South American Development Society Journal
Vol.: 12 | Nº.: 35 | **Ano:** 2026 | **ISSN:** 2446-5763 | **DOI:** 10.24325/issn.2446-5763.v12i35p54-75
Data de Submissão: 02/05/2026 **| Data de Publicação:** 30/08/2026

ANÁLISE DAS AMEAÇAS CIBERNÉTICAS À CADEIA DE SUPRIMENTOS E DOS POSSÍVEIS CONTROLES DE SEGURANÇA: UM ESTUDO BIBLIOMÉTRICO E REVISÃO SISTEMÁTICA DA LITERATURA

ANALYSIS OF CYBERSECURITY THREATS TO THE SUPPLY CHAIN AND POSSIBLE SECURITY CONTROLS: A BIBLIOMETRIC STUDY AND SYSTEMATIC LITERATURE REVIEW

Fernanda Lie Matsunaga - Faculdade de Tecnologia de São Paulo – FATEC-SP.
<fernandaliematsunaga@gmail.com>

Prof. Dr. Carlos Hideo Arima - Faculdade de Tecnologia de São Paulo – FATEC-SP.
<charima@uol.com.br>

Nichols Aron Jasper - Faculdade de Tecnologia de São Paulo – FATEC-SP.
<nicholsaron@hotmail.com>

Resumo

Com a crescente complexidade e interconectividade dos ecossistemas digitais, os riscos cibernéticos também se ampliaram, especialmente no contexto das cadeias de suprimentos. Nesse cenário, vulnerabilidades em qualquer elo podem ser exploradas por agentes maliciosos para comprometer infraestruturas críticas, distribuir atualizações maliciosas e acessar dados confidenciais. Esse trabalho tem como objetivo analisar as ameaças de cibersegurança que afetam a cadeia de suprimentos, caracterizando-as com base no relatório de ameaças da cadeia de suprimentos proposto pela Agência Europeia para a Segurança das Redes e da Informação (ENISA) e identificando suas finalidades. Outrossim, a pesquisa também busca compreender quais soluções tecnológicas e estratégicas são eficazes na mitigação desses riscos, caracterizadas com base nas famílias de controles C-SCRM propostas pelo National Institute of Standards and Technology (NIST). A metodologia adotada baseia-se em uma revisão bibliográfica com enfoque qualitativo, por meio da análise de artigos acadêmicos e publicações especializadas, abrangendo o período de 2020 a 2025. Os resultados apontam uma grande quantidade de ameaças que comprometem a segurança cibernética das cadeias de suprimentos, evidenciando deficiências em práticas e controles. Isso reforça a

necessidade de adoção de estratégias como Blockchain, Smart Contracts, frameworks de segurança cibernética, machine learning e antimalware, integradas a plataformas de gerenciamento de riscos cibernéticos. O estudo apresenta que a resiliência cibernética da cadeia de suprimentos depende da capacidade das organizações de identificar, mitigar e responder às ameaças presentes em todos os seus elos.

Palavras-chave: Cibersegurança; Segurança da informação; Cadeia de suprimentos; Riscos cibernéticos; Ameaças cibernéticas.

Abstract

With the increasing complexity and interconnectivity of digital ecosystems, cyber risks have also expanded, particularly in the context of supply chains. In this scenario, vulnerabilities in any link of the chain can be exploited by malicious actors to compromise critical infrastructures, distribute malicious updates, and gain unauthorized access to confidential data. This study aims to analyze the cybersecurity threats affecting the supply chain, characterizing them based on the Supply Chain Threat Report proposed by the European Union Agency for Cybersecurity (ENISA) and identifying their purposes. Furthermore, the research also seeks to understand which technological and strategic solutions are effective in mitigating these risks, characterized based on the C-SCRM control families proposed by the National Institute of Standards and Technology (NIST). The methodology adopted is based on a qualitative literature review, analyzing academic articles and specialized publications, covering the period from 2020 to 2025. The results indicate a wide range of threats that compromise the cybersecurity of supply chains, highlighting deficiencies in practices and controls. This reinforces the need to adopt strategies such as Blockchain, Smart Contracts, cybersecurity frameworks, machine learning, and antimalware solutions integrated with cyber risk management platforms. The study presents that the cyber resilience of the supply chain depends on the ability of organizations to identify, mitigate, and respond to threats present across all links of the chain.

Keywords: Cybersecurity; Information security; Supply chain; Cyber risks; Cyber threats.

Introdução

A cadeia de suprimentos transcende o simples fluxo de materiais, englobando também a circulação integrada de informações, serviços e recursos financeiros. Devido à sua relevância para o negócio, a continuidade operacional e a segurança da informação dessas cadeias são necessárias para proteção contra ameaças que podem comprometer a estrutura da organização. (HASSIJA et al., 2021).

A crescente dependência das tecnologias digitais nas cadeias de suprimentos trouxe à tona vulnerabilidades e ameaças significativas no âmbito de cibersegurança. Essas ameaças, cada vez mais sofisticadas, podem resultar em consequências severas, incluindo, a perda de dados estratégicos, interrupções nos processos operacionais, impactos financeiros e a deterioração da confiança por parte dos consumidores, dentro outros efeitos adversos (ADEWUSI; EYO-UDO, 2022).

