelos inteligentes em dispositivos de borda ou gateways reduz a latência e evita a sobrecarga de servidores centrais. Essa abordagem distribuída é também defendida por Tariq *et al.* (2023), que destacam a integração de modelos embarcados como forma de garantir monitoramento em tempo real e respostas imediatas às ameaças detectadas. No mesmo sentido, Kołaczek (2025) propõe a utilização de arquiteturas

Revista ARACÊ
ISSN: 2358-2472

hierárquicas do tipo borda–névoa–nuvem em combinação com aprendizado federado, a fim de equilibrar desempenho, consumo de recursos e preservação de privacidade.

Nesse cenário, destaca-se o Sistema Colaborativo de Detecção de Intrusões (CIDS), descrito por Kołaczek (2025), como uma alternativa viável à centralização excessiva. Esse sistema opera por meio de uma arquitetura federada, o que permite a detecção de intrusões com redução significativa de latência e tráfego de rede, sem comprometer a precisão. Tariq *et al.* (2023) também reconhecem o aprendizado federado como uma solução para as limitações impostas por políticas de privacidade, visto que os modelos são treinados localmente, sem a necessidade de transmissão de dados brutos. Tal característica é especialmente relevante em aplicações sensíveis, como monitoramento urbano ou de saúde.

Apesar dos benefícios, a literatura reconhece limitações importantes nas aplicações atuais de IA em IoT. De acordo com Tariq *et al.* (2023), ainda persistem desafios como a escassez de dados rotulados, o elevado custo computacional de treinamento dos modelos e a vulnerabilidade a ataques adversariais. Kołaczek (2025) enfatiza que, em dispositivos com recursos restritos, mesmo modelos leves de IA podem representar um consumo excessivo de energia e processamento. Sahu e Mazumdar (2024) também alertam que a detecção baseada em aprendizado depende de treinamento prévio consistente, o que nem sempre é viável em ambientes heterogêneos e descentralizados.

Nesse contexto, observa-se a aplicação de técnicas específicas de aprendizado profundo para lidar com fluxos contínuos de dados em tempo real. Segundo Sahu e Mazumdar (2024), redes neurais recorrentes e autoencoders têm apresentado desempenho satisfatório em ambientes com conectividade intermitente ou limitações arquiteturais severas. De forma semelhante, Tariq *et al.* (2023) observam que a IA é capaz de identificar padrões sutis que escapariam de métodos tradicionais baseados em regras, o que reforça sua aplicabilidade em situações de anomalias de baixo sinal. Entretanto, a efetividade dessas abordagens continua condicionada à qualidade dos dados de entrada.

O debate também se estende à questão da interoperabilidade entre os sistemas inteligentes de detecção e as demais camadas da infraestrutura IoT. Embora Kołaczek (2025) reconheça a utilidade de ferramentas como o banco de dados automatizado *VARIoT*, voltado ao mapeamento de vulnerabilidades, ainda persiste a dificuldade de integrar essas informações a sistemas de resposta autônomos. Essa limitação operacional é agravada pela heterogeneidade das plataformas, conforme discutido por Sahu e Mazumdar (2024), o que dificulta a atualização sincronizada de modelos de detecção e a coordenação entre diferentes nós da rede.

Revista ARACÊ
ISSN: 2358-2472

Nesse sentido, é pertinente observar que, embora os sistemas baseados em IA apresentem desempenho superior na identificação de ameaças, sua viabilidade depende de condições específicas de operação. A seguir, destaca-se uma citação direta representativa dessa limitação:

> Embora a IA ofereça vantagens significativas na detecção de ameaças em redes IoT, seu sucesso depende da disponibilidade de conjuntos de dados rotulados representativos, o que ainda constitui um obstáculo prático para a maioria das aplicações industriais (Sahu; Mazumdar, 2024, p. 12).

Dessa forma, infere-se que a IA, embora tecnicamente viável e eficaz, exige uma infraestrutura de suporte robusta e estratégias de treinamento contínuo para alcançar níveis aceitáveis de segurança. A ausência desses elementos compromete não apenas a capacidade de resposta, mas também a confiabilidade dos alertas gerados, sobretudo em aplicações críticas que exigem alta disponibilidade. Assim, o debate atual concentra-se menos na substituição de métodos tradicionais e mais na viabilidade operacional da inteligência artificial como componente integrado a uma estratégia ampla e adaptável de defesa cibernética em ambientes IoT.

