REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

VULNERABILIDADES DE SEGURANÇA NOS SISTEMAS IOT DURANTE A TRANSIÇÃO PARA REDES 5G/6G: DESAFIOS E SOLUÇÕES TECNOLÓGICAS

SECURITY VULNERABILITIES IN IOT SYSTEMS DURING THE TRANSITION TO 5G/6G NETWORKS: CHALLENGES AND TECHNOLOGICAL SOLUTIONS

VULNERABILIDADES DE SEGURIDAD EN SISTEMAS IOT DURANTE LA TRANSICIÓN A REDES 5G/6G: RETOS Y SOLUCIONES TECNOLÓGICAS

Gabriel Victor Rodrigues Cardoso[1], Jhennifer Santana Moura[1], Diego Santos Almeida Pinto[2]

e6106908
https://doi.org/10.47820/recima21.v6i10.6908

PUBLICADO: 10/2025

RESUMO

A presente pesquisa bibliográfica explora o contexto da Internet das Coisas (IoT) e a sua relação crítica com a segurança cibernética em face da evolução das tecnologias de comunicação móvel para as redes 5G e 6G. O objetivo é analisar como a implementação de soluções IoT, aproveitando a latência ultrabaixa e a densidade de conexão do 5G/6G, amplifica as vulnerabilidades de segurança inerentes a esses dispositivos, como ataques de *Root-of-Trust* comprometido e ataques de negação de serviço distribuído (DDoS) em larga escala. Observa-se que, apesar do potencial de inovação em serviços críticos (e.g., telemedicina), a adoção segura enfrenta barreiras significativas, como a necessidade de investimentos em infraestrutura de segurança de borda, a escassez de talentos especializados e a gestão de questões éticas e de privacidade de dados em ambientes massivamente interconectados. Este trabalho busca identificar os principais desafios competitivos e de resiliência proporcionados pela convergência IoT-5G/6G e as questões críticas que os líderes de tecnologia precisam superar. A metodologia empregada é a revisão bibliográfica, utilizando artigos científicos, relatórios de mercado e obras especializadas para fundamentar a análise do panorama atual e futuro. Conclui-se que a segurança *end-to-end* proativa é um vetor indispensável para a confiança e competitividade, exigindo das empresas não apenas investimento tecnológico em soluções como Inteligência Artificial (IA) para detecção de anomalias e *Blockchain* para imutabilidade de dados, mas também uma profunda mudança cultural e estratégica focada em governança.

PALAVRAS-CHAVE: Internet das Coisas (IoT). Segurança Cibernética. Redes 5G/6G. Vulnerabilidades. Governança Ética.

ABSTRACT

This bibliographic research explores the context of the Internet of Things (IoT) and its critical relationship with cybersecurity in the face of the evolution of mobile communication technologies towards 5G and 6G networks. The objective is to analyze how the implementation of IoT solutions, leveraging the ultra- low latency and connection density of 5G/6G, amplifies the security vulnerabilities inherent in these devices, such as compromised Root-of-Trust attacks and large-scale Distributed Denial of Service (DDoS) attacks. It is observed that, despite the potential for service innovation in critical services (e.g., telemedicine), secure adoption faces significant barriers, such as the need for investment in edge security infrastructure, the scarcity of specialized talents, and the management of ethical and data privacy issues in massively interconnected environments. This work seeks to identify the main competitive and resilience challenges provided by the IoT-5G/6G convergence and the critical challenges that technology leaders must overcome. The methodology employed is a bibliographic review, using scientific articles, market reports, and

[1] Acadêmico (a) cursando 4° período de Gestão da Tecnologia da Informação no Centro Universitário de Goiatuba.

[2] Orientador: Professor do curso de Gestão da Tecnologia da Informação no Centro Universitário de Goiatuba

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

specialized literature to support the analysis of the current and future landscape. It is concluded that proactive end-to-end security is an indispensable vector for trust and competitiveness, requiring companies not only technological investment in solutions like Artificial Intelligence (AI) for anomaly detection and Blockchain for data immutability, but also a profound cultural and strategic shift focused on governance.

KEYWORDS: *Internet of Things (IoT). Cybersecurity. 5G/6G Networks. Vulnerabilities. Ethical Governance.*

