CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA ´PAULA SOUZA

FACULDADE DE TECNOLOGIA DE SÃO PAULO – FATEC SP

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

FERNANDA LIE MATSUNAGA

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

SÃO PAULO

2025

FERNANDA LIE MATSUNAGA

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

Trabalho de Conclusão de Curso apresentado como exigência para obtenção de título de Tecnólogo em Análise e Desenvolvimento de Sistemas

Orientado: Prof. Dr. Carlos Hideo Arima

SÃO PAULO

2025

FACULDADE DE TECNOLOGIA DE SÃO PAULO

FERNANDA LIE MATSUNAGA

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

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Parecer do Professor Orientador: _____
_____
_____
_____

Orientador: Prof. Dr. Carlos Hideo Arima

SÃO PAULO, 29 de junho de 2025.

À minha família que me ensinou que
quando as raízes são profundas,
não há razão para temer o vento.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Com a crescente complexidade e interconectividade dos ecossistemas digitais, os riscos cibernéticos também se ampliaram, especialmente no contexto das cadeias de suprimentos. Esse trabalho tem como objetivo analisar as ameaças de cibersegurança que afetam a cadeia de suprimentos, identificando suas finalidades. A pesquisa também busca compreender quais soluções tecnológicas e estratégicas são eficazes na mitigação dessas ameaças. 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* (IA) e anti-malware, integradas a plataformas de gerenciamento de riscos cibernéticos. O estudo apresenta que a resiliência cibernética da cadeia de suprimentos está diretamente relacionada à 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, ciberataques, soluções de segurança.

ABSTRACT

With the increasing complexity and interconnectivity of digital ecosystems, cyber risks have also expanded, especially in the context of supply chains. This study aims to analyze the cybersecurity threats affecting the supply chain, identifying their purposes. The research also seeks to understand which technological and strategic solutions are effective in mitigating these threats. The methodology is based on a qualitative literature review through the analysis of academic articles and specialized publications covering the period from 2020 to 2025. The results indicate many threats that compromise the cybersecurity of supply chains, highlighting deficiencies in practices and controls. This reinforces the need for the adoption of strategies such as Blockchain, Smart Contracts, cybersecurity frameworks, machine learning (AI), and anti-malware solutions integrated with cyber risk management platforms. The study shows that the cyber resilience of the supply chain is related to organizations' ability to identify, mitigate, and respond to threats across all its links.

Keywords: Cybersecurity, information security, supply chain, cyber risks, cyber threats, cyberattacks, security solutions.

1 INTRODUÇÃO

A cadeia de suprimentos transcende o simples fluxo de materiais, englobando também a circulação integrada de informações, serviços e recursos financeiros. Essa rede complexa e interdependente de *stakeholders* requer uma coordenação eficiente para garantir a entrega adequada dos produtos e serviços. Atualmente, as cadeias de suprimentos chegam a operar em escala global, atravessando múltiplas fronteiras geográficas e contextos socioeconômicos variados, o que impõe a necessidade de mecanismos rigorosos de controle, monitoramento e governança para assegurar sua eficácia e resiliência. Devido à sua relevância para diversos setores econômicos, a continuidade operacional e a segurança dessas cadeias são imperativas, demandando a adoção de estratégias robustas de proteção contra ameaças que possam comprometer toda a estrutura logística e comercial (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 (ADEWUSI; EYO-UDO, 2022).

Uma vez dentro do perímetro dos sistemas corporativos, atacantes podem assumir o controle de infraestruturas críticas, distribuir atualizações maliciosas de softwares e acessar dados confidenciais de forma não autorizada. Tais ataques geralmente se originam a partir da exploração de vulnerabilidades presentes nos fornecedores das organizações, os quais podem incluir desde empresas desenvolvedoras de software até prestadores de serviços essenciais, como tecnologia e telecomunicações. Além disso**,** cerca de 56% das companhias já foram vítimas de violações provocadas por brechas em seus ecossistemas de fornecedores (COLLIER, SARKIS. 2021).

Um dos propósitos fundamentais da segurança da informação e, consequentemente, cibernética, é assegurar que a confidencialidade, integridade e disponibilidade (CID) de um sistema ou componente ao longo da sua operação estejam protegidos. Quando um ativo sofre um ataque dentro da cadeia de suprimentos e entra em seu ciclo de vida, as ameaças podem persistir e passar despercebidas pelas defesas da tecnologia da informação e comunicação (TIC). Entretanto, por outro lado, temos os objetivos operacionais da segurança cibernética na cadeia de suprimentos, que envolvem a proteção da confidencialidade, integridade e disponibilidade, mencionadas anteriormente, 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.

1.1 QUESTÃO PROBLEMA

Quais são as principais ameaças de cibersegurança na cadeia de suprimentos e as soluções mais citadas como medidas e contramedidas de proteção?

1.2 OBJETIVOS GERAIS

Analisar as ameaças cibernéticas que 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.

1.3 OBJETIVOS ESPECÍFICOS

- Realizar o levantamento e a seleção de artigos científicos em bases de dados acadêmicas, com o intuito de identificar estudos relevantes para a análise das ameaças cibernéticas na cadeia de suprimentos e as soluções de mitigação.
- Realizar uma análise dos artigos científicos publicados destacando os anos com maior número de publicações e citações.
- Identificar os tipos de ataques cibernéticos direcionados à cadeia de suprimentos.
- Identificar as soluções mais citadas pelos artigos para mitigar as ameaças.
- Estabelecer uma correlação entre as técnicas de ataque identificadas e as famílias de controles de segurança da informação.

1.4 ESTRUTURA DO TRABALHO

Esta monografia está dividida em cinco partes principais que organizam o desenvolvimento da pesquisa de forma objetiva.

A introdução apresenta o tema da cibersegurança na cadeia de suprimentos, destacando sua relevância diante das atuais ameaças cibernéticas. Neste tópico, é apresentado a questão problema, que define o foco principal da pesquisa, seguida pelos objetivos gerais e específicos, que esclarecem as metas amplas e detalhadas

do estudo. Por fim, inclui-se a descrição da estrutura do trabalho, que orienta o leitor sobre a organização dos capítulos e o conteúdo abordado em cada um, facilitando a compreensão do desenvolvimento do tema ao longo do trabalho.

A Fundamentação Teórica, na qual são apresentados os principais conceitos relacionados à segurança da informação na cadeia de suprimentos. Nesse tópico são explorados o gerenciamento cibernético dos riscos na cadeia de suprimentos, as ameaças cibernéticas mais relevantes nesse ecossistema e as soluções que as mitigam.

No tópico seguinte, é detalhada a Metodologia adotada para a realização do estudo. Nele são descritos o tipo de pesquisa, as técnicas e ferramentas utilizadas para a coleta e análise de dados, os critérios de seleção das publicações e as etapas do processo investigativo, com o intuito de garantir rigor e coerência à abordagem adotada. Além disso, são apresentados quais foram os resultados obtidos da metodologia e sobre os dados das publicações selecionadas.

Já o tópico sobre a Análise dos Resultados, são discutidos os dados obtidos a partir da pesquisa. Essa seção busca interpretar os achados da revisão literária realizada, relacionando-os com os objetivos definidos a procura de responder à questão problema definida para este estudo.

Por fim, o último tópico apresenta as Consideração Finais, reunindo as conclusões do trabalho, a relevância dos resultados para o campo da segurança da informação na cadeia de suprimentos e sugestões para estudos futuros ou para aprimoramentos nas práticas de combate às ameaças cibernéticas.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os principais conceitos relacionados à segurança da informação na cadeia de suprimentos. Inicialmente é explorado as ameaças. Em seguida, as soluções e estratégias de mitigação dessas ameaças. Por fim, é apresentado o gerenciamento de riscos cibernéticos aplicadas à cadeia de suprimentos.

2.1 Ameaças na Cadeia de Suprimentos

Problemas relacionados à segurança da informação podem surgir em qualquer etapa de uma cadeia de suprimentos. A proteção global dessa cadeia pode ser determinada por seu ponto mais vulnerável. Logo, um agente mal-intencionado focará seus esforços no elo mais fraco para conseguir um acesso indevido.

Adicionalmente, os terceiros frequentemente não estão integrados aos procedimentos internos de gestão de riscos na cadeia de suprimentos, o que representa uma vulnerabilidade cibernética relacionada a acessos não autorizados. Além disso, muitos fornecedores contam com defesas cibernéticas insuficientes para impedir acessos indevidos, tornando-se uma das principais razões para incidentes de vazamento de dados envolvendo fornecedores (HASSIJA *et al.,* 2021). Ataques que são voltados para ambientes virtuais e digitais podem comprometer a confidencialidade, integridade e disponibilidade das informações e dos sistemas, permitindo a modificação de parâmetros de operações, a inserção de malware ou o sequestro de dados sensíveis.

As ameaças e vulnerabilidades ultrapassam os modelos tradicionais de ataques virtuais, como por exemplo, negação de serviço (DoS), invasões com o intuito de sabotagem ou ataques por meio de *ransomware* (GUPTA *et al.,* 2020). De fato, muitas das ameaças que são listadas pelos autores mostram que apesar da associação delas serem exclusivamente relacionadas a ambientes digitais ou virtuais, a realidade é que as ameaças ultrapassam as fronteiras do ciberespaço e geram impactos concretos no mundo físico.

Ataques cibernéticos direcionados a sistemas industriais, cadeias de suprimentos ou dispositivos conectados (IoT) podem comprometer equipamentos físicos, interromper operações e causar falhas produtivas.

Nas organizações, equipamentos como sensores e máquinas automatizadas podem ser vulneráveis a invasões, permitindo que agentes mal-intencionados acessem indevidamente redes ou alterem o funcionamento de processos. A ausência de mecanismos de proteção eficazes nesses equipamentos pode fazer com que esses ativos sejam utilizados para desencadear ataques mais abrangentes, impactando negativamente na produção.

Na cadeia de suprimentos os invasores podem comprometer o fornecedor ou prestador de serviço terceirizado como forma de acessar redes mais abrangentes. Por exemplo, a invasão de um sistema de uma empresa de logística pode atrasar a entrega de insumos essenciais, causando prejuízos operacionais e financeiros (ADEWUSI, CHIEKEZIE, EYO-UDO. 2022).

Segundo (BAYRAMOVA, EDWARDS, ROBERTS. 2021), os ataques cibernéticos podem ser divididos entre quatro partes vulneráveis, sendo eles: pessoas, *software, hardware* e rede que são exploradas pelos adversários para mineração de dados, espionagem cibernética e violação de dados. Dentre as quatro partes, os ataques direcionados às pessoas se destacam como os mais vulneráveis e suscetíveis a ciberataques, sendo frequentemente explorados por meio de técnicas como *phishing*, *whaling* e engenharia social. Essa parte refere-se à exploração do comportamento humano, incluindo ações, decisões e falhas, como porta de entrada para ciberataques e ameaças à segurança cibernética, tornando os usuários alvos estratégicos para as ameaças.

Os ataques à cadeia de suprimentos que possuem como alvo o *software*, visam comprometer as organizações por meio de inserção de código malicioso em componentes utilizados durante o desenvolvimento ou distribuição de *softwares*. Exemplos comuns dessas ameaças incluem: *softwares* maliciosos (*malware*), *zero-day* e SQL injection. Como consequência, alguns casos como o ataque à plataforma *Orion* da SolarWinds apresentam como essas falhas podem ser exploradas para atingir milhares de organizações (LADISA *et. al.,* 2023).

Já a parte vulnerável que tem como alvo os *hardwares*, abrange ameaças que envolvem a manipulação física ou lógica de componentes eletrônicos e dispositivos ao longo da cadeia de suprimentos. Diferentemente dos ataques que exploram vulnerabilidades de *softwares*, esses ataques possuem como alvo equipamentos, dispositivos físicos e seus elementos técnicos, podendo comprometer a integridade, confiabilidade e autenticidade dos produtos. Entre os exemplos mais comuns estão a falsificação de componentes eletrônicos, ataques físicos e uso de dispositivos falsificados/adulterados desde a fabricação, que permitem acesso remoto ou coleta não autorizada de dados. Muitas dessas ameaças passam despercebidas pelas defesas tradicionais e representam riscos significativos para setores críticos como telecomunicações, defesa, saúde e manufatura (GUPTA *et al.,* 2020).

Por fim, têm os ataques direcionados à rede, que são uma das principais ameaças à segurança das cadeias de suprimentos, especialmente devido à crescente dependência de sistemas interconectados e da Internet das Coisas (IoT) que vem sendo cada vez mais utilizados nos processos de produção das organizações. Entre os ataques mais comuns, estão os de negação de serviço (DoS) que sobrecarregam servidores e redes com tráfego excessivo, resultando na interrupção de serviços essenciais, incluindo aqueles que utilizam plataformas baseadas em *blockchain* e tecnologias de registro distribuídos (ETEMADI, GELDER, STROZZI. 2021). Além

disso, falhas de segurança em protocolos de comunicação que são amplamente utilizados em dispositivos IoT, possibilitam o acesso não autorizado e ataques que comprometem tanto da integridade quanto a disponibilidade das redes. Dispositivos com portas abertas e senhas frágeis representam vulnerabilidades exploradas por agentes maliciosos para invadir sistemas e manipular dados sensíveis, impactando desde processos agrícolas até operações logísticas dentro da cadeia de suprimentos (BHAT *et al.,* 2021).