5 TECNOLÓGICA E PERCEPÇÃO DE SEGURANÇA NA ADOÇÃO DE SOLUÇÕES IOT EM CONTEXTOS URBANOS

A adoção de tecnologias baseadas na Internet das Coisas (IoT) em ambientes urbanos está diretamente condicionada à percepção de segurança por parte dos cidadãos. Essa percepção não decorre apenas de características técnicas, mas é moldada por fatores sociopolíticos e institucionais que afetam a confiança pública. Conforme observado por Sahu e Mazumdar (2024), a utilização de sensores de vigilância, sistemas de mobilidade conectada e dispositivos urbanos inteligentes está condicionada à expectativa de que os dados gerados não serão expostos a usos indevidos, o que impõe exigências elevadas quanto à integridade e à transparência desses sistemas.

Adicionalmente, a ausência de comunicação clara e acessível sobre os mecanismos de proteção da informação pode gerar resistência à adoção, mesmo em cenários nos quais a segurança técnica é satisfatória. Para Sahu e Mazumdar (2024), a percepção de risco é, muitas vezes, mais determinante do que os indicadores objetivos de segurança. Nesse contexto, torna-se necessário considerar não apenas os aspectos técnicos das soluções IoT, mas também as estratégias de governança da informação, especialmente em iniciativas de cidade inteligente voltadas à coleta de dados sensíveis.

A esse respeito, Romani *et al.* (2023) observam que a aceitação pública de tecnologias digitais depende da coerência entre o discurso institucional e as práticas observadas. Em outras palavras, mesmo sistemas tecnicamente robustos podem ser rejeitados se forem percebidos como instrumentos

Revista ARACÊ
ISSN: 2358-2472

de controle, em especial quando não há mecanismos transparentes de prestação de contas. Essa posição é reforçada pelo argumento de que,

> [...] a aceitação de soluções inteligentes pelos cidadãos não depende apenas de seu desempenho técnico, mas da clareza com que seus propósitos são comunicados e da coerência entre discurso institucional e práticas observadas. Ambiguidades nesse processo comprometem a credibilidade das iniciativas (Romani *et al.*, 2023, p. 8).

Nesse sentido, Kołaczek (2025) introduz um elemento complementar ao debate ao enfatizar a dimensão emocional da resposta cidadã a incidentes de cibersegurança. Segundo o autor, dispositivos que integram o cotidiano doméstico, como câmeras inteligentes, provocam reações mais intensas quando violados, o que evidencia a relação direta entre segurança percebida e aceitação tecnológica. As implicações disso extrapolam o âmbito técnico, indicando que estratégias de proteção precisam considerar as reações afetivas da população e não apenas indicadores formais de desempenho.

A partir dessa perspectiva, Tariq *et al.* (2023) destacam que a confiança institucional exerce papel central na adesão a serviços públicos conectados. A ausência de regulamentações claras, associada à percepção de opacidade nos métodos de coleta e tratamento de dados, intensifica a desconfiança e desestimula o engajamento da população com soluções baseadas em IoT. Assim, a efetividade das políticas públicas digitais passa a depender não apenas do desenvolvimento tecnológico, mas da capacidade das instituições de assegurar legitimidade aos processos decisórios que envolvem tecnologia.

Por conseguinte, a implementação de dispositivos conectados em ambientes urbanos exige a articulação entre segurança técnica, arquitetura normativa e mecanismos de participação cidadã. Romani *et al.* (2023) identificam que a coprodução de políticas públicas digitais, com inclusão da sociedade civil nos processos deliberativos, fortalece a percepção de legitimidade e amplia a aceitação de soluções tecnológicas. A ausência desse tipo de engajamento, por outro lado, tende a alimentar o ceticismo e a rejeição, ainda que os sistemas ofereçam vantagens objetivas.

Em consonância com essa abordagem, Sahu e Mazumdar (2024) defendem a necessidade de políticas públicas orientadas por princípios de privacidade desde a concepção (*privacy by design*), combinadas com auditorias contínuas e estratégias de anonimização de dados. Tais mecanismos não apenas reforçam a proteção técnica, como também contribuem para a construção de confiança junto aos usuários. Contudo, sem ações coordenadas de comunicação institucional, esses avanços permanecem invisíveis para o público e ineficazes do ponto de vista social.

Além disso, a literatura revela que o desconhecimento sobre os protocolos de segurança implementados alimenta o temor de vigilância generalizada. Tariq *et al.* (2023) observam que esse

Revista ARACÊ
ISSN: 2358-2472

receio não se fundamenta apenas na possibilidade técnica de interceptação, mas na ausência de controle percebido pelos cidadãos quanto ao destino de seus dados. Para reverter esse cenário, os autores apontam para a necessidade de campanhas educativas, auditorias públicas e marcos regulatórios auditáveis.