RESUMEN
La presente investigación bibliográfica explora el contexto del Internet de las Cosas (IoT) y su relación crítica con la ciberseguridad ante la evolución de las tecnologías de comunicación móvil hacia las redes 5G y 6G. El objetivo es analizar cómo la implementación de soluciones de IoT, aprovechando la latencia ultrabaja y la densidad de conexión del 5G/6G, amplifica las vulnerabilidades de seguridad inherentes a estos dispositivos, como ataques de Root-of-Trust comprometido y ataques de denegación de servicio distribuido (DDoS) a gran escala. Se observa que, a pesar del potencial de innovación en servicios críticos (e.g., telemedicina), la adopción segura enfrenta barreras significativas, como la necesidad de inversiones en infraestructura de seguridad de borde, la escasez de talentos especializados y la gestión de cuestiones éticas y de privacidad de datos en entornos masivamente interconectados. Este trabajo busca identificar los principales desafíos competitivos y de resiliencia proporcionados por la convergencia IoT-5G/6G y los desafíos críticos que los líderes de tecnología deben superar. La metodología utilizada es la revisión bibliográfica, empleando artículos científicos, informes de mercado y obras especializadas para respaldar el análisis del panorama actual y futuro. Se concluye que la seguridad proactiva end-to-end es un vector indispensable para la confianza y la competitividad, que exige a las empresas no solo inversión tecnológica en soluciones como Inteligencia Artificial (IA) para detección de anomalías y Blockchain para inmutabilidad de datos, sino también un profundo cambio cultural y estratégico enfocado en la gobernanza.

PALABRAS CLAVE*: Internet de las Cosas (IoT). Ciberseguridad. Redes 5G/6G. Vulnerabilidades. Gobernanza Ética.*

INTRODUÇÃO

A Internet Das Coisas (IoT) transcendeu a esfera da conectividade básica e se consolidou como um imperativo estratégico, assumindo o papel de principal catalisadora da próxima onda de transformação digital, impulsionada pelas redes 5G e 6G. Sua capacidade de processamento distribuído na borda (*Edge Computing*) de automação cognitiva e a promessa de interconexão massiva (mMTC) confere-lhe um potencial disruptivo na otimização de processos e na geração de novos modelos de negócios. Não é meramente um diferencial: a adoção estratégica da IoT em redes avançadas se tornou uma condição *sine qua non* para a manutenção da competitividade em um mercado global cada vez mais volátil e demandante.

A crescente e complexa integração de bilhões de dispositivos IoT em diversas operações corporativas e civis, abrangendo desde o *front-office* (monitoramento remoto e cidades inteligentes) até o *back-office* (gestão de *supply chain* automatizada e manutenção preditiva), impõe um debate rigoroso sobre sua real segurança, seus benefícios sistêmicos e os obstáculos estruturais que as organizações precisam superar. A expansão exponencial da

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

superfície de ataque e a limitação de recursos de *hardware* dos dispositivos de borda tornam vulnerabilidades simples em ameaças de grande escala, especialmente sob as exigências de latência ultrabaixa do 5G.

Este é o problema da pesquisa: Como as características arquiteturais das redes 5G/6G, como a latência ultrabaixa e a densidade de conexão, exacerbam as vulnerabilidades de segurança inerentes aos sistemas IoT, e qual é a natureza dos desafios éticos, tecnológicos e humanos que configuram as principais barreiras à sua adoção plena e sustentável?

O objetivo geral deste trabalho é conduzir uma análise aprofundada das vulnerabilidades de segurança cibernética e dos desafios da implementação de sistemas IoT em ambientes 5G/6G, e, a partir dessa análise crítica, propor um conjunto robusto de estratégias e práticas tecnológicas para uma adoção que seja eticamente responsável, tecnologicamente viável e sustentavelmente segura.

Os objetivos específicos são: (1) identificar e detalhar os principais vetores de ataque e as vulnerabilidades de segurança que são intensificados pela latência ultrabaixa e pelo *Massive Machine Type Communication* (mMTC) das redes 5G/6G; (2) mapear os desafios mais comuns enfrentados pelas organizações na adoção de segurança para IoT-5G/6G, como a fragmentação de padrões, a limitação de recursos de dispositivos *edge* e as complexas implicações éticas ligadas à privacidade massiva de dados; e (3) propor um roteiro com estratégias e melhores práticas, desenhado para guiar gestores e líderes na implementação sustentável da segurança, com foco em tecnologias como IA e *Blockchain*.

A justificativa principal do estudo reside na sua relevância empírica e na urgência acadêmica em prover diretrizes claras. A ausência de um plano estratégico bem articulado para essa transição tecnológica pode levar a ataques de *ransomware* em larga escala e ao comprometimento de infraestruturas críticas, impactando negativamente a produtividade, a eficiência e, em última instância, a segurança nacional. O estudo visa preencher essa lacuna, oferecendo uma análise detalhada e balizada na literatura para uma implementação de IoT que seja segura e sustentável a longo prazo.

1. REFERENCIAL TEÓRICO

A integração da Internet das Coisas (IoT) com as redes móveis de quinta e sexta geração (5G/6G) simboliza uma revolução na infraestrutura digital global, transformando o modo como dados são produzidos, processados e protegidos. O conceito de IoT, originalmente formulado por Ashton (2009), evoluiu de simples sensores conectados para ecossistemas ciberfísicos complexos, em que dispositivos inteligentes operam de forma autônoma e colaborativa.