2.2 Soluções de mitigações das ameaças

Qualquer tipo de ameaça cibernética pode vir a afetar o processo de produção e da cadeia produtiva. Consequentemente, qualquer solução eficaz exige a consideração de ambos os elos. Prevenir os ataques exige uma estratégia abrangente que considere aspectos físicos e digitais dos sistemas, combinando práticas de segurança voltadas tanto para a infraestrutura quanto para os sistemas operacionais e aplicativos (BHAT *et al.,* 2021).

No entanto, para compreender os aspectos relacionados à segurança, é necessário mapear as ameaças presentes ao longo das fases da cadeia de suprimentos. A análise do fluxo de elementos físicos e digitais bem como o reconhecimento de riscos envolvidos nesses cenários, pode auxiliar de maneira significativa na formulação e na construção de estratégias de segurança mais eficientes e alinhadas às especificidades da cadeia de suprimentos (GUPTA *et al.,* 2020).

A adoção de medidas preventivas e de boas práticas é para reforçar a proteção das cadeias de suprimento. Tecnologias inovadoras, como o uso de sistemas inteligentes para identificação de ameaças, a manutenção constante por meio de atualizações periódicas e a incorporação de soluções baseadas em inteligência artificial, contribuem de forma significativa para o aprimoramento das defesas cibernéticas. Além disso, estratégias voltadas ao fator humano, como o treinamento e conscientização em segurança da informação, são fundamentais para minimizar falhas decorrentes de comportamentos inseguros. Do mesmo modo, estabelecer políticas especificas de segurança cibernética e *frameworks* de cibersegurança são passos para consolidar uma estrutura de defesa coesa e eficiente (ADEWUSI, CHIEKEZIE, EYO-UDO. 2022).

Diante desses desafios, torna-se evidente a necessidade de adotar soluções eficazes que atendam às exigências crescentes de segurança nas cadeias de suprimentos, especialmente no contexto digital. 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 deste estudo.

2.2.1 Blockchain

O *blockchain* é uma tecnologia de registro descentralizado que permite a troca segura de dados entre participantes de uma rede. Essa base distribuída armazena blocos de informações conectados e protegidos contra alterações e fraudes. O *blockchain* combina múltiplas tecnologias, como ferramentas de desenvolvimento, criptografia, sistemas de banco de dados e análise de dados, o que expande consideravelmente seu leque de aplicações em diferentes áreas (KAMBLE *et al*., 2021).

Aplicada à cadeia de suprimentos, o *blockchain* promove uma integração eficiente entre os diversos participantes. Essa conectividade cobre todas as etapas da cadeia, favorecendo ganhos como maior transparência nas operações, rastreamento detalhado, redução de riscos, controle de processos produtivos e melhorias na documentação (BAYRAMOVA, EDWARDS, ROBERTS. 2021).

As principais vantagens do *blockchain* decorrem de suas características técnicas. A descentralização elimina a necessidade de intermediários para validar transações, reduzindo falhas e vulnerabilidades, enquanto a arquitetura *peer-to-peer* garante alta disponibilidade e dificulta interrupções. O controle seletivo do acesso protege a integridade dos dados, permitindo que apenas usuários autorizados compartilhem informações. A rastreabilidade é assegurada por registros permanentes e carimbos temporais, aumentando a confiabilidade das transações. A transparência fortalece a confiança entre os participantes e a segurança é reforçada por criptografia que previne os acessos não autorizados. A imutabilidade impede alterações nos registros sem o consenso da maioria dos nós, dificultando fraudes. Além disso, a tecnologia reduz custos operacionais ao eliminar intermediários e otimizar processos como auditorias e governança, enquanto seu sistema evita a inclusão de dados incorretos. Por fim, a estrutura distribuída permite atualizações simultâneas, elevando a eficiência e confiabilidade da rede (ETEMADI, GELDERM, STROZZI. 2021).

2.2.2 Smart contracts

Smart Contracts, ou contratos inteligentes, são programas automatizados que, integrados à tecnologia *blockchain*, executam transações automaticamente ao serem cumpridas certas condições. Na cadeia de suprimentos, eles permitem a transferência imediata de fundos ao fornecedor após o recebimento do produto conforme acordado (FARSI, RATHORE, BAKIRAS. 2021).

Além da automatização, os *smart contracts* asseguram resultados consistentes e passíveis de validação, como ocorre em processos de análise de crédito, nos quais diferentes partes podem revisar as operações garantindo precisão e confiabilidade. Também se destacam a imutabilidade e possibilidade de rastreamento,

proporcionadas pela tecnologia *blockchain*, o que dificulta ações fraudulentas e permite o acompanhamento detalhado de todas as execuções (ZHENG *et al.,* 2022).

2.2.3 *Frameworks* de segurança cibernética

Um *framework* pode ser entendido como uma estrutura sistematizada que guia a implementação de práticas, métodos ou tecnologias para alcançar objetivos específicos. No campo da cibersegurança e da tecnologia *blockchain,* os *frameworks* são desenvolvidos para enfrentar desafios como escalabilidade, interoperabilidade e proteção (ETEMADI, GELDER, STROZZI. 2021).

Um exemplo está nas parcerias público-privadas, que colaboram na criação de *framework* e normas de cibersegurança voltadas para setores específicos. Essas estruturas são elaboradas a partir do compartilhamento de informações sobre ameaças emergentes e melhores práticas, possibilitando que diferentes segmentos fortaleçam suas defesas conjuntas (ADEWUSI, CHIEKEZI, EYO-UDO. 2022).

No contexto da cadeia de suprimentos, destaca-se o NIST SP 800-161r1, um *framework* desenvolvido pelo National Institute of Stardards and Technology (NIST), que oferece orientações para a gestão de riscos de cibersegurança em cadeias de suprimentos de sistemas e organizações. Ele exemplifica como um *framework* pode ser formalizado por uma autoridade governamental e amplamente adotado para aumentar a resiliência e a segurança em nível setorial (BOYENS *et al.*, 2022).

Portanto, os *frameworks* têm em comum o objetivo de estruturar soluções para desafios complexos, fornecendo diretrizes organizadas e flexíveis que atendem às demandas específicas de cada área.

2.2.4 *Machine learning* (Inteligência Artificial)

O machine learning (ML), uma das áreas mais relevantes da inteligência artificial, tem sido progressivamente incorporado à gestão da cadeia de suprimentos devido à sua capacidade de simplificar processos complexos e promover a eficiência operacional (HASSIJA *et al.,* 2021).

Algoritmos de *deep learning* e *machine learning* podem ser utilizados para monitorar o comportamento de nós sensores em uma rede, a fim de detectar padrões de conduta suspeitos ou maliciosos. Ao comparar o comportamento atual de um nó com seu padrão comportamental previamente definido, é possível isolar ou remover o nó comprometido sem comprometer a integridade da rede como um todo (BHAT *et al.,* 2022). Tal abordagem é especialmente relevante em ambientes distribuídos e conectados, onde a presença de um único ponto de falha pode comprometer a segurança de toda a cadeia de suprimentos.

Além disso, estratégias de segurança fundamentadas em mecanismos de detecção precoce têm sido amplamente recomendadas para fortalecer a resiliência das cadeias de suprimentos diante de ameaças cibernéticas. Nessa perspectiva, algoritmos de inteligência artificial, quando aplicados em conjunto com práticas de gerenciamento de configurações e identificação de dados sensíveis, possibilitam a definição de parâmetros de referência para o monitoramento dos fluxos de informações entre sistemas e processos. Com base nessas referências, é possível aplicar técnicas analíticas baseadas em *machine learning* e inteligência artificial (IA) para detectar alterações anômalas nesses fluxos, as quais podem constituir indícios iniciais de exploração de falhas por atores com intenções maliciosas (MARTÍNEZ, DURÁN. 2021). Adicionalmente, o uso de algoritmos avançados permite a identificação de padrões incomuns que poderiam não ser notados por soluções tradicionais, reforçando a capacidade de respostas a incidentes e contribuindo para estratégias de mitigação mais eficazes na cadeia de suprimentos (ADEWUSI, CHIEKEZI, EYO-UDO. 2022).

Entretanto, é importante frisar que a eficácia dessas soluções baseadas em *machine learning* dependem fortemente da qualidade dos dados utilizados, da escolha apropriada dos algoritmos e da adoção de práticas éticas e transparentes. Modelos complexos que operam sem clareza sobre os dados de treinamento e os parâmetros empregados, podem comprometer tanto a confiança quanto a responsabilidade na tomada de decisões automatizadas (HASSIJA *et al.,* 2021).

2.3 CSCRM (*Cybersecurity Supply Chain Risk Management*)

A Gestão de Riscos de Cibersegurança na Cadeia de Suprimentos (*Cybersecurity Supply Chain Risk Managent* – C-SCRM) é um processo sistemáticos que visa proteger a cadeia de suprimentos contra ameaças cibernéticas que podem comprometer ativos, dados e operações da organização (BOYENS *et al.*, 2022). Ao comparar a abordagem que é utilizada na gestão de riscos da informação, o C-SCRM propõe uma visão mais abrangente integrando elementos como processos, pessoas e tecnologia, considerando o aspecto relacional entre os fornecedores, parceiros e terceiros da cadeia de suprimentos (SPEKMAN e DAVIS, 2004).

Baseada na teoria do C-SCRM, essa visão abrangente tem como consequência uma melhor resiliência cibernética que pode ser obtida por meio da identificação de um alinhamento apropriado entre o grau de risco presente na cadeia de uma organização e a sua capacidade de resposta para lidar com esses riscos. Por conseguinte, esse ajuste para aumentar a resiliência pode ser atingida ao reconhecer uma correspondência apropriada entre a exposição aos riscos da cadeia de suprimentos de uma empresa e o respectivo grau de prontidão para enfrentar esses riscos (CREAZZA *et al.,* 2022).

A abrangência do C-SCRM dentro da organização envolve diversos *stakeholders*, incluindo a segurança da informação, privacidade, desenvolvedores e implementadores de sistemas, aquisição, compras, área jurídica e recursos humanos (BOYENS *et aç,.*2022). Consequentemente, é necessário que a organização esteja comprometida e envolvida com o C-SCRM, principalmente da alta liderança, para que as ameaças sejam tratadas de forma eficiente (CREAZZA *et al.,* 2022).

Portanto, o C-SCRM é necessário para que as empresas saibam gerenciar os riscos cibernéticos de forma integrada e continua na cadeia de suprimentos, envolvendo diversas áreas da organização. Essa abordagem holística fortalece a resiliência contra ameaças, permite uma melhor tomada de decisão estratégica e reduz impactos negativos, garantindo a segurança e a continuidade dos negócios.

3 METODOLOGIA DE PESQUISA

A metodologia adotada para esta pesquisa baseou-se nos princípios da revisão sistemática da literatura, com o objetivo de identificar, analisar e sintetizar de maneira organizada e estruturada os estudos mais relevantes relacionados ao tema em questão. O processo foi conduzido em etapas bem definidas, garantindo precisão científica, clareza e possibilidade de reprodutibilidade dos resultados.

Com o intuito de identificar os principais termos e conceitos mais recorrentes na literatura, elaborou-se uma nuvem de palavras a partir da seleção de um referencial teórico previamente estabelecido. Esse procedimento permitiu a análise do estado do problema pesquisado, considerando a perspectiva teórica e os trabalhos acadêmicos já desenvolvidos sobre o tema (MARCONI; LAKATOS, 2003). Acerca disso, tornou-se possível nortear a pesquisa com uma fundamentação, sustentada por produções científicas relevantes, evidenciando o domínio adequado sobre as principais correntes teóricas que embasam e contextualizam o estudo.

O relatório técnico "*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations"* identificado como "NIST SP 800-161r1" e publicado em maio de 2022 pelo Instituto Nacional de Padrões e Tecnologia (NIST), foi adotado como um referencial teórico para o gerenciamento de riscos da cadeia de suprimentos. Especificamente, foi utilizado o tópico 2.2, intitulado "*Cybersecurity Risks Throught Supply Chains",* que apresenta uma visão detalhada sobre os riscos cibernéticos que se manifestam a partir da cadeia de suprimentos.

Para realizar a análise textual, foi utilizado a linguagem de programação R, com suporte do ambiente de desenvolvimento integrado RStudio. A partir de pacotes especializados em mineração de texto, foi realizado um pré-processamento de texto, envolvendo: conversão de todas as letras para minúsculas, remoção de pontuações, números, espaços em branco extras e eliminação de palavras irrelevantes em inglês. Ao possuir o texto limpo, foi construído uma *Term-Document Matrix* (TDM), que quantifica a frequência das palavras contidas no documento. A partir dessa matriz, foram extraídos os termos mais frequentes e, por consequência, gerada a nuvem de palavras. Na imagem gerada, exibida na Figura 1, as palavras que aparecem com maior tamanho são aquelas que mais aparecem no texto inserido e aquelas que ficam menores são as que menos aparecem.