Diante disso, os objetivos operacionais da segurança cibernética na cadeia de suprimentos, envolvem a proteção da confidencialidade, integridade e disponibilidade, além da garantia da autenticidade e exclusividade dos componentes (EGGERS, 2021). De acordo com Adewusi; Eyo-Udo (2022), as estratégias de mitigação incluem soluções tecnológicas, abordagens centradas no fator humano, medidas políticas e regulatórias. Logo, a integração desses elementos contribui para o aprimoramento da segurança e da resiliência contra as ameaças cibernéticas.

Esta pesquisa busca entender quais são as principais ameaças de cibersegurança na cadeia de suprimentos e as soluções mais citadas como medidas e contramedidas de proteção. Logo, o artigo tem como objetivo analisar as ameaças cibernéticas que mais impactam a cadeia de suprimentos e identificar as soluções mais utilizadas pelas organizações para mitigá-las, com ênfase em boas práticas de segurança da informação conforme normas.

Referencial teórico

Esta seção aborda os conceitos de segurança da informação na cadeia de suprimentos, as ameaças, as soluções e estratégias de mitigação, além do gerenciamento de riscos cibernéticos.

Ameaças

Problemas de segurança da informação surgem em qualquer etapa da cadeia de suprimentos, sendo que, o ponto mais vulnerável determina o local da proteção. Muitas das vezes, as ameaças e vulnerabilidades podem ultrapassar os modelos tradicionais de ataques virtuais, como negação de serviço (DoS), invasões com o intuito de sabotagem ou ataques por meio de *ransomware* (GUPTA *et al.,* 2020). Além disso, os ataques cibernéticos direcionados a sistemas industriais, cadeias de suprimentos ou dispositivos conectados (IoT) podem comprometer sistemas ciberfísicos, interromper operações e causar falhas produtivas.

Normalmente, agentes mal-intencionados exploram fornecedores e terceiros, para obter acessos indevidos, causar vazamento de dados ou comprometer os pilares de segurança da informação (HASSIJA et al., 2021).

Os ataques se concentram em quatro frentes principais. A primeira envolve as pessoas, que são exploradas por meio de *phishing*, *whaling* e engenharia social. Em seguida, o software torna-se alvo de malware, vulnerabilidades zero-day e SQL injection. Além disso, o hardware pode sofrer falsificação, adulteração e manipulação de componentes. Por fim, as redes também apresentam vulnerabilidades relacionadas a ataques de DoS, falhas de protocolos e dispositivos IoT inseguros.

Consequentemente, ataques a qualquer uma dessas frentes pode comprometer serviços críticos, desde operações logísticas até processos agrícolas (ETEMADI; GELDER; STROZZI, 2021; BHAT et al., 2021).

Soluções de mitigações das ameaças

Visto que as ameaças cibernéticas podem impactar o processo produtivo e a cadeia de suprimentos, torna-se necessária a adoção de soluções que integrem aspectos físicos e digitais. A prevenção exige estratégias abrangentes, desde a proteção da infraestrutura até dos sistemas e aplicativos (BHAT *et al.,* 2021). Para construir defesas que sejam eficazes, é necessário mapear as ameaças presentes em cada fase da cadeia para alinhar as estratégias de segurança às particularidades desse ecossistema (GUPTA *et al.,* 2020).

A partir do mapeamento, medidas preventivas e de boas práticas podem ser aplicadas de forma mais direcionada. Logo, o uso de sistemas inteligentes, atualizações periódicas, inteligência artificial e o fortalecimento do fator humano por meio de treinamentos, e *frameworks* de cybersegurança, consolida defesas mais eficientes na cadeia de suprimentos (ADEWUSI, CHIEKEZIE, EYO-UDO. 2022).

Frameworks, como o NIST SP 800-161r1, estruturam soluções para desafios complexos, oferecendo diretrizes flexíveis para escalabilidade, interoperabilidade e proteção, orientando a gestão de riscos de cibersegurança na cadeia de suprimentos (ETEMADI, GELDER, STROZZI. 2021). Além disso, o *machine learning* (ML), área da inteligência artificial, contribui para simplificar processos, aumentar a eficiência operacional e fortalecer a resiliência das cadeias de suprimentos diante de ameaças cibernéticas (HASSIJA *et al.,* 2021).

Portanto, nesse cenário, diversas tecnologias e práticas têm-se destacado por sua eficácia na prevenção, detecção e resposta a ameaças cibernéticas que são vistas ao longo desta pesquisa.

C-SCRM (*Cybersecurity Supply Chain Risk Management*)

A Gestão de Riscos de Cibersegurança na Cadeia de Suprimentos (C-SCRM) é um processo sistemático voltado para proteger ativos, dados e operações da cadeia de suprimentos contra ameaças cibernéticas (BOYENS *et al.*, 2022). Diferente da gestão de riscos da informação o C-SCRM propõe uma visão mais abrangente

integrando processos, pessoas e tecnologia. Além da relação entre os fornecedores, parceiros e terceiros (SPEKMAN e DAVIS, 2004).

Sua implementação envolve múltiplos *stakeholders*, como segurança da informação, privacidade, desenvolvimento de sistemas, aquisições, jurídico e recursos humanos, exigindo comprometimento da alta direção para tratar as ameaças de forma eficiente (BOYENS *et aç,.*2022). Portanto, o C-SCRM possibilita uma abordagem holística que fortalece a resiliência organizacional, melhora a tomada de decisão e reduz impactos negativos, garantindo a segurança e a continuidade dos negócios.