Com o 5G, caracterizado pela latência ultrabaixa, alta confiabilidade e densidade massiva de conexões (mMTC), a IoT passou a abranger aplicações críticas, como cidades inteligentes, *e-*

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

health, manufatura 4.0 e veículos autônomos (Yin *et al.,* 2020). Já o 6G, previsto para a próxima década, promete uma integração ainda mais profunda entre redes e inteligência artificial, com suporte a comunicações táteis e cognitivas (*tactile internet*), expandindo tanto as oportunidades quanto os riscos de segurança (Shafi *et al.,* 2020).

Sob essa ótica, a IoT deixa de ser apenas uma ferramenta de automação e torna-se a espinha dorsal da transformação digital, redefinindo modelos de negócio, cadeias produtivas e até a gestão pública. Contudo, a ampliação da superfície de ataque — ocasionada pela interconexão de bilhões de dispositivos com recursos limitados de processamento e criptografia — expõe vulnerabilidades estruturais que desafiam os paradigmas tradicionais de cibersegurança (Boussaha *et al.,* 2023). Essas vulnerabilidades se intensificam no 5G/6G devido ao uso de virtualização, fatiamento de rede (*network slicing*), e computação de borda (*Edge Computing*), que redistribuem a segurança de forma descentralizada, tornando-a mais difícil de controlar. A literatura contemporânea reforça que a evolução tecnológica não pode ser dissociada de uma visão ética e social. A governança da IoT precisa considerar os impactos sobre a privacidade, a autonomia e a confiança digital, conforme argumentam Ziegeldorf, Morchon e Wehrle (2014), que enfatizam o risco de "vigilância ubíqua" em sistemas interconectados.

A proteção de dados, nesse contexto, não é apenas uma questão técnica, mas de legitimidade social, especialmente sob a égide da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que impõe princípios de transparência, finalidade e segurança no tratamento automatizado de informações. Portanto, o referencial teórico deve ser compreendido como um eixo triplo que articula tecnologia, segurança e ética, onde o sucesso da IoT em redes 5G/6G depende tanto da robustez das soluções técnicas quanto da maturidade ética e regulatória de quem as implementa.

1.1. Benefícios da Segurança Proativa no Contexto Empresarial

A segurança proativa em sistemas IoT integrados às redes 5G/6G não é apenas uma prática preventiva, mas uma vantagem competitiva e estratégica. Segundo Davenport e Ronanki (2018), as empresas que adotam inteligência artificial (IA) para automação de processos e defesa cibernética conseguem reduzir o tempo médio de resposta a incidentes e elevar a confiabilidade dos serviços.

A aplicação de algoritmos de aprendizado de máquina e *deep learning* na detecção de anomalias permite identificar padrões invisíveis à análise humana, tornando possível antecipar ataques cibernéticos antes que causem danos reais. O uso de IA e *Big Data Analytics* em ambientes corporativos conectados potencializa a eficiência operacional e reduz custos de manutenção. Por exemplo, a IBM (2023) demonstrou em estudos de caso que empresas que integraram IA à segurança de IoT reduziram em até 44% o tempo de detecção de ameaças.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Além disso, a automação da ciberdefesa permite que as equipes humanas se concentrem em tarefas estratégicas, como análise de risco e desenvolvimento de políticas de governança. Essa abordagem reforça a tese de que a segurança baseada em dados é um ativo de inovação — não um custo.

Outro benefício fundamental é o aumento da resiliência cibernética. Com o uso de *Edge Computing*, é possível processar dados próximos à origem, reduzindo latência e tornando a resposta a incidentes mais ágil e descentralizada. A descentralização também favorece a continuidade dos serviços mesmo em caso de falha parcial da rede. Segundo Al-Garadi *et al.* (2018), arquiteturas de segurança distribuída são essenciais para ambientes com alta densidade de dispositivos, pois reduzem o impacto de ataques de negação de serviço (DDoS). Além dos ganhos técnicos e financeiros, há o fortalecimento da confiança digital — um dos pilares da economia de dados.

Consumidores e parceiros tendem a preferir empresas que demonstram comprometimento com a segurança e a privacidade, criando uma vantagem reputacional sustentável. Andrews, Cherian e Mady (2022) argumentam que o *Blockchain*, ao oferecer rastreabilidade e imutabilidade das transações, amplia a confiança entre as partes e reduz fraudes em ecossistemas IoT. Assim, segurança proativa não é apenas defesa: é uma estratégia de crescimento e fidelização.

1.2. Desafios na Implementação da Segurança para IoT-5G/6G nas Organizações

Apesar das vantagens, a implementação da segurança em ambientes IoT-5G/6G enfrenta desafios multidimensionais — técnicos, humanos e econômicos. O primeiro obstáculo é a heterogeneidade dos dispositivos e protocolos, que dificulta a padronização de mecanismos de proteção. Muitos dispositivos IoT operam com sistemas embarcados simples, sem recursos suficientes para criptografia avançada, autenticação multifator ou atualizações *OTA* (*Over-the-Air*). Essa limitação cria pontos vulneráveis na arquitetura, frequentemente explorados por atacantes em cadeias de suprimento (Yin *et al.,* 2020).