O resultado apresentado mostra que as palavras que mais foram utilizadas foram: *supply, chain, cybersecurity, risk* e *vulnerabilities*.

Figura 1 – Nuvem de palavras

Fonte: Resultado da Pesquisa

Utilizando as palavras mais recorrentes no texto, foi possível identificar os principais temas abordados no conteúdo analisado, consequentemente, deu-se início a bibliometria sobre este estudo utilizando o software "*Publish or Perish v8.17.4863",* no dia 03 de maio de 2025, para levantar e identificar os artigos mais citados e influentes.

Nesta etapa do trabalho, foi utilizado as bases de dados Google Scholar e OpenAlex a fim de pesquisar os artigos referentes ao tema abordado entre o período de 2020 e 2025. Com base nas palavras identificadas na nuvem de palavras em conjunto com outras termos que fazem associação ao assunto em estudo, foram realizadas as seguintes buscas apresentadas na Tabela 1, resultando em um total de 2.566 registros encontrados.

Tabela 1 - Lista de pesquisas realizadas

Título	**Palavra-chave**	**Base de Dado**	**Resultados**
Supply chain OR "Third-Party" OR "Vendor"	("Supply chain" OR "Third-Party" OR "Vendor") AND ("Cybersecurity" OR "Information Security") AND ("risk" OR " vulnerabilities" OR "threats")	Google Scholar	995
"Supply Chain"	Cybersecurity AND "threats"	OpenAlex	371
"Supply Chain"	cybersecurity risk AND cybersecurity threats	OpenAlex	329
("Cybersecurity" OR "Information Security")	("Supply chain" OR "Third-Party" OR "Vendor") AND	Google Scholar	268

AND ("Supply" OR "Third Party")	("Cybersecurity" OR "Information Security") AND ("risk" OR " vulnerabilities" OR "threats")		
Supply Chain	cybersecurity AND risk AND vulnerabilities AND threats	OpenAlex	248
Supply Chain	Supply Chain AND "Cybersecurity risk"	OpenAlex	137
Supply Chain	Cybersecurity AND cyberattacks	OpenAlex	126
Supply Chain	Supply Chain AND "cybersecurity threats"	OpenAlex	92

Fonte: OpenAlex e Google Scholar

A inclusão do termo "*cyberattacks*" entre as palavras-chave utilizadas na análise bibliométrica deu-se pela sua centralidade conceitual no campo da segurança da informação. Esse termo é amplamente empregado na literatura científica e técnica para designar ações maliciosas que visam comprometer sistemas computacionais, redes ou dados, alinhando-se diretamente com o estudo das ameaças cibernéticas e suas formas de mitigação.

Durante a etapa de triagem, foi realizada a verificação de duplicidade entre os registros coletados. Como resultado, 1.226 artigos duplicados foram identificados e excluídos do processo, restando 1.340 registros únicos que seguiram para as próximas fases da análise.

Também foram retirados 50 registros que não continham informações sobre a data em que foi publicado, totalizando 1.290 registros selecionados até o momento.

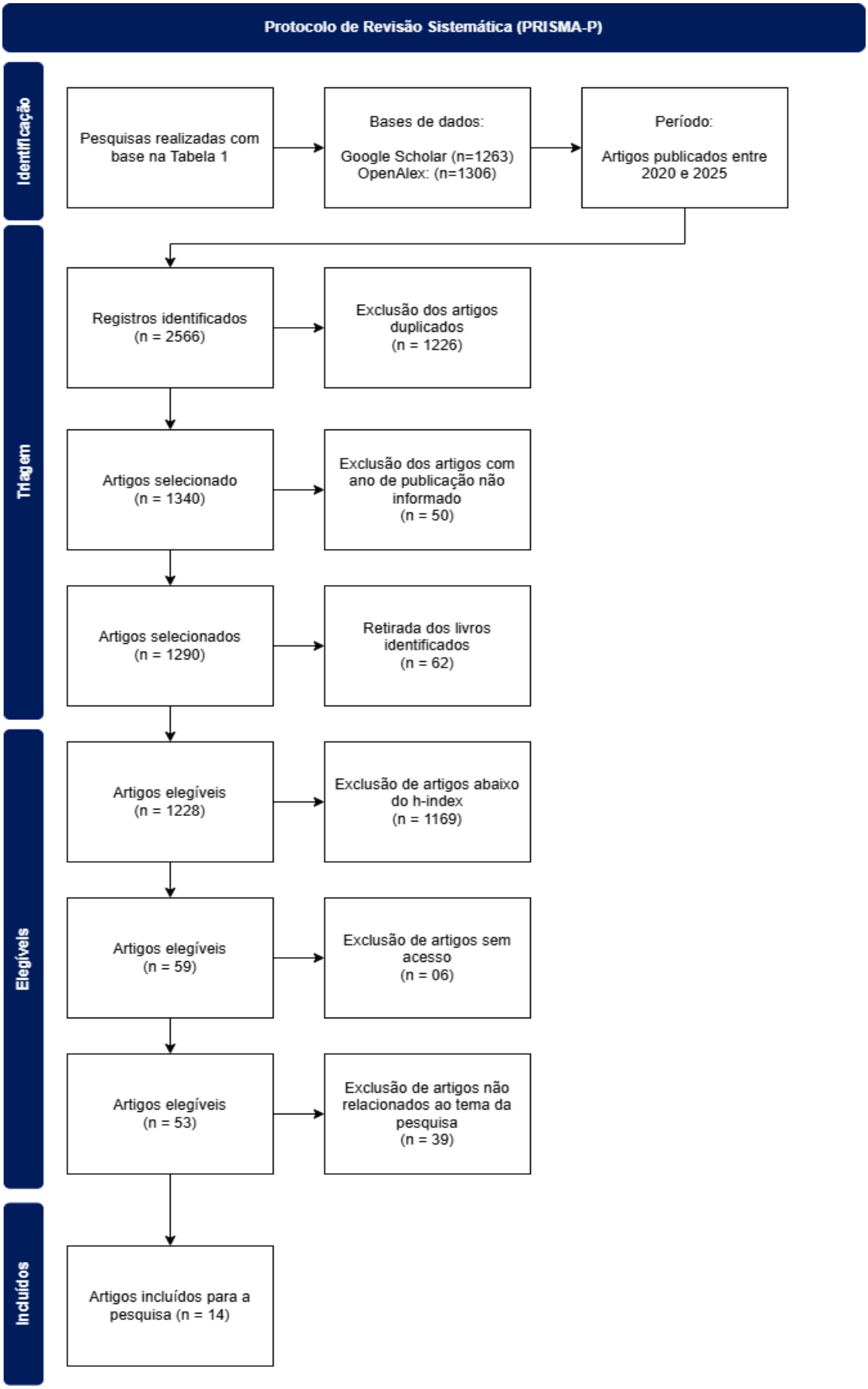
Além disso, foram excluídos 62 registros que foram identificados como livro ou patente, tendo em vista que uma grande parte dos livros não tendem a acompanhar com a mesma velocidade os avanços tecnológicos e normativos. Assim, optou-se por priorizar o uso de artigos acadêmicos e publicações técnicas que proporcionem uma abordagem mais atualizada e especializada. Ao fim deste processo, sobraram um total de 1.228.

Durante a etapa de registros elegíveis, realizou-se o corte dos artigos que possuíam um total de citações abaixo do h-index (n = 57), totalizando 1.169 registros excluídos e um total de 59 registros para verificação pós-triagem.

Ao tentar acessar os 59 registros de artigos elegíveis, constatou-se que seis registros não estavam acessíveis, fazendo com essa quantia fosse removida, totalizando 53 registros para serem verificados. Após a avaliação dos registros, foram selecionados 14 registros que continham as informações procuradas.

Diante dessas informações, empregou-se o protocolo PRISMA para representar os resultados obtidos conforme ilustrado na Figura 2.

Figura 2 – Diagrama/Fluxo do protocolo PRISMA-P



Fonte: Fundamentado na estrutura PRISMA-P

Os artigos incluídos na seleção estão dispostos na Tabela 2.

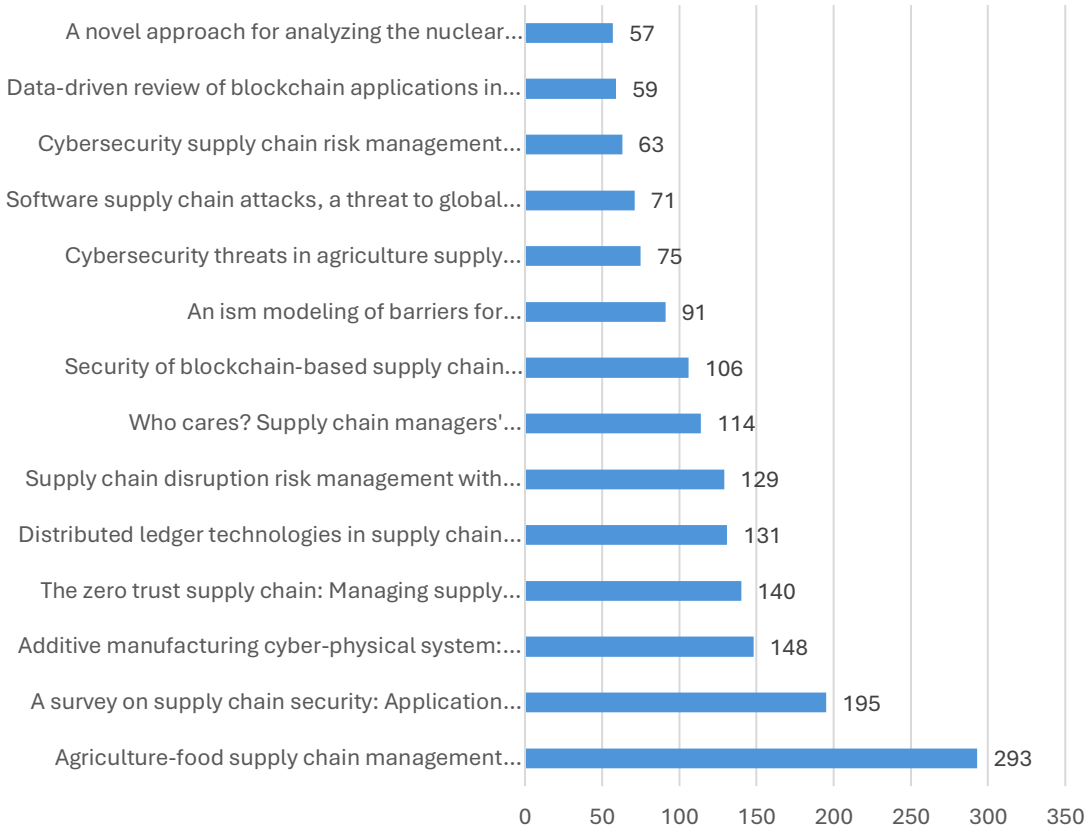
Tabela 2 - Tabulação dos artigos incluídos na pesquisa

ID	CITAÇÕES	NOME	PUBLICADOR	ANO	AUTOR	PAÍS
1	293	Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability	mdpi.com	2021	Showkat Ahmad Bhat, Nen-Fu Huang, Ishfaq Bashir Sofi, Muhammad Sultan	Taiwan, Canada, Paquistão
2	195	A survey on supply chain security: Application areas, security threats, and solution architectures	ieeexplore.ieee.org	2020	Vikas Hassija , Vinay Chamola , Senior Member, IEEE, Vatsal Gupta, Sarthak Jain, and Nadra Guizani	India e USA
3	148	Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks	ieeexplore.ieee.org	2020	Nikhil Gupta, Akash Tiwari, Satish T. S. Bukkapatnam, Ramesh Karri	EUA
4	140	The zero trust supply chain: Managing supply chain risk in the absence of trust	Taylor &Francis (International Journal of Production Research)	2021	Zachary A. Collier, Joseph Sarkis	EUA e Finlandia
5	131	Distributed ledger technologies in supply chain security management: A comprehensive survey	ieeexplore.ieee.org	2021	Mary Asante, Gregory Epiphaniou, Member, IEEE Carsten Maple, Fellow, IEEE, Haider Al-Khateeb, Mirko Bottarelli, Kayhan Zrar Ghafoor	Reino Unido e Iraque
6	129	Supply chain disruption risk management with blockchain: A dynamic literature review	mdpi.com	2021	Niloofar Etemadi, ORCID,Yari Borbon-Galvez, ORCID, Fernanda Strozzi ORCID and Tahereh Etemadi	Bélgica, Irã e Itália
7	114	Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era	emerald.com	2022	Alessandro Creazza Claudia Colicchia Salvatore Spiezia Fabrizio Dallari	Itália
8	106	Security of blockchain-based supply chain management systems: challenges and opportunities	mdpi.com	2021	Sana Al-Farsi,Muhammad Mazhar Rathore and Spiros Bakiras	Qatar
9	91	An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity	mdpi.com	2021	Niloofar Etemadi, Pieter Van Gelder, Fernanda Strozzi	Itália, Holanda
10	75	Cybersecurity threats in agriculture supply chains: A comprehensive review	researchgate.net	2022	Adebunmi Adewusi, Nsisong Louis Eyo-Udo	EUA e Nigéria
11	71	Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study	iieta.org	2021	Jeferson Martínez, Javier M. Durán	Colômbia
12	63	Cybersecurity supply chain risk management practices for systems and organizations	csrc.nist.gov	2022	Jon Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, Matthew Fallon	EUA
13	59	Data-driven review of blockchain applications in supply chain management: key research themes and future directions	Taylor &Francis	2023	Truong Van Nguyen, Hiep Cong Fama, Minh Nhat Nguyen, Li Zhou, Mohammadreza Akbari	Reino Unido, Vietnã, Austrália
14	57	A novel approach for analyzing the nuclear supply chain cyber-attack surface	Elsevier	2021	Shannon Eggers	EUA

Fonte: Resultado da Pesquisa

O Figura 3 apresenta uma visualização ordenada com base na quantidade de citações recebidas por cada artigo, permitindo facilitar a identificação dos artigos mais referenciados até os menos mencionados.