Metodologia de pesquisa

A metodologia adotada nesta pesquisa baseou-se nos princípios da revisão sistemática da literatura, com o objetivo de identificar e analisar os estudos mais relevantes sobre o tema, assegurando rigor metodológico e reprodutibilidade dos resultados. Como referência complementar, foi utilizado o relatório técnico "NIST SP 800-161r1". Especificamente, o tópico 2.2, intitulado "*Cybersecurity Risks Through Supply Chains",* que apresenta uma visão detalhada sobre os riscos cibernéticos que se manifestam a partir da cadeia de suprimentos. Fundamentando-se nessa referência, foram extraídos os termos mais frequentes e–gerada a nuvem de palavras destacando-se: *supply, chain, cybersecurity, risk* e *vulnerabilities*.

Com base nas palavras mais recorrentes identificadas na nuvem de palavras, iniciou-se a análise bibliométrica utilizando o *software* "*Publish or Perish v8.17.4863",* no dia 03 de maio de 2025 para identificar os artigos mais citados e influentes. Com base nas palavras identificadas na nuvem de palavras, foi realizada a etapa de definição da estratégia de busca, onde foram utilizados para o título a *string* consolidada: "*Supply Chain* OR *Third-Party* OR *Vendor* OR *Information Security* OR *Cybersecurity*". Já no caso das palavras-chaves, a formulação utilizada foi: *(Supply Chain OR Third-Party OR Vendor) AND (Cybersecurity OR Information Security) AND (Risk OR Vulnerabilities OR Threats OR Cybersecurity Risk OR Cybersecurity Threats OR Cyberattacks)"*. Além disso, o termo "*cyberattacks*" foi incluído nas palavras-chave devido à sua relevância conceitual em segurança da informação, representando ações maliciosas que comprometem sistemas, redes ou dados.

A fim de padronizar o processo de seleção, foi utilizado o protocolo de revisão sistemática (PRISMA-P). Na etapa de identificação, as pesquisas seguindo a *string* que foi consolidada abrangendo artigos publicados entre 2020 e 2025, resultaram em 2.566 registros provenientes das bases Google Scholar (n = 1.263) e OpenAlex (n = 1.303). Na triagem inicial foram removidos 1.226 artigos duplicados, 50 sem data de publicação e 62 identificados como livros ou patentes, restando 1.228 registros. Em seguida, artigos com citações abaixo do h-index (n = 57) foram excluídos, resultando em 59 registros, dos quais seis estavam inacessíveis, fazendo com que restassem apenas 53 para verificação.

A etapa de inclusão, o número final de artigos incorporados à pesquisa foi de 14, que atenderam a todos os critérios estabelecidos para a revisão sistemática, conforme a Tabela 1.

Tabela 1 Tabulação dos artigos incluídos na pesquisa

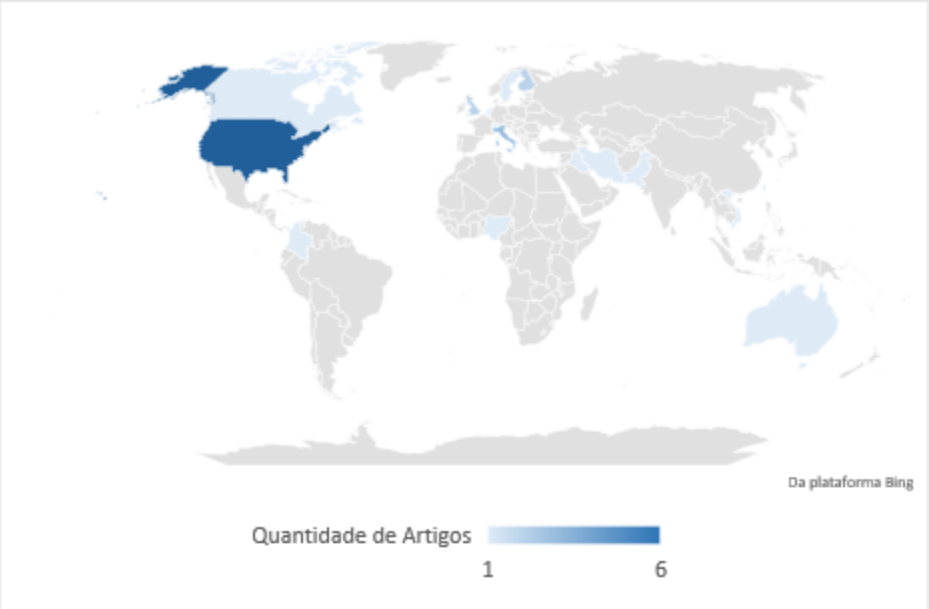
Citações	Nome	Ano	País
195	A survey on supply chain security: Application areas, security threats, and solution architectures	2020	Índia e EUA
148	Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks	2020	EUA
293	Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability	2021	Taiwan, Canada, Paquistão
140	The zero trust supply chain: Managing supply chain risk in the absence of trust	2021	EUA e Finlândia
131	Distributed ledger technologies in supply chain security management: A comprehensive survey	2021	Reino Unido e Iraque
129	Supply chain disruption risk management with blockchain: A dynamic literature review	2021	Bélgica, Irã e Itália
106	Security of blockchain-based supply chain management systems: challenges and opportunities	2021	Qatar
91	An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity	2021	Itália, Holanda

71	Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study	2021	Colômbia
57	A novel approach for analyzing the nuclear supply chain cyber-attack surface	2021	EUA
114	Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era	2022	Itália
75	Cybersecurity threats in agriculture supply chains: A comprehensive review	2022	EUA e Nigéria
63	Cybersecurity supply chain risk management practices for systems and organizations	2022	EUA
59	Data-driven review of blockchain applications in supply chain management: key research themes and future directions	2023	Reino Unido, Vietnã, Austrália

Fonte: Resultado da pesquisa (2025).