Outro desafio relevante é o alto custo de infraestrutura de segurança. Implementar *network slicing*, virtualização e criptografia pós-quântica requer investimentos significativos em *hardware*, licenciamento e especialistas. Pequenas e médias empresas são as mais afetadas, o que aprofunda o fosso digital e compromete a democratização da segurança (Enisa, 2024).

A escassez de talentos especializados é igualmente crítica. Segundo relatório da *Cybersecurity Ventures* (2023), há um *déficit* global estimado de 3,5 milhões de profissionais em cibersegurança, número que tende a crescer com a expansão da IoT. Essa falta de especialistas impede a consolidação de estratégias robustas de proteção. Brynjolfsson e McAfee (2014) já destacavam que a automação massiva exige um redesenho da força de trabalho, com foco em *reskilling* e *upskilling* contínuos.

ISSN: 2675-6218 - RECIMA21
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

Além dos fatores técnicos e humanos, há desafios éticos e regulatórios. O tratamento massivo de dados sensíveis em IoT — especialmente em setores como saúde e transporte — levanta questões de privacidade e discriminação algorítmica. Modelos de IA mal treinados podem reproduzir vieses, comprometendo decisões automatizadas (como bloqueio de acessos ou priorização de tráfego). Essa problemática é amplamente discutida por Mittelstadt *et al.*, (2016), que defendem que a IA aplicada à segurança deve seguir princípios de *Explainability* e *Fairness* para garantir legitimidade e conformidade com legislações como a LGPD e a GDPR.

1.3. Estratégias para uma Adoção de Segurança Sustentável

Diante desses desafios, torna-se essencial adotar estratégias evolutivas e sustentáveis para consolidar a segurança em ecossistemas IoT-5G/6G. O primeiro passo é a criação de arquiteturas de segurança orientadas ao risco, que priorizem ativos críticos e implementem controles proporcionais à exposição. *Frameworks* como o NIST *Cybersecurity Framework* (2020) e a ISO/IEC 27001 servem como base para estabelecer políticas e métricas de maturidade cibernética. A integração de *DevSecOps* é uma das abordagens mais promissoras, pois insere a segurança desde o início do ciclo de desenvolvimento, promovendo automação, auditoria contínua e correções ágeis.

Essa prática reduz falhas em produção e permite que equipes de desenvolvimento e segurança atuem de forma colaborativa (IBM, 2023). A capacitação humana é outro eixo central. Programas de *reskilling* e *upskilling* precisam ser incorporados às estratégias de segurança, capacitando profissionais para operar soluções de IA, analisar anomalias e compreender os limites éticos do uso de dados. Davenport e Kirby (2020) ressaltam que o futuro da segurança dependerá da combinação entre competências técnicas e pensamento crítico, pois a tecnologia sozinha não garante proteção integral.

Por fim, a sustentabilidade da segurança em IoT requer uma governança ética e transparente. Isso implica em desenhar algoritmos explicáveis, auditáveis e livres de viés, além de implementar *Privacy by Design* em todos os níveis do sistema. Conforme Radanliev *et al.,* (2022), o futuro das redes 6G demandará “segurança cognitiva”, baseada em IA autônoma capaz de aprender padrões comportamentais e responder de forma preditiva a ameaças, mas sempre dentro de limites éticos e regulatórios claros.

Assim, a segurança sustentável deve ser entendida como um processo contínuo, dinâmico e interdisciplinar — uma integração entre tecnologia, pessoas e valores.

2. MÉTODOS

A metodologia adotada nesta pesquisa foi delineada a partir de uma abordagem qualitativa, exploratória e descritiva, sustentada pelo método de Revisão Bibliográfica

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

Sistematizada. A escolha dessa abordagem se justifica pelo caráter recente e dinâmico do tema — a segurança em sistemas IoT durante a transição para as redes 5G e 6G —, um campo em constante transformação, onde as evidências empíricas ainda estão em construção. De acordo com Gil (2019), a pesquisa exploratória é a mais adequada quando o objetivo é compreender fenômenos complexos e emergentes, nos quais as variáveis ainda não estão claramente definidas, sendo essencial para a formulação de hipóteses e o aprofundamento teórico.

Para consolidar o referencial e estruturar a análise, esta investigação foi dividida em três fases metodológicas interdependentes.

A primeira fase consistiu na identificação e seleção das fontes. Foi realizada uma busca sistemática em bases acadêmicas de alto impacto, incluindo *IEEE Xplore, ScienceDirect, Scopus, SpringerLink* e *ACM Digital Library*, além de documentos técnicos de órgãos internacionais, como ENISA (*European Union Agency for Cybersecurity*), ITU (*International Telecommunication Union*) e NIST (*National Institute of Standards and Technology*). Foram utilizados descritores em português e inglês, tais como "*IoT security*", "*5G vulnerabilities*", "*6G architecture*", "*cybersecurity governance*", "*AI ethics*" e "*blockchain IoT*". Essa etapa seguiu os princípios da metodologia PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), a fim de garantir rastreabilidade e transparência na seleção do material.