Figura 3 – Gráfico de citações por artigo

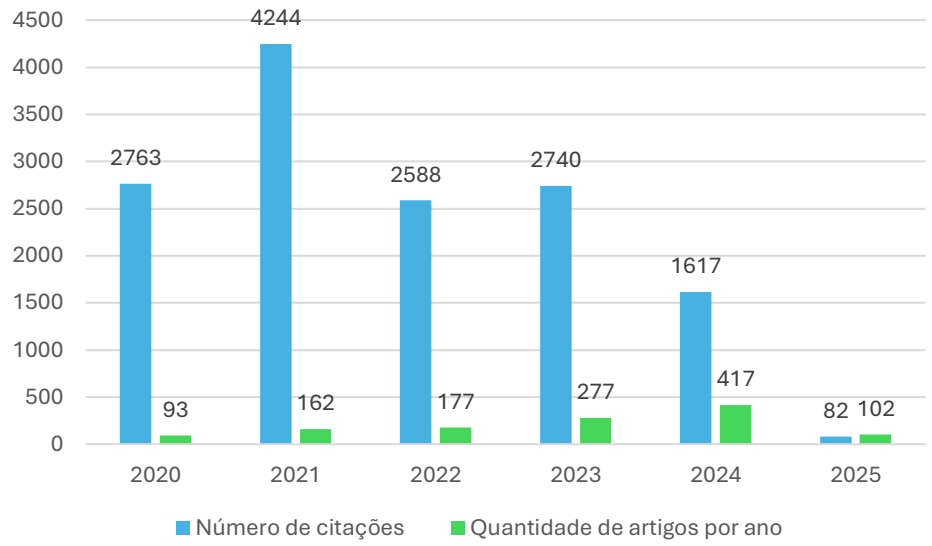


Fonte: Resultado da Pesquisa

Como por ser visto, o artigo "*Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability*" possui 293 citações sendo o artigo mais citado dentre os selecionados. Já o artigo "*A novel approach for analyzing the nuclear supply chain cyber-attack surface*", dentre todos os artigos selecionados é o que possui menos citações, tendo um total de 57 citações.

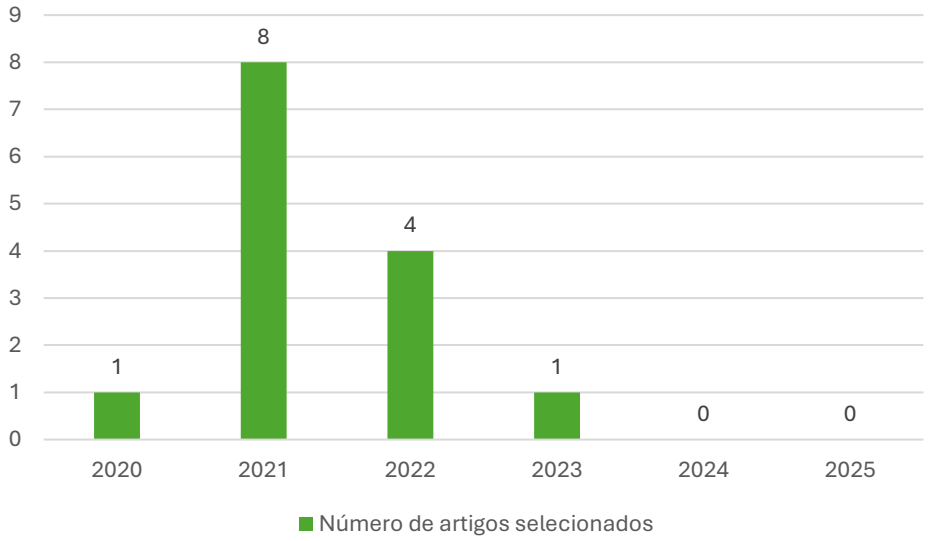
Com o objetivo de compreender a evolução do interesse acadêmico no tema e o impacto das publicações ao longo do tempo, foram analisados quatro conjuntos de dados: o primeiro referente ao total de artigos elegíveis, o segundo composto da quantidade total de citações das publicações elegíveis, o terceiro constituído apenas pelos artigos que atenderam aos critérios de inclusão e exclusão definidos, e o quarto constituído a partir das citações pertencentes as publicações selecionadas.

Figura 4 – Publicações e citações por ano no período analisado (Elegíveis)



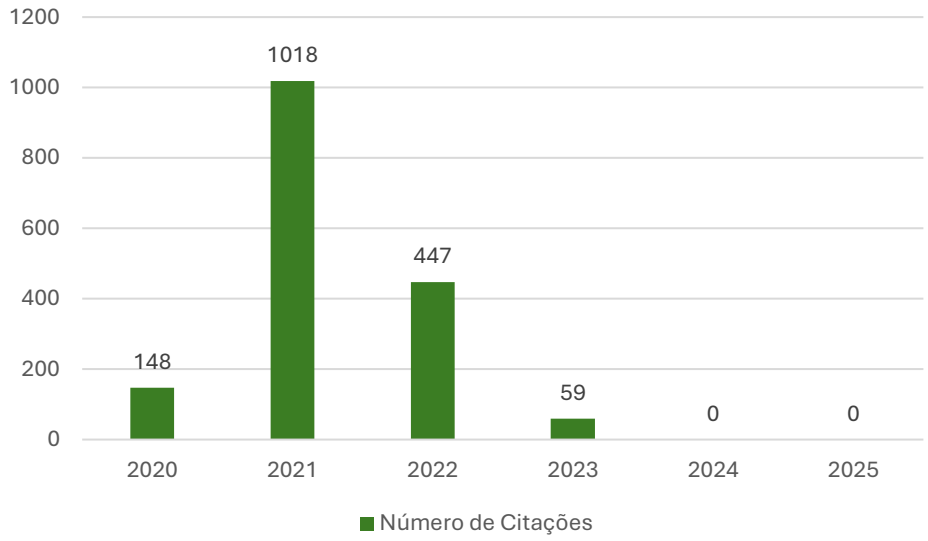
Fonte: Resultado do levantamento dos artigos elegíveis

Figura 5 – Publicações por ano no período analisado (Selecionados)



Fonte: Resultado da Pesquisa

Figura 6 – Citações anuais dos artigos selecionados



Fonte: Resultado da Pesquisa

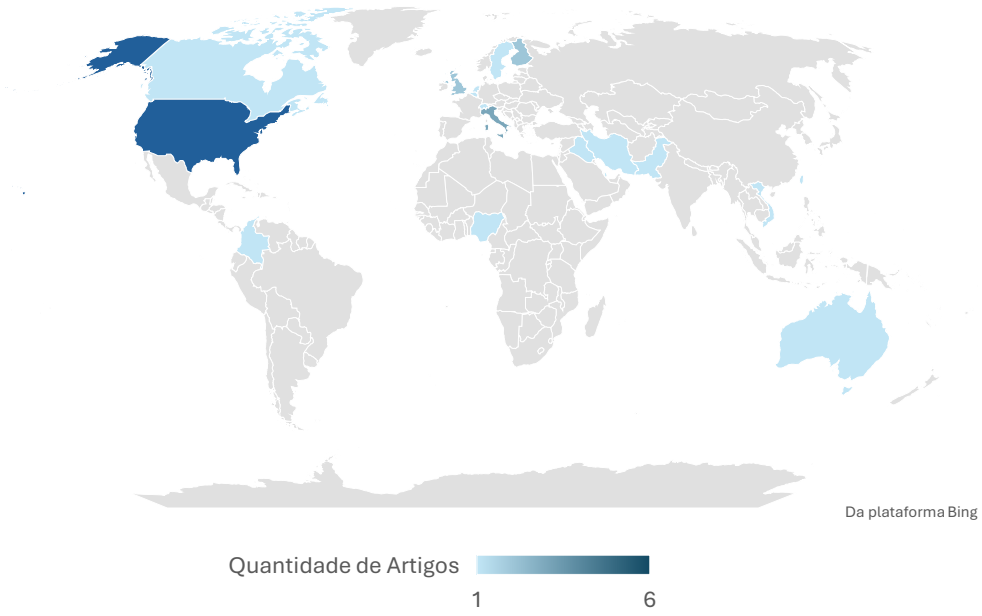
O Figura 4 que representa a quantidade de publicações e citações dos artigos elegíveis, ou seja, aqueles poderiam fazer parte da análise final. Nele, é possível verificar que, no ano de 2020, foram publicados 93 artigos que, juntos, acumulam 2.763 citações. Em 2021, houve 162 publicações que totalizam 4.244 citações. No ano seguinte, foram divulgados 177 artigos totalizando 2.588. Já em 2023, foram identificados 277 artigos que juntos correspondem a 2.740 citações. Em 2024, registraram-se 417 artigos, que juntos somam 1.617 citações. Por fim, até maio de 2025, houve apenas 102 artigos publicados totalizando 82 citações.

Conforme o Figura 5 e o Figura 6, por sua vez, representam os dados dos conjuntos finais de artigos selecionados. Neles, é possível observar que, em 2020, foi selecionado apenas uma publicação com 148 citações. No ano seguinte, 2021, foram selecionados oito artigos, totalizando 1.018 citações. Em 2022 foram quatro publicações com um total de 447 citações, e em 2023 apenas 1 artigo foi selecionado, com 59 citações. Além disso, como pode ser observado, dos artigos selecionados, nenhum deles foi publicado nos anos de 2024 e 2025.

O *software* "*Publish or Perish v8.17.4863"*, utilizado para a busca dos artigos, não disponibiliza diretamente o país de origem das publicações obtidas, o que impossibilitou o levantamento dessas informações para todos os artigos elegíveis. Essas limitações ocorrem porque os dados extraídos, principalmente da base de dados Google Scholar, não incluem um campo específico com essas informações. Entretanto, foi possível realizar a análise manualmente para os artigos que foram selecionados na etapa final, por meio das afiliações institucionais dos autores, permitindo uma visão precisa sobre quais são os países que mais contribuíram com

publicações relevantes para o estudo dentro do conjunto final analisado conforme a ilustração da Figura 7.

Figura 7– Distribuição de publicações por país



Fonte: Resultado da pesquisa

Para aprimorar a visualização e a compreensão dos dados, foi inserida a Tabela 3 contendo a quantidade de artigos citados por país. Essa apresentação permite uma visão mais clara sobre quais foram as nações que mais contribuíram, em termos quantitativos, com as publicações relevantes entre os artigos selecionados.

Tabela 3 - Distribuição de publicações por país

Países	Quantidade de Artigos
EUA	6
Itália	3
Finlândia	2
Reino Unido	2
Canadá	1
Taiwan	1
Paquistão	1
Suécia	1
Suíça	1
Iraque	1
Bélgica	1
Irã	1
Qatar	1
Holanda	1

Nigéria	1
Colômbia	1
Vietnã	1
Austrália	1

Fonte: Resultado da Pesquisa

Com a Figura 7 e a Tabela 3 observa-se uma predominância de publicações oriundas dos Estados Unidos e seguido pela Itália. Essa análise permite compreender a concentração geográfica da produção científica sobre o tema, o que pode influenciar nas abordagens metodológicas e nos contextos analisados.

4 ANÁLISE DE RESULTADOS

Nesta seção, são apresentados os principais resultados obtidos a partir da revisão sistemática e análise bibliométrica realizada. Foram analisados os artigos selecionados que mais citados, os países que possuem maior número de publicações, além da evolução da quantidade de artigos e citações ao longo do tempo, considerando os dados antes e após a aplicação dos critérios de elegibilidade. Além disso, são apresentados uma avaliação dos principais tipos de gerenciamentos, tecnologias e ameaças relacionadas à segurança da cadeia de suprimentos (*supply chain*) dos artigos selecionados. Esses dados permitem compreender as tendências da pesquisa na área de segurança cibernética e da informação na área de *Supply Chain*, os focos predominantes dos estudos e os temas de maior relevância científica.