Por fim, deve-se reconhecer que a confiabilidade das soluções IoT em contextos urbanos é uma construção sociotécnica, na qual as dimensões técnica, institucional e perceptiva se inter-relacionam. Romani *et al.* (2023) argumentam que a confiança da população não se limita ao dispositivo em si, mas envolve a trajetória histórica das relações entre cidadãos e instituições públicas. Portanto, a segurança em ambientes urbanos conectados requer, mais do que eficiência operacional, o reconhecimento da cidadania como elemento ativo na definição das tecnologias que impactam sua vida cotidiana.

6 RESULTADOS E DISCUSSÃO

Com base nos dados analisados e nas reflexões teóricas sustentadas pelos autores selecionados, os resultados do estudo indicam que a segurança na Internet das Coisas (IoT) não pode ser compreendida apenas sob a ótica técnica, mas exige uma abordagem multidimensional que envolva confiabilidade tecnológica, percepção social e políticas públicas inclusivas. Os três eixos analisados, fragilidades técnicas, aplicações de inteligência artificial (IA) na detecção de ameaças e confiabilidade percebida em contextos urbanos, demonstraram ser interdependentes e determinantes para a viabilidade das soluções baseadas em IoT.

Entre as principais conclusões, destaca-se que a fragmentação dos dispositivos e a ausência de padronização de protocolos agravam as falhas de autenticação, atualização e infraestrutura de rede, tornando os sistemas IoT altamente vulneráveis. Isso compromete sua escalabilidade e dificulta a adoção em ambientes urbanos críticos. Autores como Sahu e Mazumdar (2024), Kołaczek (2025) e Tariq *et al.* (2023) confirmam que os dispositivos de IoT, quando operando com firmware obsoleto ou expostos a redes não seguras, representam uma ameaça estrutural ao ecossistema digital. Além disso, as soluções tradicionais de segurança não se mostram compatíveis com as limitações computacionais dos dispositivos, o que reforça a urgência de métodos adaptativos e eficientes.

Outro resultado relevante foi a confirmação da eficácia das aplicações de inteligência artificial na detecção de ameaças. A utilização de modelos de aprendizado de máquina distribuído, como aprendizado federado e autoencoders, mostrou-se promissora para operar em tempo real e com menor dependência da nuvem. No entanto, os autores apontam obstáculos práticos relacionados à carência de bases de dados rotuladas e ao alto custo computacional. A literatura revisada também demonstra que,

Revista ARACÊ
ISSN: 2358-2472

apesar de tais limitações, a IA representa uma alternativa superior aos métodos baseados em assinaturas estáticas, sobretudo em ambientes heterogêneos e dinâmicos como os da IoT.

Adicionalmente, os resultados revelam que a percepção de segurança por parte dos cidadãos é tão importante quanto os aspectos técnicos. Em cenários urbanos, a aceitação das tecnologias de IoT depende fortemente da transparência institucional, da clareza nos propósitos das soluções e da existência de canais participativos para o público. A desconfiança social e a falta de controle percebido sobre o uso de dados são apontadas na literatura como obstáculos à adesão, mesmo quando os sistemas oferecem benefícios tangíveis. Isso confirma que a segurança é uma construção sociotécnica, que envolve a interação entre o design tecnológico e os marcos regulatórios que sustentam sua legitimidade.

Contudo, é importante destacar as limitações das descobertas. A maior parte das evidências presentes nos estudos analisados provêm de modelos teóricos e simulações em ambientes controlados. Como apontado por Kołaczek (2025), a implementação de soluções baseadas em IA em dispositivos de baixa capacidade computacional ainda enfrenta desafios operacionais significativos. Além disso, os estudos revisados concentram-se majoritariamente em cenários urbanos de países desenvolvidos, o que limita a generalização dos achados para contextos de infraestrutura precária ou regulação instável.

Alguns resultados inesperados também merecem atenção. Apesar da suposição de que a sofisticação tecnológica garantiria maior aceitação social, observou-se que dispositivos mais avançados, como câmeras inteligentes, geram maior rejeição quando associados a riscos de privacidade. Isso sugere que o fator emocional e subjetivo tem peso considerável na percepção de segurança, como já sugerido por Romani *et al.* (2023). Esse aspecto, muitas vezes negligenciado, impõe a necessidade de estratégias de comunicação e educação digital alinhadas ao contexto cultural dos usuários.