O *software Publish or Perish v8.17.4863*, utilizado na busca, não fornece diretamente os países de origem das publicações, limitando o levantamento completo dessas informações. Contudo, por meio da análise manual das afiliações institucionais dos autores dos artigos selecionados, foi possível identificar os países que mais contribuíram com publicações relevantes para o estudo conforme a Figura 1.

Figura 1 Distribuição de publicações por país



Fonte: Resultado da pesquisa (2025).

Resultados e discussão

Esta seção apresenta os principais resultados da revisão sistemática e análise bibliométrica, contemplando os setores analisados, os países com maior número de publicações, os principais tipos de ameaças, práticas de gerenciamento e tecnologias vinculadas à segurança da informação na cadeia de suprimentos. Esses dados permitem identificar temas de maior relevância científica na área de cibersegurança aplicada a cadeia de suprimento.

Artigos selecionados

Os artigos selecionados abrangem distintos setores da economia, evidenciando os desafios relacionados à segurança da informação nas cadeias de suprimentos e as tecnologias emergentes. O setor agroalimentar destaca-se pelo uso de *blockchain* e IoT para assegurar rastreabilidade, transparência e proteção nas cadeias agrícolas. Da mesma forma, a manufatura aditiva e os sistemas ciberfísicos revelam vulnerabilidades relacionadas à impressão 3D e à integração entre cadeias físicas e digitais. O setor de bens de consumo é explorado nos estudos que analisam a percepção de gestores sobre os riscos cibernéticos, enquanto a indústria nuclear recebe atenção específica em função da avaliação de vulnerabilidades críticas em sua cadeia de fornecimento.

Paralelamente, diversos estudos adotam uma abordagem mais abrangente e transversal, tratando de cadeias de suprimentos em geral. Esses estudos enfatizam práticas de gestão de riscos, a adoção de tecnologias, bem como estratégias de segurança. Ressaltam-se ainda publicações voltadas ao setor de *software* e tecnologia da informação, exemplificadas pelo caso da SolarWinds, além de diretrizes aplicáveis em diferentes indústrias. No conjunto, as pesquisas convergem para reforçar a importância e da resiliência das cadeias de suprimentos em ambientes digitais.

Evolução das publicações e citações

Em 2020, foram selecionados dois artigos, com total de 343 citações. No ano seguinte, 2021, representou o pico tanto em quantidade de artigos, quanto em impacto, com 8 publicações e 1.018 citações, resultado diretamente associado aos efeitos da pandemia da COVID-19. A crise global expôs a fragilidade das cadeias de suprimentos tradicionais e acelerou a digitalização, ampliando uso de IoT, nuvem e *blockchain*, aumentando a superfície de ataque e impulsionando o desenvolvimento de soluções de cibersegurança mais robustas (ADEWUSI, CHIEKEZIE, EYO-UDO. 2022).

Após 2021, observou-se uma redução no número de estudos incluídos, refletindo tanto a mudança de foco das pesquisas quanto o maior rigor nos critérios de seleção. Apesar disso, os trabalhos mantiveram impacto relevante, indicando amadurecimento do campo. A ausência de artigos mais recentes pode estar ligada à baixa maturidade das pesquisas ou ao tempo insuficiente para obter maior reconhecimento acadêmico.

Portanto, 2021 se destaca como o ano com maior concentração de artigos e de citações, indicando um período produtivo e relevante para o tema.

Distribuição geográfica das publicações

A compreensão da distribuição geográfica das publicações permite identificar quais países têm se destacado na produção científica sobre o tema analisado. Logo, este subtópico apresenta os dados referentes às nacionalidades das afiliações institucionais dos autores dos artigos selecionados.

O Estados Unidos se destaca com seis publicações, o que representa a maior contribuição entre os países analisados. Essa predominância pode estar associada ao alto investimento em pesquisa e desenvolvimento, e à ampla infraestrutura acadêmica disponível no país. Além disso, a expressiva participação do país no volume de publicações pode estar relacionada ao fato de o país ser um dos principais alvos de ataques cibernéticos em escala global. Esse cenário de alta

exposição reforça a necessidade de desenvolvimento de estudos, ferramentas e estratégias de gestão de riscos cibernéticos, o que possivelmente impulsiona a produção acadêmica nacional sobre o tema.

Na sequência, a Itália aparece com três artigos, seguido por Reino Unido com duas publicações. Esses países também são conhecidos por suas universidades de alto impacto na área de tecnologia.

Consequentemente, observa-se que a distribuição geográfica não apenas indica os maiores polos de pesquisa, mas também reflete as necessidades e vulnerabilidades específicas de cada região, evidenciando uma relação direta entre contextos socioeconômico e produção científica.