A segunda fase compreendeu a avaliação crítica e categorização das fontes. Os artigos e relatórios foram filtrados conforme critérios de relevância científica, atualidade (2018–2024), impacto de citação e aderência temática ao objeto de estudo. Ao todo, foram identificadas 126 publicações, das quais 58 atenderam aos critérios de inclusão. Cada fonte foi analisada segundo sua contribuição para quatro dimensões: (1) conceitos fundamentais de IoT e redes 5G/6G; (2) vulnerabilidades e vetores de ataque; (3) estratégias tecnológicas de mitigação, como IA, *Blockchain* e *Edge Computing*; e (4) aspectos éticos, regulatórios e de governança. Essa categorização permitiu a construção de um panorama teórico consistente e multidimensional, alinhado à complexidade do tema.

Na terceira fase, realizou-se uma análise de conteúdo, conforme a metodologia de Bardin (2016), voltada à interpretação qualitativa dos dados textuais. Essa técnica possibilitou a identificação de padrões discursivos e tendências temáticas recorrentes entre os autores. As informações extraídas foram sintetizadas e organizadas em eixos analíticos, que serviram de base para o desenvolvimento das seções "Resultados e Discussão" e "Considerações Finais".

A análise de conteúdo, nesse contexto, foi crucial para transcender o simples levantamento de informações, permitindo compreender como a literatura articula as relações entre tecnologia, segurança, ética e governança na IoT.

A natureza qualitativa do estudo reflete a preocupação em compreender o fenômeno da segurança digital de forma interpretativa, e não meramente estatística.

ISSN: 2675-6218 - RECIMA21
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

De acordo com Flick (2020), a pesquisa qualitativa busca interpretar significados e contextos sociais, o que se alinha à proposta deste trabalho ao tratar de dimensões éticas, humanas e organizacionais da adoção da IoT em redes avançadas. Complementarmente, a pesquisa apresenta um caráter descritivo, pois visa registrar, analisar e interpretar o estado atual da arte, sem manipular variáveis ou interferir empiricamente nos fenômenos observados.

Outro ponto metodológico importante é a triangulação das fontes. Para garantir maior validade e confiabilidade dos resultados, a análise cruzou evidências provenientes de estudos acadêmicos, relatórios técnicos e estudos de caso secundários. Essa triangulação seguiu o modelo proposto por Denzin (2017), que defende o uso de múltiplas perspectivas para ampliar a consistência das interpretações. Foram consultados, por exemplo, relatórios da Huawei (2023), Ericsson (2023) e IBM (2023), que documentam implementações reais de segurança distribuída e uso de IA em ambientes 5G corporativos.

Além disso, foi aplicado um método dedutivo-indutivo, partindo da análise teórica dos conceitos(dedutivo) para a inferência de tendências e práticas (indutivo). Assim, a revisão não se limitou à descrição da literatura, mas buscou compreender como as teorias se traduzem em estratégias práticas de mitigação de riscos e como estas são condicionadas por fatores técnicos e humanos.

A validação científica da metodologia adotada foi garantida por três elementos: (1) o uso de fontes reconhecidas e revisadas por pares; (2) a análise sistemática e categorizada das informações; e (3) o alinhamento com metodologias aceitas pela comunidade acadêmica internacional, como PRISMA e Bardin. A preocupação com a replicabilidade e rastreabilidade das etapas visa conferir transparência e rigor à pesquisa, permitindo que outros pesquisadores reproduzam o processo em contextos similares.

Por fim, a metodologia incorpora uma perspectiva ético-reflexiva, considerando a necessidade de alinhar a pesquisa científica à responsabilidade social no uso de tecnologias emergentes. Isso inclui a observância das diretrizes da LGPD (Lei nº 13.709/2018) e dos princípios de *Responsible Research and Innovation* (RRI) que preconizam a integração entre inovação tecnológica e impacto humano. Tal perspectiva é especialmente relevante em estudos sobre IoT, onde o processamento massivo de dados pode afetar direitos fundamentais à privacidade e à segurança informacional. Assim, a metodologia aqui empregada não se limita à Revisão de Literatura, mas constitui um instrumento de análise crítica, capaz de identificar lacunas, sintetizar contribuições e apontar caminhos para o desenvolvimento de soluções sustentáveis de segurança em sistemas IoT nas redes 5G e 6G.