Diante dessas evidências, recomenda-se que pesquisas futuras aprofundem a relação entre segurança percebida e design institucional das tecnologias, especialmente em regiões onde a confiança nas instituições públicas é historicamente frágil. Também se sugere o desenvolvimento de estudos empíricos sobre a efetividade de soluções baseadas em IA em dispositivos de IoT operando em ambientes reais, com restrições de largura de banda e energia. Por fim, é fundamental que as próximas investigações priorizem abordagens interdisciplinares, unindo engenharias, ciências sociais e direito, para tratar a segurança da IoT como um problema integrado que transcende a dimensão técnica.

Revista ARACÊ
ISSN: 2358-2472

7 CONCLUSÃO

As considerações finais deste estudo reforçam a relevância da análise integrada sobre a segurança na Internet das Coisas (IoT), especialmente em contextos urbanos. A pesquisa permitiu responder de forma clara às questões levantadas na introdução e aprofundadas na metodologia, que buscavam compreender quais são as fragilidades técnicas dos dispositivos IoT, como a inteligência artificial pode contribuir para a detecção de ameaças nesses ambientes e de que maneira a percepção de segurança influencia a adoção dessas tecnologias por parte da sociedade.

Os objetivos propostos foram plenamente alcançados. O primeiro objetivo, relacionado à identificação das vulnerabilidades técnicas na infraestrutura de IoT — como falhas de autenticação, ausência de atualizações seguras e redes expostas — foi abordado a partir de uma análise teórica fundamentada, que evidenciou o impacto direto desses fatores na segurança dos sistemas. O segundo objetivo, que tratava da aplicação de técnicas de inteligência artificial para mitigar riscos em tempo real, foi igualmente respondido ao demonstrar-se que modelos de aprendizado de máquina, especialmente quando utilizados em arquiteturas distribuídas, oferecem soluções promissoras, ainda que enfrentem desafios de implementação e limitação de dados. O terceiro objetivo, voltado à análise da confiabilidade tecnológica e percepção social da segurança em ambientes urbanos, destacou a importância da confiança institucional, da transparência e do engajamento cidadão na viabilidade de políticas públicas baseadas em IoT.

Como conclusão geral, verificou-se que a segurança na IoT não pode ser tratada exclusivamente como uma questão técnica. Ela depende da integração entre inovação tecnológica, desenho regulatório e aceitação social. Dispositivos inseguros, por mais avançados que sejam, tendem a ser rejeitados quando associados à exposição de dados pessoais ou ao risco de vigilância injustificada. Portanto, a confiança do usuário final é um componente estratégico para o sucesso de qualquer iniciativa baseada nessa tecnologia.

Dentre as lacunas identificadas, destaca-se a ausência de estudos empíricos que considerem ambientes com infraestrutura limitada, bem como a carência de abordagens interdisciplinares que envolvam engenharia, ciências sociais e direito. Sugere-se, assim, que pesquisas futuras explorem contextos mais diversos e realistas, testando soluções de segurança em dispositivos de baixa capacidade computacional, além de investigar a efetividade de campanhas de conscientização sobre o uso responsável da IoT. Estudos longitudinais também seriam bem-vindos, a fim de observar como a percepção de segurança evolui ao longo do tempo e influencia a aceitação tecnológica em diferentes perfis sociais e geográficos.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

KOŁACZEK, G. Tecnologias da Internet das Coisas (IoT) na cibersegurança: desafios e oportunidades. **Applied Sciences**, v. 15, n. 8, p. 1-5, 2025.

ROMANI, G. F.; PINOCHET, L. H. C.; PARDIM, V. I.; SOUZA, C. A. de. A segurança como fator-chave para a cidade inteligente: a confiança dos cidadãos e o uso de tecnologias. **Revista de Administração Pública**, v. 57, n. 2, p. e2022-0145,2023.

SAHU, S. K.; MAZUMDAR, K. Explorando ameaças de segurança e técnicas de soluções para a Internet das Coisas (IoT): das vulnerabilidades à vigilância. **Frontiers in Artificial Intelligence**, v. 7, p. 1-16, 2024.

SANTANA, A. C. A.; NARCISO, R.; FERNANDES, A. B. Explorando as metodologias científicas: tipos de pesquisa, abordagens e aplicações práticas. **Caderno Pedagógico**, v. 22, n. 1, e13333, 2025.

TARIQ, U.; AHMED, I.; BASHIR, A. K.; SHAUKAT, K. Uma análise crítica da segurança cibernética e futuras direções de pesquisa para a Internet das Coisas: uma revisão abrangente. **Sensors**, v. 23, n. 8, p. 4117, 2023.