Ameaças cibernéticas e soluções na cadeia de suprimentos

A partir da sistematização dos dados obtidos das ameaças e das soluções, foi possível estabelecer uma correlação entre as técnicas de ataques mais recorrentes e as famílias de controles de segurança para C-SCRM para enfrentá-los. Com base na análise, foi desenvolvida uma correlação das técnicas de ataques com as categorias organizadas de controle da segurança da informação.

Com base na análise detalhada, foram desenvolvidas descrições concisas para cada ameaça, facilitando a compreensão das principais questões discutidas na literatura sobre segurança da cadeia de suprimentos, conforme a Tabela 2.

Tabela 2 Levantamento das ameaças cibernéticas

Ameaças	Taxonomia de Técnicas de Ataque	Finalidade	Qtde. Artigos
Falsificação de informações ou ativos	*Counterfeiting / Malware Infection / Trusted Relationship*	Enganar sistemas ou pessoas por meio da criação ou alteração fraudulenta de formas físicas, dados ou registros para obter vantagem indevida.	11
Fraudes	*Social Engineering / Phishing*	Obter ganhos financeiros ou estratégicos por meio da inserção de códigos maliciosos,	7

		manipulação de dados ou produtos falsificados, explorando a confiança entre empresas e seus fornecedores para violar sistemas, roubar informações e comprometer operações.	
Vazamento/ Violação de Dados	*Malware Infection / Exploiting Software Vulnerability / Exploiting Configuration Vulnerability / Trusted Relationship / Open-Source Intelligence* (OSINT)	Divulgação não autorizada de informações confidenciais, seja por meio de ações criminosas ou falhas internas.	6
Negação de serviço	*Exploiting Software Vulnerability / Malware Infection*	Tornar sistemas ou serviços indisponíveis, sobrecarregando servidores com tráfego excessivo e interrompendo o acesso por usuários legítimos	6
Insider Threat	*Trusted Relationship*	Alguém com acesso autorizado causa danos intencional ou acidental a recursos, pessoas ou sistemas.	5
Ataques *Sybil*	*Counterfeiting*	Manipular ou controlar redes descentralizadas ao criar múltiplas identidades falsas, permitindo ao invasor obter vantagem indevida	4
Man-in-the-middle	*Exploiting Configuration Vulnerability*	Modificar ou excluir o conteúdo da mensagem durante a transmissão entre duas entidades e, em seguida, envia-a ao destino.	4
Falta de transparência	*Exploiting Configuration Vulnerability*	Ocultar atividades ilegítimas, dificultar a rastreabilidade de ações e facilitar fraudes ou manipulações na cadeia de suprimentos.	3
Malware	*Malware Infection / Drive-by Compromise*	Danificar ou acessar sistemas de forma ilegal	3
Phishing	*Phishing / Social Engineering*	Utiliza técnicas de enganação para obter acesso não autorizado a informações confidenciais, como senhas, dados bancários ou sistemas internos, geralmente com o	3

		objetivo de roubo financeiro, espionagem, sabotagem ou outros tipos de fraudes.	
Roubo de credenciais (*Credential Theft*)	*Phishing / Malware Infection*	Obter acesso não autorizado a sistemas, redes ou informações sensíveis, utilizando identidades legítimas para realizar ações maliciosas.	3

Fonte: Resultado da pesquisa (2025).

Diante das ameaças cibernéticas identificadas na cadeia de suprimentos, é necessário compreender as medidas e controles desenvolvidos para sua mitigação. Nesse contexto, a Tabela 3 apresenta as famílias de controles de segurança para C-SCRM, segundo o NIST SP 800-161r1 (BOYENS *et al.*, 2022), com uma breve descrição de seus objetivos, visando facilitar a compreensão do papel de cada grupo de controles na mitigação de riscos e proteção organizacional.

Tabela 3 Resumo dos objetivos das famílias de controles C-SCRM

SIGLA	Nome da Família de Controles	Objetivo / Finalidade da Família
AC	*Access Control*	Garantir que apenas usuários, processos e dispositivos devidamente autorizados tenham acesso aos sistemas de informação, limitando suas ações aos privilégios definidos, a fim de proteger dados e recursos contra acessos não autorizados
AT	*Awareness and Training*	Assegurar que todos os colaboradores compreendam os riscos de segurança da informação relacionados às suas funções e estejam capacitados, por meio de treinamento apropriados, para cumprir suas responsabilidades de forma segura e em conformidade com as políticas e normas da organização
AU	*Audit and Accountability*	Garantir que a criação, proteção e retenção de registros de auditoria que permitam identificar e rastrear atividades nos sistemas de informação, promovendo a responsabilização dos usuários e possibilitando a detecção e resposta a ações indevidas ou não autorizadas
CA	*Assessment, Authorization and Monitoring*	Garantir que os controles de segurança dos sistemas de informação sejam regularmente avaliados, autorizados e monitorados para