3. RESULTADOS E DISCUSSÃO

A partir da Revisão Bibliográfica Sistematizada e da análise de conteúdo conduzida, os

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

resultados deste estudo revelam um panorama complexo e multifacetado da segurança em sistemas IoT no contexto das redes 5G e 6G. A literatura converge em um ponto essencial: a segurança deixou de ser um elemento complementar da infraestrutura digital para se tornar o núcleo estratégico da transformação tecnológica. A integração de IoT, 5G e futuramente 6G cria um ecossistema hiperconectado em que bilhões de dispositivos trocam dados sensíveis em tempo real, tornando a confiança e a resiliência operacional, ativos críticos de valor empresarial e nacional.

Os resultados apontam que as organizações que adotam segurança proativa e distribuída alcançam maior estabilidade e vantagem competitiva. Isso ocorre porque a segurança em tempo real, sustentada por inteligência artificial (IA) e aprendizado de máquina, é capaz de detectar anomalias com precisão crescente.

Em estudos conduzidos por Al-Garadi *et al.* (2018) e confirmados por o relatório *AI-Driven Threat Detection* (IBM, 2023), algoritmos de *deep learning* reduziram o tempo médio de resposta a incidentes de 17 horas para menos de 20 minutos em ambientes industriais conectados. Essa redução de latência operacional não apenas evita perdas financeiras, mas também assegura continuidade em serviços críticos, como telemedicina e transporte autônomo.

Um dos eixos centrais observados é o da resiliência cibernética, que se consolida como a principal métrica de maturidade digital. A literatura recente, representada por Boussaha *et al.,* (2023), argumenta que a capacidade de uma rede de isolar ataques, manter sua integridade e se recuperar rapidamente é o novo diferencial competitivo. No contexto de 5G/6G, essa resiliência é viabilizada por arquiteturas descentralizadas e pela adoção do paradigma *Zero Trust*, em que cada dispositivo e cada requisição devem ser autenticados continuamente. Essa abordagem, impulsionada pelo uso de *Edge Computing* e *Blockchain*, substitui o modelo tradicional de perímetro, ampliando a segurança mesmo em redes fragmentadas e geograficamente dispersas.

A aplicação de *Blockchain* é especialmente relevante nos resultados da pesquisa. Diversos autores (Andrews; Cherian; Mady, 2022; Wang *et al.,* 2023) destacam que a imutabilidade e a rastreabilidade dessa tecnologia proporcionam uma camada adicional de integridade e auditoria aos sistemas IoT. Por exemplo, em cadeias logísticas inteligentes, o *Blockchain* garante que, cada etapa de transporte ou produção seja autenticada e registrada de forma descentralizada, prevenindo adulterações e aumentando a confiabilidade dos dados.

No entanto, o desafio está na escalabilidade — a sobrecarga de energia e o tempo de processamento ainda limitam sua aplicação em dispositivos de borda com recursos restritos, exigindo o desenvolvimento de soluções híbridas que combinem eficiência e segurança.

Outro resultado expressivo refere-se ao descompasso entre a sofisticação tecnológica e a capacitação humana. A literatura é unânime ao reconhecer que a falta de profissionais especializados constitui uma barreira estrutural à implementação eficaz da segurança em IoT-

ISSN: 2675-6218 - RECIMA21
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

5G/6G. A Enisa (2024) destaca que a Europa e a América Latina enfrentam *déficits* de até 30% em talentos de cibersegurança, principalmente em áreas críticas como criptografia pós-quântica, análise forense e *DevSecOps*. Esse *déficit* leva muitas organizações a dependerem de soluções automatizadas de IA, que, embora eficientes, também podem introduzir riscos éticos, como a falta de explicabilidade nas decisões.

O papel da governança ética emerge, então, como um dos principais resultados e temas de discussão. A IA aplicada à segurança pode reproduzir vieses de dados ou bloquear acessos de forma discriminatória se treinada com conjuntos enviesados. Mittelstadt *et al.,* (2016) defendem que a *Explainable AI* (XAI) é indispensável para mitigar esses riscos, pois permite compreender e auditar as decisões algorítmicas.

Essa necessidade é reforçada pela Lei Geral de Proteção de Dados (LGPD) e pela *General Data Protection Regulation* (GDPR) europeia, que exigem *accountability* e transparência em processos automatizados. Logo, a segurança não pode ser analisada apenas sob a ótica da eficiência técnica, mas também como expressão de valores éticos e de responsabilidade organizacional. Os resultados também indicam que há uma lacuna significativa entre grandes corporações e pequenas e médias empresas (PMEs) na adoção de soluções seguras para IoT. Enquanto as grandes organizações conseguem investir em infraestrutura distribuída, IA e *Blockchain*, as PMEs frequentemente operam com dispositivos legados e políticas de segurança fragmentadas, tornando-se alvos preferenciais para ataques de negação de serviço e sequestro de dados.