4.1 Artigos mais citados

Nesta subseção, são apresentados os artigos selecionados na análise que obtiveram maior número de citações. O objetivo é destacar as publicações de maior impacto acadêmico dentro da seleção estabelecida, considerando que a quantidade de citações pode influenciar nos estudos científicos e refletir na relevância do assunto além de fornecer um resumo conciso sobre conteúdo de cada artigo selecionado.

Conforme o Figura 3, observa-se que os artigos mais citados abordam temas diretamente ligados à aplicação de tecnologias emergentes na segurança das cadeias de suprimentos. O destaque vai para o artigo "*Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability*", com 293 citações, refletindo no interesse na interoperabilidade de blockchain empresariais e no uso da IoT para rastreabilidade no setor agroalimentar. Em segundo lugar, encontra-se o artigo "*A survey on supply chain security: Application areas, security threats, and solution architectures"*, com 195 citações, demonstra sua importância como base teórica ao oferecer uma visão abrangente sobre ameaças e arquitetura de segurança. Já o terceiro mais citado, "*Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks",* com 148 citações, ressalva os riscos associados à manufatura aditiva e sistemas ciber-físicos, mostrando o impacto dessas tecnologias no aumento da complexidade e vulnerabilidade das cadeias de suprimentos. Dessas publicações com mais citações, observa-se a uma valorização de soluções tecnológicas como resposta às crescentes exigências por segurança e resiliência nesse contexto.

Na sequência, são apresentados os conteúdos analisados dos 14 artigos selecionados.

1° Artigo: *Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability* (BHAT *et al.,* 2021) propõe a arquitetura Agri-SCM-BIoT, que integra blockchain e internet das coisas (IoT) para aprimorar a gestão das cadeias de suprimentos agrícolas, especialmente frente à crescente complexidade e interconectividade desses sistemas. A pesquisa destaca a demando por maior transparência, rastreabilidade, segurança e sustentabilidade, ao mesmo tempo que analisa os riscos cibernéticos associados à cadeia de suprimentos e IoT, como falhas de autenticação, falta de transparência e ausência de criptografia. O blockchain surge, assim, como uma solução viável para mitigar essas vulnerabilidades e fortalecer a segurança e integridade das operações na agricultura.

2° *A survey on supply chain security: Application areas, security threats, and solution architectures* (HASSIJA *et al.,* 2021) aborda os desafios e ameaças de segurança nas cadeias de suprimentos diante da crescente conectividade global e do aumento do comércio internacional. O artigo analisa as vulnerabilidades existentes e apresenta tecnologias emergentes focadas na segurança, como blockchain, aprendizado de máquina (IA) e funções fisicamente unclonáveis (PUFs), que podem contribuir para mitigar riscos cibernéticos e fraudes.

3° Artigo: *Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks* (GUPTA *et al.,* 2020) apresenta a manufatura aditiva (AM) que tem se destacado por sua eficiência e flexibilidade, integrando cadeias de suprimentos físicas e digitais em um sistema cyber-físico. Essa integração traz novas ameaças de segurança, como ataque aos equipamentos, materiais e projetos, além de ameaças como engenharia reversa e falsificação. O artigo destaca a necessidade de atualizar as estratégias de cibersegurança para proteger toda a cadeia de suprimentos da AM, identificando vulnerabilidades e lacunas nas soluções atuais.

4° Artigo: *The zero trust supply chain: Managing supply chain risk in the absence of trust* (COLLIER, SARKIS. 2021) introduz a ideia de uma cadeia de suprimentos com *zero trust*, considerando que todos os participantes podem representar riscos. Essa estratégia fortalece a segurança interna por meio de rigorosos mecanismos de controle de acesso, em oposição às abordagens tradicionais focadas na proteção do perímetro.

5° Artigo: *Distributed ledger technologies in supply chain security management: A comprehensive survey* (ASANTE *et al.*, 2021) apresenta os desafios que as cadeias de suprimentos enfrentam que elevam os custos e atrasam processos. Tecnologias de Ledger Distribuídos (DLT) podem diminuir esses problemas ao aumentar a transparência, descentralização do controle e a melhoria da gestão da informação.

6° Artigo: *Supply chain disruption risk management with blockchain: A dynamic literature review* (ETEMADI *et al.* 2021) analisa o uso do blockchain para aumentar a resiliência das cadeias de suprimentos diante de riscos e incertezas. Utilizando uma abordagem bibliométrica chamada SLNA, a pesquisa combina revisão sistemática e análise de redes da literatura. O trabalho enfatiza a importância do blockchain no

controle de riscos digitais, no reforço da proteção das cadeias de suprimentos, abordando temas como proteção de dados, o uso de *smart contracts*, sistemas de rastreamento e prevenção de fraudes.

7° Artigo: *Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era* (CREAZZA *et al.* 2022) apresenta as percepções de gestores sobre riscos cibernéticos nas cadeias de suprimentos, destacando a necessidade de estratégias alinhadas entre os diferentes atores. A pesquisa foi realizada com empresas do setor de bens de consumo na Itália e propõe uma taxonomia de riscos cibernéticos, considerando falhas em sistemas, malwares, vazamento de dados e roubo de credenciais, reforçando que, além da probabilidade e impacto, a ocorrência real dos incidentes de também deve ser levada em conta para aprimorar a capacidade de respostas cibernéticas da cadeia de suprimentos.

8° Artigo: *Security of blockchain-based supply chain management systems: challenges and opportunities* (AL-FARSI, RATHORE, BAKIRAS. 2021) investiga as ameaças práticas e vulnerabilidades presents em sistemas de gestão de cadeias de suprimentos baseados em blockchain. Embora a tecnologia ofereça benefícios ainda existem riscos significativos de ataques cibernéticos. O trabalho analisa vulnerabilidades relacionados com *smart contracts*, ao ambiente de excução do blockchain e à confiança entre os serviços da cadeia. Ao mapear os desafios técnicos, o artigo destaca pesquisas que precisam ser exploradas para garantir a segurança efetiva desses sistemas.

9° Artigo: *An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity* (ETEMADI, GELDER, STROZZI, 2021) foca nos principais desafios de segurança na adoção do blockchain para gestão de riscos cibernéticos nas cadeias de suprimentos. Por meio da modelagem estrutural interpretativa (ISM), se identificam questões críticas, como a imaturidade tecnológica, vulnerabilidades em *smart contracts*, a robustez e a confiabilidade do sistema. O artigo ressalta a importância de superar barreiras para fortalecer a proteção e resiliência cibernética nas cadeias de suprimentos usando o blockchain.

10° Artigo: *Cybersecurity threats in agriculture supply chains: A comprehensive review* (ADEWUSI, CHIEKEZIE, EYO-UDO. 2022) aborda os riscos cibernéticos nas cadeias de suprimentos do setor agrícola, ressaltando fragilidades decorrentes do uso de tecnologias como IoT e blockchain. Nele é evidenciado os prejuízos financeiros e operacionais causados por ataques, além de destacar a necessidade de implementar controles de segurança, manter os sistemas atualizados, utilizar inteligência artificial e promover capacitações. Além disso, salienta a relevância de políticas regulatórias e da cooperação entre setores público e privado para assegurar a resistência e continuidade dessas cadeias em ambiente digital crescente.

11° Artigo: *Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study* (MARTÍNEZ, DURÁN. 2021) Analisa o ataque à cadeia de suprimentos exemplificado pelo caso SolarWinds, no qual a reutilização massiva de código aberto e de terceiro gerou vulnerabilidades explorada pelos invasores. A pesquisa revisa literatura acadêmica, relatórios governamentais e publicações de empresas de segurança e propõe práticas de defesa, como *zero trust,* autenticação multifator e uso de *software bill of materials* (SBOM).

12° Artigos: *Cybersecurity supply chain risk management practices for systems and organizations* (BOYENS *et al.* 2022) é um guia técnico desenvolvido *pela National Institute of Standards and Technology* (NIST) que orienta organizações a identificar, avaliar e mitigar riscos cibernéticos na cadeia de suprimentos, especialmente relacionados à presença de funcionalidades maliciosas, falsificações e vulnerabilidades decorrentes de práticas inadequadas. Esse artigo ressalva a importância de incorporar a gestão de riscos cibernéticos na cadeia de suprimentos (C-SCRM) às práticas de gerenciamento de riscos organizacionais, por meio de criação de estratégias, diretrizes e planos estruturados que assegurem a proteção, robustez e confiabilidade dos produtos e serviços ao longo de seu ciclo de vida.

13° Artigo: *Data-driven review of blockchain applications in supply chain management: key research themes and future directions* (NGUYEN *et al.* 2022) apresenta uma abordagem de revisão da literature sobre aplicações de blockchain na gestão da cadeia de supriementos. O estudo analisou 108 artigos identificando dez temas principais, como rastreabilidade, sustentabilidade e logística. Também sugere cinco caminhos futuros, como integração com outras tecnologias, uso de criptoativos e foco em impactos socioambientais.

14° Artigo: *A novel approach for analyzing the nuclear supply chain cyber-attack surface* (EGGERS, 2021) Analisa as vulnerabilidades cibernéticas na cadeia de suprimentos do setor nuclear, destacando que, apesar dos avanços na proteção das instalações, a cadeia de fornecimento continua exposta a riscos. O artigo apresenta um diagrama da superfície de ataque cibernético na cadeia de suprimentos com a finalidade de auxiliar na detecção de vulnerabilidades associadas a hardware, firmware, software e dados de sistema durante todas as etapas do ciclo de vida da cadeia. Esse instrumento funciona como apoio estratégico para especialistas e estudiosos afeiçoarem métodos e soluções voltados à gestão de riscos cibernéticos no setor.

4.2 Evolução das publicações e citações (antes e depois da seleção)

Este tópico aborda a evolução das quantidades de publicações e das citações entre os anos de 2020 e 2025. Inicialmente, é realizada a análise do Figura 4 que representa a quantidade de publicações e citações do conjunto inicial de artigos, ou

seja, antes da aplicação dos critérios de seleção. Em seguida, serão analisados o Figura 5 e o Figura 6, que apresentam os dados referentes ao conjunto final dos artigos selecionados, já filtrados de acordo com os critérios estabelecidos na metodologia. É essencial destacar que os dados referentes a 2025 foram apresentados nos gráficos, contudo, não foram analisados nem comparados com os anos anteriores por se tratar de um ano que ainda está em curso.

Na Figura 4, observa-se um crescimento contínuo no número de publicações ao longo do ano. Em 2020, foram publicados 93 artigos, número que aumentou em 2021, chegando a 162 artigos. Esse crescimento manteve-se nos anos seguintes, 177 em 2022, 277 em 2023 e um pico em 2024, com 417 publicações. Entretanto, observa-se que a quantidade de citações não acompanhou essa mesma tendência de alta. O pico ocorreu em 2021, com uma soma de 4.244 citações, mesmo com número inferior de publicações em relação aos anos seguintes. Em 2022 e 2023, as citações apresentaram variação, com 2.588 e 2.740 registros, respectivamente. Por sua vez, em 2024, apesar do elevado volume de artigos publicados, o total de citações registrou queda, atingindo apenas 1.617.

Esse contraste entre o volume de publicações e o número de citações pode indicar, entre outras possiblidades, uma saturação do tema nos anos mais recentes, uma possível redução na relevância dos artigos publicados ou ainda que os artigos mais recentes ainda não tiveram tempo suficiente para serem amplamente citados. Tais aspectos reforçam a importância de análise qualitativas complementares, como a seleção criteriosa dos estudos mais relevantes.

Embora esse descompasso entre o volume de publicações e o número de citações possa oferecer *insights* significativos, cabe destacar que este não é objetivo central desta pesquisa. Por essa razão, tais aspectos não serão explorados em profundidade.

Em seguida, a Figura 5 e a Figura 6 apresentam os dados que correspondem ao conjunto final dos artigos selecionados. Ao comparar com o panorama inicial, é possível observar o impacto da aplicação dos critérios de elegibilidade na representatividade das citações.

O Figura 5 mostra que após a aplicação dos critérios de elegibilidade, apenas 14 artigos foram considerados significativos para o estudo. Em 2020, apenas um artigo foi considerado relevante para compor o conjunto final da análise. Em 2021, o número de artigos selecionado aumentou para oito, representando o pico de inclusão no período analisado. Já em 2022, houve uma queda para quatro artigos, seguida de uma nova queda em 2023, com apenas um artigo selecionado. Por fim, nenhum artigo foi incluído na seleção final em 2024 ou em 2025, o que pode estar relacionado à baixa maturidade desses trabalhos ou ao fato de não atenderem aos critérios definidos.