		assegurar sua eficácia, corrigir vulnerabilidades e manter a operação segura dos sistemas organizacionais
CM	*Configuration Management*	Certificar que a criação, atualização e gestão das configurações e inventários dos sistemas de informação, assegurando que as definições de segurança adequadas sejam implementadas e preservadas durante todo o ciclo de vida dos recursos tecnológicos da organização
CP	*Contingency Planning*	Assegurar a criação, manutenção e execução eficaz de planos que permitam a resposta rápida a emergências, a recuperação de dados e a continuidade dos sistemas de informação essenciais, assegurando a operação ininterrupta da organização mesmo em situações críticas
IA	*Identification and Authentication*	Assegurar que apenas usuários, processos e dispositivos devidamente identificados e autenticados possam acessar os sistemas de informação, fortalecendo a segurança e prevenindo acessos não autorizados.
IR	*Incident Response*	Garantir que a organização possua processos estruturados para identificar, responder, conter e recuperar-se de incidentes de segurança, além de registrar e comunicar adequadamente esses eventos às partes responsáveis, minimizando impactos e fortalecendo a resiliência dos sistemas
MA	*Maintenance*	Assegurar a realização regular e adequada da manutenção dos sistemas de informação, controlando os recursos e procedimentos utilizados para preservar a integridade, disponibilidade e segurança dos sistemas
MP	*Media Protection*	Garantir a proteção, controle de acesso e o descarte seguro dos meios que armazenam informações, prevenindo o acesso não autorizado e a divulgação inadvertida de dados sensíveis
PE	*Physical and Environmental Protection*	Garantir a segurança dos sistemas de informação e da infraestrutura física contra acessos indevidos, riscos ambientais e avarias, proporcionando um ambiente protegido e adequado para o funcionamento estável e seguro dos recursos tecnológicos da organização
PL	*Planning*	Assegurar a elaboração e manutenção de planos de segurança que detalhem os controles adotados e orientem o comportamento dos usuários, promovendo a proteção eficaz dos sistemas de informação da organização
PM	*Program Management*	Implementar controles organizacionais que coordenem e apoiem o programa de segurança da informação, garantindo uma gestão integrada e eficaz dos riscos em toda a empresa
PS	*Personnel Security*	Assegurar que indivíduos em posições críticas sejam confiáveis, proteger os ativos da organização durante mudanças de pessoal e aplicar

		medidas disciplinares para garantir o cumprimento das normas de segurança
PT	*Personally Identifiable Information Processing and Transparency*	Assegurar o manejo correto e transparente dos dados pessoais identificáveis, incentivando a cooperação com fornecedores para compreender e ajustar suas políticas de privacidade às demandas da organização, garantindo a segurança e conformidade no processamento dessas informações
RA	*Risk Assessment*	Realizar avaliações regulares dos riscos que os sistemas de informação e o tratamento das informações podem representar para as operações, ativos e pessoas da organização, visando identificar, analisar e mitigar possíveis impactos negativos.
SA	*System and Services Acquisition*	Garantir recursos, integrar segurança no desenvolvimento, controlar o uso de software e assegurar que terceiros protejam adequadamente os sistemas e informações da organização
SC	*System and Communications Protection*	Proteger e acompanhar as comunicações nos pontos essenciais dos sistemas, utilizando métodos de engenharia e desenvolvimento que aumentem a segurança e a confiabilidade das informações na organização
SI	*System and Information Integrity*	Assegurar a detecção, correção rápida de vulnerabilidades, defesa contra malware e resposta eficaz a alertas de segurança para manter a integridade e proteção dos sistemas e informações da organização
SR	*Supply Chain Risk Management*	Identificar, avaliar e mitigar riscos relacionados à cadeia de suprimentos, garantindo a segurança e integridade dos produtos, serviços e informações fornecidos por terceiros, minimizando impactos adversos na organização

Fonte: Resultado da pesquisa (2025).

A partir disso, as soluções de segurança encontradas foram associadas às famílias de controles, permitindo um alinhamento entre as práticas recomendadas a riscos cibernéticos na cadeia de suprimentos e os controles específicos para a gestão de riscos cibernéticos na cadeia de suprimentos, como pode ser visto na Tabela 4.

Tabela 4 Levantamento das soluções mais citadas pelos artigos

Soluções	Família de Controles	Finalidade	Artigos

Blockchain	SC, SI, CM, SR	Promover segurança de dados; rastreabilidade de dados, transparência; contratação inteligente; eficiência; e descentralização.	11
Smart Contracts	SC	Automatizar e tornar transparente o cumprimento de acordos, promovendo confiança sem intermediários, ao executar ações automaticamente com autenticação segura.	8
Frameworks para Gestão de Riscos Cibernéticos	RA, RM, SR	Conjuntos estruturados de práticas e padrões que orientam a proteção de sistemas contra ameaças digitais (ex. NIST CSF, ISO 27001)	6
Machine Learning (IA)	SC, CA	Aplicar análises para identificar anomalias subsequentes nos fluxos de dados, utilizando algoritmos que podem revelar insights, prever tendências/vulnerabilidades e otimizar as operações da cadeia de suprimentos.	5
RFID	PE, IA, PM, SA	Identificar e rastrear objetos automaticamente usando ondas de rádio, facilitando o controle e a gestão de inventários, ativos e processos logísticos.	3
Autenticação Multi-Camada	AC, IA	Fortalecer os métodos de autenticação ao requerer diversos fatores de verificação antes de permitir o acesso a sistemas essenciais.	3
Anti-malware	SC, SI	Proteger contra acessos não autorizados e ataques maliciosos.	2
Avaliação de terceiros	RA, SR, SA	Ajuda a garantir a conformidade com esses padrões e identificar áreas que precisam de melhorias. Ao seguir os padrões estabelecidos, as organizações podem aprimorar sua postura de segurança e reduzir o risco de ameaças cibernéticas.	2
Mecanismos de Tolerância a Falhas Bizantinas	SI, SC	Permitir que uma rede alcance consenso mesmo na presença de nós defeituosos ou maliciosos que possam não responder corretamente ou fornecer informações enganosas.	2