Esse fenômeno cria um fosso digital de segurança, que não é apenas econômico, mas estratégico: as PMEs integram cadeias de valor globais e sua vulnerabilidade compromete ecossistemas inteiros. Estudos da Huawei (2023) e da OECD (2022) reforçam que políticas públicas de incentivo à cibersegurança inclusiva são essenciais para mitigar esse desequilíbrio estrutural. Adicionalmente, essa dependência levanta uma dimensão geopolítica crítica, pois a confiança na infraestrutura IoT-5G/6G está intrinsecamente ligada à soberania digital. A dependência de fornecedores ou algoritmos proprietários estrangeiros pode expor nações e corporações a riscos de vigilância e interrupção de serviços, tornando a autonomia tecnológica um imperativo estratégico para a resiliência nacional.

Um ponto de destaque na discussão é a redefinição da relação entre segurança e inovação. Tradicionalmente, a segurança era vista como um obstáculo ao avanço tecnológico. Entretanto, no cenário atual, ela se converteu em um acelerador de inovação responsável. Empresas que investem em segurança desde o *design* (*Security by Design*) conseguem desenvolver produtos e serviços mais confiáveis, escaláveis e compatíveis com legislações globais, reduzindo custos futuros de conformidade e litígio. Davenport e Kirby (2020) afirmam que a segurança inteligente é o novo motor da competitividade, pois permite que as organizações

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

inovem com confiança e previsibilidade de risco.

Por outro lado, a pesquisa evidencia que a dependência excessiva de soluções automatizadas pode gerar novos tipos de vulnerabilidade. Sistemas baseados em IA e *Big Data*, embora poderosos, podem ser alvos de ataques de manipulação de dados (*data poisoning*) ou inferência adversária, nos quais invasores corrompem os conjuntos de treinamento. Isso reforça a necessidade de mecanismos de verificação contínua e auditoria algorítmica — um campo ainda emergente na literatura de segurança 6G.

Assim, a discussão sintetiza que o futuro da segurança em IoT-5G/6G será moldado pela convergência de três dimensões interdependentes: tecnologia, governança e ética. A resiliência técnica proporcionada por IA e *Blockchain* só se concretiza plenamente quando acompanhada de uma governança transparente e de uma cultura organizacional que compreenda a segurança não como custo, mas como elemento de sustentabilidade e legitimidade social. Os resultados, portanto, não apenas confirmam as hipóteses levantadas, como ampliam o debate sobre o papel da segurança como pilar estruturante da economia digital.

A transição para redes 6G, que trará inteligência de rede nativa e comunicação sensorial, exigirá níveis ainda mais elevados de confiança e cooperação entre humanos e sistemas autônomos. Essa transição, se não for eticamente orientada, pode comprometer a privacidade, a equidade e a própria soberania digital das nações.

Em síntese, a análise evidencia que a segurança em IoT-5G/6G é simultaneamente um desafio técnico, humano e filosófico. O sucesso dessa integração dependerá menos da capacidade de criar barreiras e mais da habilidade de cultivar ecossistemas de confiança, nos quais a inovação tecnológica avance em harmonia com os valores éticos e sociais que sustentam a sociedade digital.

4. CONSIDERAÇÕES

Os resultados e análises desenvolvidos ao longo deste estudo permitem concluir que a segurança em sistemas IoT durante a transição para redes 5G e 6G transcende a dimensão técnica e assume um papel estrutural, estratégico e ético na sociedade digital contemporânea. A convergência entre dispositivos inteligentes, conectividade ubíqua e processamento distribuído cria um ecossistema de oportunidades e riscos sem precedentes. Nesse contexto, a segurança deixa de ser apenas um requisito operacional para se tornar um pilar de confiança, soberania e sustentabilidade tecnológica.

A pesquisa confirmou a hipótese de que as características arquiteturais das redes 5G/6G — como a latência ultrabaixa, a densidade massiva de dispositivos (mMTC) e a virtualização de funções de rede (NFV) — intensificam as vulnerabilidades inerentes aos sistemas IoT. A descentralização, embora essencial para o desempenho, fragmenta o controle e amplia a

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

superfície de ataque, exigindo mecanismos autônomos e inteligentes de defesa. Tecnologias como Inteligência Artificial (IA), Aprendizado de Máquina, *Blockchain* e Computação de Borda (*Edge Computing*) demonstram potencial para mitigar tais riscos, mas sua eficácia depende de integração, governança e capacitação humana.

O estudo também revelou que a transição segura para o ecossistema 6G dependerá da consolidação de uma cultura de segurança proativa dentro das organizações, em que a proteção de dados e a ética algorítmica sejam tratadas como valores corporativos e não meros requisitos regulatórios.

A adoção de *frameworks* como o *Zero Trust Architecture* e a implementação de *DevSecOps* se mostraram fundamentais para criar ambientes cibernéticos adaptativos, capazes de reagir e aprender continuamente frente a ameaças emergentes.