A Figura 6, por sua vez, mostra que, mesmo após uma redução expressiva no número de publicações, o número de citações dos artigos selecionados permanece elevado, o que reforça a relevância dos estudos filtrados. Em 2020, o artigo possui sozinho um total de 148 citações. O ano de pico no período analisado, 2021, concentrou 1.018 citações provenientes dos oito artigos selecionados. Em 2022, os quatro artigos escolhidos totalizaram 447 citações e, por fim, em 2023, o único artigo selecionado deste ano teve 59 citações. Assim como observado anteriormente, os anos de 2024 e 2025 não apresentaram citações uma vez que nenhum artigo foi selecionado nesses períodos.

A partir dessa análise, observa-se que ao comparar os dados apresentados no Figura 4 com os das Figuras 5 e 6, o conjunto inicial demostra uma tendência de crescimento no número de publicações ao longo dos anos, esse aumento não foi acompanhado de uma elevação proporcional nas citações. Por outro lado, os dados do conjunto final revelam que, embora o número de publicações seja menor, os artigos selecionados apresentam maior densidade de citações, indicando que os estudos selecionados têm maior impacto acadêmico.

O aumento expressivo no número de citações em 2021 está ligado ao impacto da pandemia da COVID-19 nas cadeias de suprimentos globais. A crise global evidenciou a fragilidade das cadeias tradicionais, que passaram a depender cada vez mais de sistemas digitais interconectados e tecnologia da informação para garantir a continuidade operacional (HASSIJA, 2021). Essa dependência crescente resultou em uma crescente exposição a novas vulnerabilidade, sobretudo em ambientes remotos e distribuídos.

Além disso, o rápido avanço da digitalização durante a pandemia, incluindo o uso intensificado de dispositivos IoT, sistemas em nuvem e plataformas blockchain, aumentou significativamente a superfície de ataque para agentes maliciosos (ADEWUSI, CHIEKEZIE, EYO-UDO. 2022). Por fim, a dificuldade em manter operações seguras durante os períodos de restrições e lockdowns, combinada à aceleração da transformação digital, impulsionou o desenvolvimento de soluções de cibersegurança mais robustas e integradas.

Portanto, como pode ser visto, 2021 se destaca como o ano com maior concentração de artigos e de citações, indicando que esse período particularmente produtivo e relevante para o tema em questão. Além disso, observa-se que o ano de 2024 apresentou uma baixa representatividade em citações, o que pode estar associado ao pouco tempo de exposição dessas publicações.

4.3 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. Este

subtópico apresenta os dados referentes às nacionalidades das afiliações institucionais dos autores dos artigos selecionados.

A partir da Figura 7 em conjunto com a Tabela 3, observa-se uma forte concentração da produção científica em determinados países, indicando polos de pesquisas mais consolidados com o tema em questão. Os Estados Unidos se destacam de forma expressiva, com 6 publicações, o que representa a maior contribuição entre os países analisados. Essa predominância pode estar associada ao alto investimento em pesquisa e desenvolvimento, bem como à ampla infraestrutura acadêmica disponível no país. Além disso, a expressiva participação dos Estados Unidos no volume de publicações pode estar relacionada ao fato de o país ser um dos principais alvos de ataques cibernéticos em escala global. Como uma das maiores economias do mundo e com forte presença tecnológica em setores estratégicos. 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 Finlândia e Reino unido, cada um com duas publicações. Esses países também são conhecidos por suas universidades de alto impacto na área de tecnologia.

Além desses, dos artigos selecionados, nota-se uma ampla diversidade de nacionalidades com uma única publicação como Canadá, Taiwan, Paquistão, Suécia, Suíça, Iraque, Bélgica, Irã, Qatar, Holanda, Nigéria, Colômbia, Vietnã e Austrália.

Essa diversidade geográfica, ainda que concentrada em maior escala em países desenvolvidos, demonstra que o debate científico sobre o tema da pesquisa é amplamente disseminado, com contribuições relevantes vindas de todos os continentes.

4.4 Ameaças cibernéticas e soluções na cadeia de suprimentos

Neste tópico, é apresentada uma análise que relaciona as ameaças cibernéticas na cadeia de suprimentos com as soluções de mitigação identificadas na literatura. Em seguida, as ameaças e as soluções de segurança da informação foram segregadas por técnicas de ataques e categorias organizadas de controle (medidas de segurança), respectivamente. 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. Por fim, foi desenvolvida com base na análise, uma correlação das técnicas de ataques com as categorias organizadas de controle da segurança da informação.

Com base na análise dos artigos selecionados, foi realizado um levantamento abrangente das ameaças cibernéticas que foram mencionadas. Em seguida, realizou-se a tabulação das ameaças citadas por artigo, conforme apresentado na Tabela 4, permitindo visualizar a frequência e a distribuição das principais ameaças discutidas na literatura. Essa sistematização oferece uma base para compreender os pontos críticos abordados nas pesquisas sobre segurança na cadeia de suprimentos.

Tabela 4 - Tabulação das ameaças citadas por artigo

ARTIGO	AMEAÇAS			
1	Ataque de interferência de RF	Malware	Negação de serviço	BOTNET
	Ataque de canal lateral	Ataque de repetição	Man-in-the-middle	Ataque de verificador roubado
	Ataques de força bruta	Insider Threat	Falta de transparência	Ataques a Dispositivos IoT
	Ataque de chave conhecido	Resiliência contra ataque de captura de dispositivo de detecção	Ataque de implantação de dispositivo desonesto	Ataque de buraco de minhoca
	Encaminhamento seletivo	Ataque de enfraquecimento	Ataque de 51%	Ataques de eclipse
	Ataques Sybil	Ataque de buraco negro		
2	Falsificação de informações ou ativos	Vazamento/Violação de Dados	Falta de transparência	Sniffing
	Spoofing	Man-in-the-middle	Negação de serviço	Rastreamento não autorizado
	Fraudes			
3	Falsificação de informações ou ativos	Falta de rastreabilidade	Engenharia reversa	Ataque de verificador roubado
	Ataque de canal lateral			
4	Falta de Confiança entre Partes	Falsificação de informações ou ativos	Fraudes	
5	Erros humanos	Fraudes	Manipulação automática	SQL injection
	Roubo de credenciais (Credential Theft)	Negação de serviço	Ataques Sybil	Ataques de eclipse
	Falsificação de informações ou ativos	Ataque de 51%		
6	Fraudes	Falsificação de informações ou ativos	Falta de transparência	Erros humanos
	Falta de rastreabilidade	Falha na coleta e transmissão		
7	Phishing	Falsificação de informações ou ativos	Extorsão / Chantagem (blackmailing)	Spyware
	Malware	Vazamento/Violação de Dados	Comprometimento de redes	Roubo de credenciais (Credential Theft)
	Falha no sistema ERP	Negação de serviço		
8	Falsificação de informações ou ativos	Modificação de contratos	Ataques por má configuração	Falta de Confiança entre Partes
	Ataques Sybil	Man-in-the-middle		
9	Vazamento/Violação de Dados	Fraudes	Falsificação de informações ou ativos	Spoofing
	Negação de serviço	Ataques Sybil		
10	Malware	Ransomware	Phishing	Engenharia Social
	Ataques a Dispositivos IoT	Vazamento/Violação de Dados		
11	Vazamento/Violação de Dados	Comprometimento de redes	Insider Threat	Phishing
	Ransomware	Zero Day	Roubo de credenciais (Credential Theft)	Ataques de força bruta
	Man-in-the-middle	Keyloggers		
12	Insider Threat	Hardware Supply Chain Attack	Falsificação de informações ou ativos	
13	Negação de serviço	Falsificação de informações ou ativos	Fraudes	
14	Vazamento/Violação de Dados	Fraudes	Manipulação de configuração	Falsificação de informações ou ativos

Fonte – Resultado da Pesquisa

A partir dos dados organizados na Tabela 4, foram contabilizadas as ameaças cibernéticas mencionadas em cada artigo, o que possibilitou a elaboração de uma lista ordenada de forma decrescente conforme sua frequência. Adicionalmente, fundamentado da análise detalhada dos artigos, foi possível desenvolver descrições sucintas para cada ameaça, proporcionando uma compreensão clara das principais ameaças discutidas na literatura voltada à segurança da cadeia de suprimentos conforme apresentado na Tabela 5.

Além disso, para compreender melhor como as ameaças cibernéticas afetam a cadeia de suprimentos, é essencial analisar as técnicas de ataques frequentemente utilizadas por agentes maliciosos, conforme destacados pela (ENISA, 2021). Essas técnicas representam métodos específicos por meio dos quais os atacantes exploram vulnerabilidades, obtém acesso não autorizado, manipulam informações ou causam danos a sistemas e redes.

Ao relacionar as ameaças identificadas nos artigos selecionados com as técnicas de ataque descritos, torna-se mais fácil reconhecer padrões de comportamento malicioso e, consequentemente, definir controles de segurança mais precisos e eficazes.

A seguir, apresenta-se a taxonomia dos vetores de ataque, conforme o relatório "*Threat Landscape for Supply Chain Attacks*" da (ENISA, 2021), acompanhada da descrição e do objetivo de cada técnica:

- *Malware Infection*: ataque cibernético por meio de software malicioso, como *criptominers*, vírus, *ransomware, worms e spyware*. Seus principais objetivos incluem o roubo de informação ou identidade, espionagem e negação de serviço.
- *Social Engineering*: ato de enganar uma pessoa a fim de obter informações confidenciais para conseguir acesso não autorizado a sistemas. A técnica baseia-se na manipulação psicológica da vítima, com o objetivo de cometer fraudes, espionagem ou comprometer a segurança de redes e dados.
- *Brute-Force Attack*: técnica usada para acessar contas sem conhecer as senhas, tentando várias combinações de forma repetitiva.
- *Exploiting Software Vulnerability*: exploração de falhas ou erros em um software para obter vantagens indevidas. Essa técnica é usada por atacantes para invadir, comprometer ou danificar sistemas e dados.
- *Exploiting Configuration Vulnerability*: explora falhas ou erros na configuração de sistemas, redes ou aplicações, para obter acesso não autorizado, comprometer dados ou causar danos operacionais.
- *Physical Attack or Modification*: técnica de ataque em que um invasor acessa ou altera fisicamente um dispositivo para comprometer sua segurança, como ao danificar componentes, instalar dispositivos maliciosos ou extrair informações sensíveis.

- *Open-Source Intelligence* (OSINT): explora a coleta de informações públicas disponíveis (como redes sociais, sites corporativos ou banco de dados abertos) sobre os alvos, com o intuito de planejar ataques cibernéticos com maior precisão.
- *Counterfeiting*: consiste em substituir ou incluir hardware por versões falsificadas em sistemas de informação. Essa técnica permite que agentes maliciosos comprometam dispositivos com peças não confiáveis, burlando controles de qualidade e auditorias, possibilitando a corrupção de sistemas críticos.
- *Trusted Relationship*: técnica na qual o atacante aproveita da confiança estabelecida entre organizações, sistemas ou fornecedores. Através dessa confiança, o invasor se infiltra de forma disfarçada utilizando conexões ou canais legítimos, comprometendo um alvo.
- *Drive-by Compromise*: ocorre quando sites legítimos são comprometidos e utilizados para distribuir malware aos dispositivos dos visitantes, sem que eles percebam. Esse tipo de ataque geralmente explora vulnerabilidades em navegadores ou plugins desatualizados.
- *Phishing*: técnica de engenharia social que utiliza mensagens falsas para enganar pessoas e obter informações sensíveis.

Por consequência, a Tabela 5 apresenta uma coluna que associa cada ameaça a uma ou mais técnicas de ataque, com base nas finalidades das ameaças e as características específicas de cada técnica apresentada anteriormente, permitindo a compreensão e a classificação dos diferentes tipos de ataques de forma mais clara.