Políticas de segurança cibernética	PL, PM	Definem regras para proteger dados e sistemas contra ameaças digitais	2
SIEM (*Security Information and Event Management*)	CA, IR, AU	Permitir o monitoramento em tempo real da atividade da rede e de potenciais ameaças.	2
Treinamento de conscientização de segurança	AT, PM	Promover programas de treinamento e conscientização em segurança cibernética são essenciais para reduzir erros humanos, ameaças internas e fortalecer a defesa contra ataques.	2
Zero Trust Architecture	AC, SC, CM, IR, RA, PL, SR	Parte do princípio “nunca confie, sempre verifique”, que garante que nenhum acesso seja automaticamente confiável, exigindo autenticação e autorização contínuas.	2

Fonte: Resultado da pesquisa (2025).

Por fim, baseando-se na análise das técnicas de ataque relacionadas às ameaças identificadas e nas características dos controles de segurança recomendados, foi possível estabelecer uma correlação entre as técnicas utilizadas pelos agentes maliciosos e as famílias de controles propostas pelo NIST para mitigação desses riscos. Essa avaliação permite identificar quais famílias de controles são capazes de endereçar diretamente cada técnica de ataque, proporcionando uma visão das estratégias para fortalecer a segurança da cadeia de suprimentos. Como resultado, essas correspondências foram organizadas e apresentadas na Tabela 5.

Tabela 5 Mapeamento entre técnicas de ataque e famílias de controle

Taxonomia de Técnicas de Ataque	Finalidade
Malware Infection	CM: Configuration Management
	SC: System and Communications Protection
	SI: System and Information Integrity
	IR: Incident Response
Social Engineering	AT: Awareness and Training
	AC: Access Control
	IA: Identification and Authentication
	PM: Program Management

Brute-Force Attack	AC: Access Control
	IA: Identification and Authentication
	SI: System and Information Integrity
Exploiting Software Vulnerability	CA: Security Assessment and Authorization
	CM: Configuration Management
	SA: System and Services Acquisition
	SI: System and Information Integrity
	RA: Risk Assessment
Exploiting Configuration Vulnerability	CA: Security Assessment and Authorization
	CM: Configuration Management
	MA: Maintenance
	SI: System and Information Integrity
	RA: Risk Assessment
Physical Attack or Modification	MP: Media Protection
	PE: Physical and Environmental Protection
	PM: Program Management
Open-Source Intelligence (OSINT)	CA: Security Assessment and Authorization
	CP: Contigency Planning
	PL: Planning
	PM: Program Management
	SR: Supply Chain Risk Management
Counterfeiting	SC: System and Communications Protection
	SI: System and Information Integrity
	SR: Supply Chain Risk Management
Trusted Relationship	AC: Access Control
	AU: Audit and Accountability
	CA: Security Assessment and Authorization
	SA: System and Services Acquisition
	SR: Supply Chain Risk Management
Drive-by Compromise	CM: Configuration Management
	IR: Incident Response
	MA: Maintenance
	SC: System and Communications Protection
	SI: System and Information Integrity
Phishing	AT: Awareness and Training
	PM: Program Management
	SI: System and Information Integrity

Fonte: Resultado da pesquisa (2025).

A análise da Tabela 2 evidencia que a falsificação de informações ou ativos é a principal ameaça, comprometendo a integridade de dados, processos de decisão e a confiança do mercado. Fraudes, com sete citações, destaca-se como uma preocupação significativa, enquanto, com seis ocorrências, estão as ameaças de negação de serviço (DoS) e vazamento/violação de dados que representam riscos críticos à disponibilidade e confidencialidade dos sistemas. Com cinco citações cada, man-in-the-middle e ataque Sybil revelam vulnerabilidades em comunicações e redes descentralizadas, demonstrando a importância de mecanismos de autenticação, criptografia e monitoramento. Além disso, com cinco citações, a ameaça *Insider threat* destaca o perigo de usuários autorizados explorarem privilégios para causar danos ou facilitar, de forma intencional ou acidental, causando danos a organização. Já a falta de transparência, *malware, phishing* e roubo de credenciais, com quatro menções cada reforçam a necessidade de controles técnicos.

A Tabela 4, evidencia que o *Blockchain*, com onze menções, é a solução mais destacada por garantir transparência, rastreabilidade e integridade de dados em ambientes distribuídos, prevenindo falsificações e fraudes. Os *Smart Contracts*, citados oito vezes, ampliam esse efeito ao automatizar processos e reduzir manipulações. Além disso, os *frameworks* de segurança, com seis menções, como os do NIST, oferecem diretrizes estruturadas para fortalecer as defesas. Já o uso de *machine learning* (ML), com cinco menções, auxilia no monitoramento contínuo e na detecção de anomalias.

A partir da análise das Tabelas 2 e 4 foi possível correlacionar as técnicas de ataque e os controles de segurança, resultando na Tabela 5. Essa relação evidencia as famílias mais adequadas para mitigar ameaças específicas, oferecendo uma visão integrada que facilita a identificação das práticas mais eficazes para fortalecer a segurança e a integridade das cadeias de suprimentos.