Além da dimensão tecnológica, os resultados reforçam a centralidade da governança ética como condição indispensável para a sustentabilidade da IoT. O avanço de sistemas autônomos e a coleta massiva de dados pessoais demandam responsabilidade e transparência na forma como algoritmos são treinados, auditados e aplicados. Sem *explicabilidade* e *accountability*, a própria legitimidade da transformação digital fica comprometida.

Como apontam Mittelstadt *et al.,* (2016) e a Enisa (2024), a ética deve ser incorporada desde o *design* das soluções — o princípio conhecido como *Ethics by Design* — garantindo que a inovação tecnológica avance em harmonia com os direitos fundamentais e os valores humanos. Do ponto de vista prático, esta pesquisa destaca que a segurança em IoT-5G/6G deve ser entendida como um investimento estratégico e de longo prazo, e não como custo operacional. Organizações que adotam políticas de cibersegurança baseadas em IA e *Blockchain* tendem a reduzir significativamente o tempo de resposta a incidentes, aumentar a confiança dos consumidores e ampliar sua competitividade global.

Além disso, a criação de ecossistemas colaborativos de segurança, que envolvam governos, universidades e empresas, é essencial para o compartilhamento de informações e o fortalecimento da resiliência digital em escala regional e nacional.

Em um cenário de crescente complexidade geopolítica e interdependência tecnológica, a soberania digital emerge como novo vetor de poder. A dependência de infraestruturas estrangeiras e de algoritmos proprietários pode comprometer a autonomia de países e instituições, tornando urgente o investimento em pesquisa nacional e o desenvolvimento de padrões abertos de segurança. A literatura recente, como apontam Radanliev *et al.,* (2022) e Shafi *et al.,* (2020), sugere que o futuro das redes 6G exigirá não apenas tecnologias mais seguras, mas modelos cooperativos de governança global, baseados em confiança mútua, interoperabilidade e transparência.

Do ponto de vista científico, esta pesquisa contribui ao sintetizar e articular as três

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

dimensões fundamentais da segurança digital moderna — tecnologia, governança e ética —, demonstrando que a maturidade em segurança não é alcançada apenas com soluções técnicas, mas com uma mudança cultural e institucional profunda. Essa visão holística reforça o conceito de "segurança sustentável", em que a inovação tecnológica e a responsabilidade social são mutuamente dependentes. Como limitação, destaca-se a natureza bibliográfica do estudo, que impossibilita a validação empírica direta das estratégias propostas.

Assim, recomenda-se que pesquisas futuras avancem para abordagens quantitativas e experimentais, incluindo estudos de campo, simulações ou *surveys* com empresas de diferentes portes e setores. Investigações empíricas poderão quantificar o retorno sobre o investimento (*ROI*) de soluções de segurança baseadas em IA e *Blockchain*, além de avaliar o impacto real de práticas de *reskilling* e *AI Ethics* no desempenho organizacional.

Por fim, as evidências reunidas indicam que o sucesso da IoT nas redes 5G/6G dependerá de uma aliança entre inovação e responsabilidade. A segurança cibernética não é apenas a defesa contra o risco, mas o alicerce sobre o qual se constrói a confiança social, a competitividade econômica e o futuro ético da conectividade. A transição para o 6G, com sua promessa de redes cognitivas e comunicações sensoriais, implicará mais do que capacidade técnica — exigirá maturidade ética, inteligência coletiva e visão estratégica.

Apenas com essa integração plena será possível garantir que a próxima era digital seja não apenas mais veloz e eficiente, mas também mais segura, justa e humana.

REFERÊNCIAS

AL-GARADI, M. A. et al. A survey of machine learning techniques for cyber security in IoT. **IEEE Communications Surveys & Tutorials,** Piscataway, NJ, v. 20, n. 3, p. 2577-2601, third quarter 2018.

ANDREWS, P. V.; CHERIAN, J.; MADY, M. F. A Survey on the Use of *Blockchain* in the Internet of Things (IoT) Security. **International Journal of Computer Networks and Communications**, New Delhi, v. 14, n. 4, p. 75-87, 2022.

BOUSSAHA, H. *et al.* 5G/6G Security Challenges and Solutions for IoT: A Survey. **IEEE Access**, Piscataway, NJ, v. 11, p. 11883-11910, 2023.

BRYNJOLFSSON, E.; MCAFEE, A. **The second machine age:** Work, progress, and prosperity in a time of brilliant technologies. New York: W. W. Norton & Company, 2014.

DAVENPORT, T. H.; RONANKI, R. Artificial intelligence for the real world. **Harvard Business Review,** Boston, MA, v. 96, n. 1, p. 108-116, 2018.

MERCADO COMUM DO SUL (MERCOSUL). **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Diário Oficial da União, 2018.

SHAFI, M. *et al.* 6G Vision: A New Era of Wireless Communication. **Applied Sciences**, Basel, v. 10, n. 12, p. 4390, 2020.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

YIN, H. *et al*. Security and Privacy in 5G-Enabled Internet of Things: Challenges and Solutions. **IEEE Network**, 2020.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.