Tabela 5 - Levantamento das ameaças cibernéticas

Ameaças	Taxonomia de Técnicas de Ataque	Finalidade	Quantidade 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, manipulação de dados ou produtos falsificados, explorando a confiança entre empresas e seus fornecedores para violar sistemas, roubar informações e comprometer operações.	7
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
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
Insider Threat	Trusted Relationship	Alguém com acesso autorizado causa danos intencional ou acidental a recursos, pessoas ou sistemas.	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 objetivo de roubo financeiro, espionagem, sabotagem ou outros tipos de fraudes.	3

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
Ataque de 51%	Exploiting Configuration Vulnerability / Counterfeiting	Comprometer a integridade da blockchain ao obter controle da maioria do poder computacional da rede, permitindo fraudes como o gasto duplo.	2
Ataque de canal lateral	Physical Attack or Modification	Explorar os dados sobre a implementação do sistema e a sequência de dados transmitida por ele.	2
Ataque de verificador roubado	Trusted Relationship	Obter credenciais de autenticação, como senhas temporárias (OTP), a partir do servidor durante sessões de verificação passadas ou em andamento. Depois, utiliza essas informações para entrar no sistema. Caso consiga, o atacante se passa por um usuário legítimo na sessão seguinte.	2
Ataques a Dispositivos IoT	Exploiting Software Vulnerability / Exploiting Configuration Vulnerability	Explorar vulnerabilidades em dispositivos conectados à internet para obter acesso não autorizado, comprometer dados ou controlar remotamente os equipamentos, afetando a segurança e a operação da rede.	2
Ataques de eclipse	Exploiting Configuration Vulnerability	Isolar um nó (ou conjunto de nós) da rede blockchain, controlando toda a sua comunicação.	2
Ataques de força bruta	Brute-Force Attack	O invasor tenta acessar o sistema testando várias combinações de senhas até encontrar a correta, ou busca descobrir a chave de acesso por meio de tentativas sucessivas, usando métodos de derivação conhecidos.	2
Comprometimento de redes	Exploiting Configuration Vulnerability / Drive-by Compromise	Invasão e controle não autorizados de redes de comunicação, permitindo atividades maliciosas e interrupção dos serviços.	2
Erros humanos	Trusted Relationship / Social Engineering	Falhas cometidas por pessoas durante a operação, configuração ou manutenção de sistemas, que podem gerar vulnerabilidades, falhas de segurança ou interrupções nos processos.	2
Falta de Confiança entre Partes	Trusted Relationship	Interromper ou comprometer a cooperação segura, criando desconfiança para prejudicar a comunicação, o compartilhamento de dados ou a operação conjunta.	2
Falta de rastreabilidade	Counterfeiting / Trusted Relationship / Physical Attack or Modification	Dificultar ou impedir o acompanhamento, monitoramento e verificação das etapas, origens e movimentações dentro de um processo ou sistema	2
Ransomware	Malware Infection	Comprometer sistemas e dados de uma organização por meio de seus fornecedores ou parceiros, resultando em paralisações operacionais, tentativas de extorsão e perdas econômicas significativas.	2
Spoofing	Counterfeiting / Social Engineering	Enganar sistemas ou usuários ao falsificar identidades digitais para obter acesso não autorizado, interceptar informações ou executar ataques maliciosos na cadeia de suprimentos.	2
Manipulação de configuração	Exploiting Configuration Vulnerability	Modificar intencionalmente as configurações de sistemas ou dispositivos para comprometer seu funcionamento	1
Ataque de buraco de minhoca	Exploiting Configuration Vulnerability	Enganar dois nós distantes conectando-os por um túnel de comunicação externo à rede, fazendo-os acreditar que estão próximos, mesmo estando longe.	1
Ataque de buraco negro	Trusted Relationship / Exploiting Configuration Vulnerability	Bloquear o fluxo de dados em uma rede ao direcionar e eliminar os pacotes de maneira discreta, afetando a disponibilidade das informações e minando a confiança na integridade das comunicações.	1
Ataque de chave conhecido	Open-Source Intelligence (OSINT)	Utilizando as chaves previamente violadas, um atacante busca gerar novas chaves de sessão.	1
Ataque de enfraquecimento	Exploiting Configuration Vulnerability	Busca consumir toda a energia dos nós, forçando-os a realizar processos desnecessários.	1
Ataque de implantação de dispositivo desonesto	Physical Attack or Modification	Obter controle indevido sobre sistemas protegidos, elevando privilégios para executar ações restritas.	1
Ataque de interferência de RF	Physical Attack or Modification	Utilizar diversos dispositivos distribuídos de baixa potência para bloquear sinais GNSS e outras frequências de redes celulares, causando falhas no funcionamento preciso de equipamentos agrícolas inteligentes.	1
Ataques de repetição	Drive-by Compromise	Interceptação de uma cópia dos dados trocados entre duas partes e tenta enganar um usuário legítimo ao retransmitir essas informações.	1
Ataques por má configuração	Exploiting Configuration Vulnerability	Explorar erros ou falhas na configuração de sistemas para ganhar acesso ou causar danos.	1
BOTNET	Malware Infection / Drive-by Compromise	Permitir que o invasor controle diversos dispositivos comprometidos para propagar ataques em larga escala, como disseminação de malware, envio de spam ou sobrecarga de sistemas.	1
Encaminhamento seletivo	Drive-by Compromise / Exploiting Configuration Vulnerability	Interromper ou atrasar parcialmente a comunicação entre dispositivos, causando perda de dados ou falhas, sem levantar suspeitas imediatas.	1
Engenharia reversa	Open-Source Intelligence (OSINT)	Analisar detalhadamente um produto, sistema ou software para entender seu funcionamento interno.	1
Engenharia Social	Social Engineering	Manipular pessoas para obter acesso a informações confidenciais, sistemas ou recursos, explorando a confiança humana em vez de vulnerabilidades técnicas.	1
Extorsão / Chantagem (blackmailing)	Social Engineering	Ameaçar uma pessoa ou organização para obter vantagens.	1
Falha na coleta e transmissão	Exploiting Configuration Vulnerability	Comprometer a integridade ou confidencialidade dos dados durante coleta ou envio.	1
Falha no sistema ERP	Exploiting Software Vulnerability	Software de gestão integrada apresenta erros ou interrupções, impactando negativamente os processos operacionais e o fluxo de informações na empresa.	1
Hardware Supply Chain Attack	Physical Attack or Modification	Comprometer a segurança e funcionalidade dos dispositivos físicos ao inserir componentes maliciosos.	1
Keyloggers	Malware Infection	Capturar de forma sigilosa as informações digitadas por um usuário, como credenciais de acesso, dados bancários e outras informações sensíveis, com o objetivo de roubo de identidade e espionagem.	1

Manipulação automática	Drive-by Compromise / Malware Infection	Alterar ou interferir de forma automatizada em sistemas, processos ou dados, com o objetivo de comprometer sua integridade	1
Modificação de contratos	Counterfeiting	Alterar cláusulas ou termos contratuais de forma indevida para obter benefícios ilegítimos	1
Rastreamento não autorizado	Open-Source Intelligence (OSINT)	Monitorar ou seguir atividades sem permissão, violando a privacidade.	1
Resiliência contra ataques de captura de dispositivo de detecção	Physical Attack or Modification	O invasor toma controle do dispositivo de detecção e extrai as informações para se conectar a outros dispositivos da rede. A apreensão do dispositivo causa grandes prejuízos ao sistema.	1
Sniffing	Drive-by Compromise / Exploiting Configuration Vulnerability	Interceptar e capturar dados trafegando em uma rede, com o objetivo de obter informações sensíveis sem o conhecimento dos usuários.	1
Spyware	Malware Infection	Coletar informações confidenciais do usuário sem seu consentimento, monitorando suas atividades para fins maliciosos	1
SQL injection	Exploiting Software Vulnerability	Inserir comandos maliciosos em bancos de dados para acessar ou manipular informações.	1
Zero Day	Exploiting Software Vulnerability	Explorar vulnerabilidades desconhecidas ou não corrigidas em softwares ou sistemas permitindo que invasores executem ações maliciosas antes que o desenvolvedor lance uma correção ou patch de segurança.	1

Fonte – Resultado da Pesquisa

Outrossim, a partir da análise dos artigos selecionados, procedeu-se ao levantamento detalhado das soluções de segurança da informação apresentadas. Essas soluções foram catalogadas segundo cada artigo selecionado, conforme indicado na Tabela 6, permitindo identificar sua prevalência e abrangência na literatura. Essa organização facilita a compreensão das estratégias mais adotadas para a proteção da cadeia de suprimentos contra as ameaças cibernéticas.

Tabela 6 - Tabulação das soluções citadas por artigo

ARTIGO	Soluções			
1	Blockchain	Autenticação Multi-Camada	Smart Contracts	Machine Learning (IA)
2	Blockchain	Machine Learning (IA)	PUF (Physical Unclonable Function)	Smart Contracts
	RFID			
3	Blockchain	Smart Contracts	Códigos internos embutidos nas peças	Machine Learning (IA)
4	Blockchain	Zero Trust Architecture	Políticas de segurança cibernética	
5	Blockchain	Mecanismos de Tolerância a Falhas Bizantinas	Smart Contracts	Frameworks para Gestão de Riscos Cibernéticos
6	Blockchain	Smart Contracts	Cloud-based IoT platforms	RFID
7	Treinamento de conscientização de segurança	Anti-malware	Backups múltiplos	Planos de continuidade e recuperação
	IPS (Sistema de Prevenção de Intrusões)	Infraestrutura Redundante e Distribuída	Avaliação de terceiros	
8	Blockchain	Smart Contracts	Frameworks para Gestão de Riscos Cibernéticos	Infraestrutura de Confiança (TIS)
	RFID			
9	Blockchain	Smart Contracts	Frameworks para Gestão de Riscos Cibernéticos	
10	Blockchain	Firewalls	IDS (Sistema de detecção de intrusão)	Atualizações e Patches
	Machine Learning (IA)	Treinamento de conscientização de segurança	Autenticação Multi-Camada	Avaliação de terceiros
	Simulados de phishing	Anti-malware	Políticas de segurança cibernética	Frameworks para Gestão de Riscos Cibernéticos
	SIEM (Security Information and Event Management)			
11	Blockchain	SIEM (Security Information and Event Management)	SOAR (Security Orchestration, Automation and Response)	SBOM (Software Bill of Materials)
	Machine Learning (IA)	Zero Trust Architecture	Autenticação Multi-Camada	VPN (Virtual Private Network)
	SOC (Security Operations Center)	Frameworks para Gestão de Riscos Cibernéticos		
12	Frameworks para Gestão de Riscos Cibernéticos			
13	Blockchain	Mecanismos de Tolerância a Falhas Bizantinas	Smart Contracts	

Fonte – Resultado da Pesquisa

Com base nos dados compilados na Tabela 6, foram quantificadas as soluções de segurança da informação mencionadas em cada artigo, possibilitando a criação de uma lista organizada em ordens decrescentes da frequência com que essas soluções aparecem nos artigos analisados. Essa organização não apenas revela as estratégias mais adotadas para mitigar as ameaças na cadeia de suprimentos, mas também permite identificar tendências no campo da segurança da informação.

Na Tabela 7 estão listadas as famílias de controles de segurança para C-SCRM, conforme foi referenciado no documento NIST SP 800-161r1 de (BOYENS *et al.*, 2022), acompanhadas de uma breve descrição da finalidade/objetivo de cada uma. Essa apresentação facilita a compreensão do papel que cada grupo de controles desempenha na mitigação de riscos e na proteção dos ambientes organizacionais.

Tabela 7 - 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

A partir disso, as soluções de segurança da informação encontradas foram associadas a uma ou mais dessas famílias de controles, permitindo um alinhamento estruturado entre as práticas recomendadas e os controles específicos para a gestão de riscos cibernéticos na cadeia de suprimentos. As descrições da finalidade de cada solução estão apresentadas na Tabela 8, elaboradas com base na análise aprofundada dos conteúdos dos artigos selecionados.

Tabela 8 - Levantamento das soluções mais citadas pelos artigos

Soluções	Família de Controles de Segurança para C-SCRM	Finalidade	Quantidade 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, ISO)	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
Atualizações e Patches	SI, MA	Aplicar atualizações de forma rápida e consistente para proteger os sistemas contra novas ameaças e vulnerabilidades.	1
Backups múltiplos	CP, MP	Garantir a segurança e a disponibilidade dos dados, prevenindo perdas.	1
Cloud-based IoT platforms	SC, RA	Sistema descentralizado para executar transações criptográficas e detectar/prevenir ações maliciosas	1
Códigos internos embutidos nas peças	SA, PE, IA	Garantir a autenticidade sem comprometer o tamanho ou a integridade da peça.	1
Firewalls	AC, SC	Proteger contra acessos não autorizados e bloqueia ataques maliciosos, monitorando e controlando o tráfego de rede conforme políticas de segurança definidas.	1
IDS (Sistema de detecção de intrusão)	CA, SC, AU	Monitorar uma rede ou sistema em busca de atividades suspeitas ou maliciosas.	1
Infraestrutura de Confiança (TIS)	SC, RA, SR	Ajudar a estabelecer relações confiáveis, por meio de integração segura entre sistemas digitais e não digitais no processo da cadeia de suprimentos.	1
IPS (Sistema de Prevenção de Intrusões)	SC, IR	Monitorar a rede em tempo real para detectar e bloquear automaticamente ataques e atividades maliciosas.	1
Planos de continuidade e recuperação	CP, PE, PL	Assegurar que uma organização consiga manter ou retomar rapidamente suas operações essenciais após incidentes, falhas ou desastres, minimizando impactos e prejuízos.	1

PUF (Physical Unclonable Function)	IA, PE, SC, SI	Fornecer um mecanismo de autenticação único e seguro para detectar e impedir a falsificação de dispositivos físicos dentro da cadeia de suprimentos, garantindo alta segurança para as estruturas físicas onde são implementados.	1
SBOM (Software Bill of Materials)	RA, SC, SA	Permite ao desenvolvedor garantir que os componentes estejam atualizados e responder rapidamente a novas vulnerabilidades.	1
Simulados de phishing	AT, PM	Testar e reforçar a capacidade dos funcionários de identificar e responder a ameaças cibernéticas.	1
SOAR (Security Orchestration, Automation and Response)	IR, CA	Melhorar a eficiência das operações de segurança física e digital.	1
SOC (Security Operations Center)	CA, IR	Monitorar, detectar, investigar e responder a ameaças cibernéticas 24 horas por dia. São responsáveis por proteger diversos ativos, como propriedade intelectual, dados de funcionários, sistemas empresariais e a integridade da marca.	1
VPN (Virtual Private Network)	SC	Protege os dados durante a transmissão, assegurando a segurança na troca de informações entre usuários externos e sistemas internos	1
Infraestrutura Redundante e Distribuída	CP, SC, PE	Garantir maior disponibilidade, continuidade e resiliência dos sistemas contra falhas locais ou regionais.	1

Fonte – Resultado da tabulação das soluções citadas nos artigos selecionados

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 permitiu identificar quais famílias de controles são capazes de endereçar diretamente cada técnica de ataque, proporcionando uma visão clara das estratégias para fortalecer a segurança da cadeia de suprimentos. Como resultado, essas correspondências foram organizadas e apresentadas na Tabela 9, facilitando a compreensão do alinhamento entre os vetores de ataque e os grupos de controles técnicos. Além disso, considerando que as ameaças identificadas nos artigos foram associadas às técnicas de ataque e as soluções de segurança às respectivas famílias de controles do C-SCRM, a tabela também proporciona uma visão integrada entre as ameaças identificadas nos artigos e as soluções mais indicadas para sua mitigação.