Considerações finais

Este trabalho teve como foco a análise das principais ameaças cibernéticas que afetam as cadeias de suprimentos e das soluções mais citadas para mitigá-las. Incialmente, foi realizada uma análise bibliométrica nas bases Google Scholar e OpenAlex, considerando apenas as publicações entre 2020 e 2025. Em seguida, foi aplicado o protocolo PRISMA para a triagem e seleção dos artigos, garantindo que apenas estudos diretamente relacionados à cibersegurança na cadeia de suprimentos fossem incluídos. A partir desse conjunto de trabalhos, desenvolveu-se a revisão sistemática baseada em um artigo do NIST sobre o tema permitindo a identificação das ameaças mais recorrentes e das soluções mais discutidas na literatura científica recente.

Os resultados destacaram maior preocupação como falsificação, fraudes, vazamento de dados, negação de serviço, ataques *Sybil* e *man-in-the-middle*. As soluções mais citadas foram *blockchain*, *smart contracts*, *frameworks* de segurança e *machine learning*, permitindo correlacionar técnicas de ataque, ameaças e controles para definir estratégias de mitigação mais eficazes.

A pesquisa procurou responder à questão problema, analisando as principais ameaças à cadeia de suprimentos, identificando soluções de mitigação e avaliando estudos publicados no período, com ênfase nos mais citados pela sua relevância científica.

Além disso, a pesquisa apresenta limitações principalmente relacionados ao acesso às bases de dados acadêmicas. Parte dessas bases não são de acesso aberto e, portanto, não foi possível consultar todos os artigos relevantes disponíveis, o que pode restringir a abrangência da revisão bibliográfica. Além disso, alguns artigos utilizados também possuem restrições de acesso, limitando a profundidade da análise realizada. Outro ponto é que não foi possível verificar a origem dos países de cada artigo elegíveis, o que poderia influenciar na análise geográfica dos dados. Essas limitações apontam para a necessidade de futuras pesquisas com acesso mais amplo a fontes especializadas para complementar e aprofundar os resultados obtidos.

Como trabalhos futuros, sugere-se avaliar a eficácia das soluções de mitigação por meio de estudos de caso ou simulações, visto que muitos artigos apresentam abordagens apenas teóricas. Também se propõe investigar como as empresas implementam essas soluções em suas cadeias de suprimentos, identificando as ameaças mais recorrentes, os desafios práticos, limitações e lições aprendidas na adoção dessas estratégias.

Referências bibliográficas

ADEWUSI, A.; CHIEKEZIE, C.; EYO-UDO, E. Cybersecurity threats in agriculture supply chains: A comprehensive review. **World Journal of Advanced Research and Reviews**, 2022. Disponível em: <https://www.researchgate.net/profile/Adebunmi-Adewusi/publication/384049365_Cybersecurity_threats_in_agriculture_supply_chains_A_comprehensive_review/links/67001a8df599e0392fb66b83/Cybersecurity-threats-in-agriculture-supply-chains-A-comprehensive-review.pdf> Acesso em 20 jun. 2025.

BAYRAMOVA, A.; EDWARDS, D.; ROBERTS, C. The role of blockchain technology in augmenting supply chain resilience to cybercrime. **MDPI**, v. 11, n. 7, 2021. DOI: 10.3390/buildings11070283. ISSN 2075-5309. Acesso em 19 jun. 2025.

BHAT, S.A. *et al*. Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability. **MDPI**, v. 12, n. 1, p. 40, 2022. DOI: https://doi.org/10.3390/agriculture12010040. Acesso em 19 jun. 2025.

BOYENS, J. et al. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. **National Institute of Standards and Technology**, 2022. Disponível em: https://doi.org/10.6028/NIST.SP.800-161r1-upd1. Acesso em 20 jun. 2025.

EGGERS, S. A novel approach for analyzing the nuclear supply chain cyber-attack surface. **Nuclear Engineering and Technology**, 2021. Elsevier. DOI: 10.1016/j.net.2020.08.021. Acesso em: 20 jun. 2025.

ENISA – European Union Agency for Cybersecurity. Threat Landscape for Supply Chain Attacks. **ENISA,** 2021. Disponível em: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks. Acesso em: 26 jun. 2025.

ETEMADI, N.; GELDER, P.V.; STROZZI, F**.** An ISM Modeling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply Chains towards Cybersecurity. ***Sustainability***, v. 13, n. 9, p. 4672, 2021. DOI: 10.3390/su13094672. Acesso em: 20 jun. 2025.

GUPTA, N. *et al.* Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks. **IEEE Access**, v. 8, p. 47322-47333, 6 mar. 2020. DOI: 10.1109/ACCESS.2020.2978815. Disponível em: https://doi.org/10.1109/ACCESS.2020.2978815. Acesso em: 19 jun. 2025.

HASSIJA, V. *et al***.** A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Internet of Things Journal*, [S.l.], v. 8, n. 8, p. 6222-6246, 15 abr. 2021. DOI: 10.1109/JIOT.2020.3025775. Disponível em: https://doi.org/10.1109/JIOT.2020.3025775. Acesso em: 20 jun. 2025.

LADISA, P. *et al*. SoK: Taxonomy of Attacks on Open-Source Software Supply Chains. **IEEE Symposium on Security and Privacy (SP),** May 2023, San Francisco, CA, USA. DOI: 10.1109/SP46215.2023.10179304. Acesso em 20 jun. 2025.