Tabela 9 - Mapeamento entre técnicas de ataque e famílias de controle

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

Fonte – Resultado da tabulação da relação entre ameaças identificadas e soluções de mitigação nos artigos selecionados

Analisando a Tabela 5, que apresenta as ameaças mais citadas nos artigos analisados, observa-se que a Falsificação de informações ou ativos é o risco mais recorrente, com onze menções. Isso indica uma forte preocupação com ações maliciosas que visam enganar sistemas ou pessoas por meio de criação e alteração de informações ou ativos, podendo comprometer a confiança dos consumidores e a integridade do mercado.

Em seguida, a fraudes aparece com sete citações, reforçando a preocupação significativa no contexto analisado. Esse número indica a relevância do tema dentro do conjunto de dados, sinalizando a necessidade de maior atenção para compreender suas causas e impactos.

Empatados com seis ocorrências cada, estão as ameaças significativas: negação de serviço (DoS) e vazamento/violação de Dados. Esses números indicam um foco relevante nos estudos na interrupção da disponibilidade de sistemas e na exposição de informações sensíveis, aspectos críticos para a resiliência e a continuidade das operações em ambientes digitais complexos.

A ameaça *man-in-the-middle*, com quatro menções, também possui destaque por representar riscos à integridade e confidencialidade das comunicações, sobretudo em sistemas nos quais a troca de dados entre múltiplas partes é constante. Juntamente, com quatro menções, está o ataque Sybil que mostra a preocupação com a manipulação de redes descentralizadas.

Por fim, com três citações cada, estão a falta de transparência, *malware*, *phishing,* roubo de credenciais (*Credential Theft*), e *insiders threat*. A primeira ameaça está relacionada à manipulação ou ocultação de dados e processos, sendo uma ameaça que dificulta a rastreabilidade de ações, favorecendo fraudes e violação de políticas. A segunda ameaça, está associado ao comprometimento de sistemas, por meio da execução de softwares maliciosos que visam causar danos, roubar informações ou obter controle remoto de dispositivos. Já o *phishing* demonstra a persistente vulnerabilidade humana, podendo ser direcionado para colaboradores, fornecedores ou demais agentes envolvidos na cadeia com a finalidade de obter acesso não autorizado a sistemas ou a dados sensíveis, mostrando-se uma porta aberta para ataques cibernéticos causado pelo fator humano (ADEWUSI, CHIEKEZIE, EYO-UDO. 2022). O roubo de credenciais (*Credential Theft*) está relacionado à violação de identidade e acesso não autorizado, ocorrendo quando senhas, tokens ou outros dados de autenticação são obtidos por atacantes para invadir sistemas ou passar por usuários legítimos. Por fim, a ameaça *Insider threat* refere-se a indivíduos com acesso autorizado que, de forma intencional ou acidental, causam danos a organização. Os *insiders* podem explorar o nível de privilégio que possuem para acessar dados sensíveis, prejudicar operações ou facilitar ataques externos, sendo uma ameaça difícil de detectar e mitigar devida à sua natureza privilegiada.

Em síntese, os dados reforçam que os estudos temem ameaças que afetam a confiança, a disponibilidade e a segurança da informação e produtos nas cadeias de

suprimentos. A frequência dessas citações evidencia a necessidade estratégicas de mitigação robustas, capazes de proteger não apenas os sistemas tecnológicos, mas também os processos e as relações comerciais que sustentam essas cadeias.

Em seguida, a análise da Tabela 8, permite uma visualização das abordagens consideradas eficazes pelos autores na proteção das cadeias de suprimentos. Entre as soluções mais referenciadas, destaca-se a tecnologia blockchain, com onze menções, que, conforme já abordado anteriormente, oferece transparência, rastreabilidade e integridade dos dados em ambientes distribuídos. Tais características tornam essa solução particularmente eficaz no combate à falsificação, fraudes e alteração de registros, que estão entre as ameaças mais preocupantes identificadas na literatura.

Os *smart contracts*, com oito citações, também mencionados na fundamentação teórica, atuam como um complemento direto ao blockchain, possibilitando a automação segura de processos com base em regras previamente definidas. Dessa forma, reduzem a intervenção humana e, por consequência, minimizam o risco de manipulações maliciosas atuante de forma eficaz na mitigação de fraudes, falsificação de transações, modificação de contratos e falta de transparência.

Além disso, os frameworks de segurança cibernética (seis citações), como os propostos pelo NIST, fornecem diretrizes estruturadas para o fortalecimento da segurança organizacional, sendo instrumentos na prevenção de ataques.

O uso de *machine learning* (IA), que apresentou cinco menções, tem se consolidado como ferramenta estratégica para a detecção de padrões anômalos e respostas proativas a ameaças emergentes. Essas soluções são especialmente úteis na identificação de comportamento maliciosos, como em ataques Sybil, fraudes e acessos não autorizados.

A partir da análise das finalidades e características de cada ameaça identificada na Tabela 5 e das famílias de controles apresentadas na Tabela 8, foi possível estabelecer uma correlação significativa entre as técnicas de ataques levantados e as famílias de controles para segurança da informação na cadeia de suprimentos, conforme pode ser observado na Tabela 9. Essa relação permitiu compreender quais famílias de controle são mais adequadas para enfrentar as técnicas de ataque específicas, evidenciando a eficácia e o alinhamento das tecnologias e métodos recomendados pela literatura para garantir a segurança e a integridade das cadeias de suprimentos. Dessa forma, a correlação entre as técnicas de ataque e das famílias de controles oferece uma visão integrada facilitando a identificação das práticas que podem ser utilizadas para proteção do ambiente analisado.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve como tema central a análise das ameaças cibernéticas que afetam as cadeias de suprimentos, bem como a identificação das soluções mais citadas para mitigá-las.

Para realizar a revisão sistemática da literatura, foi utilizada como referência uma seção de um artigo do NIST, que aborda as ameaças cibernéticas na cadeia de suprimentos. Em seguida, foi conduzida uma análise bibliométrica com o apoio das bases de dados Google Scholar e OpenAlex, por meio da busca de palavras-chave, com recorte temporal entre os anos de 2020 e 2025. A partir dos artigos encontrados, foi realizada uma análise qualitativa com o objetivo de selecionar apenas os artigos que apresentassem relação direta com foco da pesquisa, ou seja, aqueles que tratam de ameaças de cibersegurança na cadeia de suprimentos e as soluções utilizadas para sua mitigação.

Na análise de resultados observou-se que os estudos selecionados apresentam uma maior preocupação com ameaças, como falsificação de informações ou ativos, fraudes, vazamento/violação de dados, negação de serviço, ataques Sybil e man-in-the-middle, sendo essas as mais recorrentes na literatura analisada. Em contrapartida, as soluções mais citadas foram: *blockchain*, *smart contracts*, *frameworks* de segurança cibernética e *machine learning*. Com base nessas informações, foi possível correlacionar as técnicas de ataque associadas às ameaças e as famílias de controles de segurança da informação vinculadas às soluções, evidenciando as estratégias defensivas mais adequadas para mitigar cada técnica.

Como resultados, foi possível responder à questão-problema proposta. Os objetivos gerais e específicos também foram atingidos com êxito, por meio da análise das principais ameaças cibernéticas que afetam a cadeia de suprimentos, da identificação das soluções de mitigação mais utilizadas e da avaliação de artigos científicos publicados entre 2020 e 2025, com ênfase nos estudos mais citados apresentando maior credibilidade e relevância científica.

Esta pesquisa apresenta algumas 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, destaca-se a possibilidade de avaliar a eficácia das soluções de mitigação, por meio de estudos de caso ou simulações, a fim de verificar

o quanto soluções são, realmente, eficazes em mitigar ameaças específicas, uma vez que muitos artigos apontam soluções de forma teórica, mas faltam análises práticas comparativas. Seguindo esta mesma linha, pode-se estudar como as empresas estão implementando as soluções em seus ambientes de cadeia de suprimentos e quais são as ameaças que mais as afetam para compreender os desafios práticos, as limitações enfrentadas e lições aprendidas na adoção dessas estratégias de mitigação.

REFERÊNCIAS

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.

AL-FARSI, S.; RATHORE, M.; BAKIRAS, S. Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities. **Applied Sciences**, v. 11, n. 12, p. 5585, 2021. DOI: 10.3390/app11125585. Disponível em: https://doi.org/10.3390/app11125585. Acesso em 19 jun. 2025.

ASANTE, M. *et al*. Distributed ledger technologies in supply chain security management: A comprehensive survey. **IEEE Transactions on Engineering Management**, v. 70, n. 2, p. 713–739, 2021. DOI: 10.1109/TEM.2021.3053655. Acesso em 19 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.

COLLIER, Z. A.; SARKIS, J. The zero trust supply chain: Managing supply chain risk in the absence of trust. **International Journal of Production Research**, v. 59, n. 22, p. 6819–6832, 2021. Taylor & Francis. DOI: 10.1080/00207543.2021.1884311. Acesso em 20 jun. 2025.

CREAZZA, A.; COLICCHIA, C.; SPIEZIA, S. Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. **Supply Chain Management: An International Journal**, v. 27, n. 1, p. 30-53, 2022. DOI: 10.1108/SCM-02-2020-0073. 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.

GUGGENBERGER, T.; SCHWEIZER, A.; URBACH, N. Improving Inter-Organizational Information Sharing for Vendor Managed Inventory: Towards a Decentralized Information Hub Using Blockchain Technology. **IEEE Transactions on Engineering Management**, v. 67, n. 4, p. 1074-1085, nov. 2020. Disponível em: https://doi.org/10.1109/TEM.2020.2978628. 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.

IFTIKHAR, A. *et al.* Digital Innovation, Data Analytics, and Supply Chain Resiliency: A Bibliometric-based Systematic Literature Review. **Annals of Operations Research**, 2022. DOI: 10.1007/s10479-022-04765-6. Disponível em: https://doi.org/10.1007/s10479-022-04765-6. Acesso em: 18 jun. 2025.

KAMBLE, S. *et al*. Blockchain technology's impact on supply chain integration and sustainable supply chain performance: evidence from the automotive industry. ***Annals of Operations Research****,* v. 327, p. 575–600, 2023. DOI: 10.1007/s10479-021-04129-6. Disponível em: https://doi.org/10.1007/s10479-021-04129-6. 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.

MARTÍNEZ, J.; DURÁN, J. M. Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. **International Journal of Safety and Security Engineering**, v. 11, n. 5, p. 537-545, out. 2021. DOI: 10.18280/ijsse.110505. Acesso em 20 jun. 2025.

MOOSAVI, J. *et al*. Blockchain in supply chain management: a review, bibliometric, and network analysis. **Environmental Science and Pollution Research**, 2021. DOI: 10.1007/s11356-021-13094-3. Acesso em 18 jun. 2025.

NGUYEN, T.V. *et al*. Data-driven review of blockchain applications in supply chain management: key research themes and future directions. **Journal of Production Research**, 2023. DOI: 10.1080/00207543.2023.2165190. Acesso em 19 jun. 2025.

RAD, F. F. *et al*. Industry 4.0 and supply chain performance: A systematic literature review of the benefits, challenges, and critical success factors of 11 core technologies. **Industrial Marketing Management**, v. 105, p. 268-293, ago. 2022. DOI: 10.1016/j.indmarman.2022.06.009. Acesso em 19 jun. 2025.

ZHENG, K. *et al*. Blockchain technology for enterprise credit information sharing in supply chain finance. **Journal of Innovation & Knowledge**, v. 7, n. 4, p. 100256, out. – dez. 2022. DOI: 10.1016/j.jik.2022.100256. Acesso 19 jun. 2025.