Challenges and Solutions of Risk Management in Software Ecosystems

Gabriele da Silva Serafim de Campos[1], **Francisco Ismael Ribeiro da Silva**[1], **Paulo Malcher**[1], **Rodrigo Pereira dos Santos**[2]

[1] Universidade Federal Rural da Amazônia (UFRA)
Capitão Poço – PA – Brasil

[2]Universidade Federal do Estado do Rio de Janeiro (UNIRIO)
Rio de Janeiro – RJ – Brasil

gabbcampos64@gmail.com, frismaellsilva180@gmail.com,
paulo.malcher@ufra.edu.br, rps@uniriotec.br

Abstract. Research Context: *Software ecosystems (SECO) differ from other software development contexts and increase the complexity of risk management.* ***Scientific and/or Practical Problem:*** *It remains unclear the way risk management is conducted in SECO, which risks are specific to this context, and which solutions have been proposed.* ***Proposed Analysis:*** *This study investigates risk management in SECO by identifying SECO-specific risks, mapping solutions and their evaluations, and highlighting existing challenges.* ***Related IS Theory.*** *Socio-technical Theory provides a perspective by emphasizing the interdependence of technical and social factors in risk management in SECO.* ***Research Method:*** *We conducted a systematic mapping study following established guidelines, including study selection, data extraction, and qualitative coding.* ***Summary of Results:*** *We identified 24 SECO-specific risks, 21 solutions, of which 15 were evaluated, and 14 challenges related to risk management in SECO.* ***Contributions and Impact to IS area:*** *This study consolidates knowledge on risk management in SECO and provides insights to support researchers and practitioners in designing more effective mitigation strategies.*

1. Introdução

A complexidade crescente dos sistemas de software e a necessidade de colaboração entre múltiplas organizações impulsionaram o surgimento dos ecossistemas de software (ECOS) [Manikas 2016, Jansen 2020]. Esses ecossistemas consolidaram-se como um contexto predominante no desenvolvimento de software moderno [Damian et al. 2021] e podem ser definidos como a interação entre software e múltiplos atores em torno de uma plataforma tecnológica comum, resultando em um conjunto de contribuições que influenciam direta ou indiretamente o ecossistema [Manikas 2016]. Embora promovam benefícios como inovação e adaptabilidade, os ECOS introduzem desafios relevantes à sua sustentabilidade. Entre esses desafios, destaca-se a gerência de riscos, que é crítica diante da natureza distribuída, interdependente e, por vezes, informal das interações em ECOS [Manalif et al. 2013, Olsson e Franke 2019].

Riscos são uma parte inerente ao desenvolvimento de software e podem afetar diretamente o desempenho do projeto. Eles podem ser entendidos como eventos incertos que podem gerar efeitos negativos ou positivos em um ou mais objetivos do projeto

[Menezes Jr et al. 2019, Bilousiva et al. 2023]. Nesse contexto, a gerência de riscos visa identificar, analisar e tratar riscos de forma sistemática, complementando outros processos de gerenciamento de projetos, como os de qualidade e de requisitos [PMI 2021]. Quando os riscos não são gerenciados, eles têm o potencial de desviar o projeto do planejamento e comprometer seus resultados. Consequentemente, o sucesso do projeto está diretamente relacionado à eficácia do processo de gerência de riscos [Menezes Jr et al. 2019].

A gerência de riscos em ECOS difere de outros contextos de desenvolvimento de software [Manalif et al. 2013, Mandych et al. 2023]. Em contextos mais tradicionais, o escopo dos projetos tende a ser mais delimitado e o número de partes interessadas é reduzido. Em contraste, os ECOS exigem abordagens que considerem múltiplos interesses, tomada de decisão descentralizada, diversidade de artefatos e evolução contínua das plataformas [Mandych et al. 2023]. A estrutura aberta e dinâmica dos ECOS aumenta a complexidade da gerência de riscos, sendo necessário adotar estratégias específicas para identificar, analisar, mitigar e monitorar riscos nesse contexto [Hou e Jansen 2024].

Apesar do avanço das pesquisas em ECOS, até onde se sabe, não há um estudo secundário voltado à gerência de riscos nesse contexto. No entanto, diversos trabalhos reconhecem que tais riscos diferem daqueles comumente analisados em outros contextos de desenvolvimento de software [Manalif et al. 2013, Mandych et al. 2023, Schueller e Wachs 2024]. Diante desse cenário, este estudo tem como objetivo investigar a gerência de riscos em ECOS, buscando identificar os principais riscos presentes nesse contexto, mapear as soluções propostas para gerenciá-los, analisar em que medida essas soluções têm sido avaliadas e apontar os desafios existentes. Para isso, foi conduzido um mapeamento sistemático da literatura (MSL), que é uma abordagem estruturada para identificar, categorizar e analisar evidências científicas [Petersen et al. 2015].

Como resultados, foram identificados 24 riscos específicos para ECOS e 21 soluções para gerenciá-los, categorizadas em *frameworks*, modelos, práticas, ferramentas e métodos. Dentre essas soluções, 15 foram avaliadas em diferentes contextos, enquanto 6 não apresentaram avaliação formal. Além disso, foram identificados 14 desafios relacionados à gerência de riscos em ECOS. Este estudo utiliza como referência conceitual a Teoria Sociotécnica [Trist 1981], que reconhece a interdependência entre componentes técnicos e sociais em sistemas e defende que mudanças em um desses elementos afetam todo o sistema. Essa perspectiva ajuda a explicar como riscos em ECOS emergem da interação entre tecnologia, processos e pessoas, oferecendo subsídios para estratégias de mitigação mais eficazes. De forma complementar, os achados dialogam com o desafio de "*Visão Sociotécnica dos Sistemas de Informação*", identificado pelo I Grandes Desafios em Sistemas de Informação no Brasil 2016–2026 (GranDSI-BR) [Boscarioli et al. 2017], ao evidenciar que a gerência de riscos em ECOS demanda a integração de aspectos técnicos e sociais inerentes ao ecossistema.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta a fundamentação teórica e os trabalhos relacionados; a Seção 3 descreve o método de pesquisa; a Seção 4 apresenta os resultados; a Seção 5 discute as contribuições do estudo; a Seção 6 apresenta as ameaças à validade; e, por fim, a Seção 7 conclui o artigo com considerações finais e trabalhos futuros.

2. Fundamentação teórica e trabalhos relacionados

2.1. Ecossistemas de software

Desde o livro seminal de [Messerschmitt e Szyperski 2003], ECOS se tornou um tópico ativo de pesquisa inspirado por conceitos de ecossistemas de negócios e naturais [Mens e Roover 2023]. ECOS podem ser definidos e interpretados de diferentes perspectivas e, de acordo com [Mens e Roover 2023], [Manikas 2016] combinou todas as perspectivas usadas em outras definições de ECOS em uma única definição abrangente, apresentada na Seção 1. Para [Manikas 2016], ECOS se caracterizam por redes dinâmicas e complexas de atores (e.g., desenvolvedores, empresas, comunidades e usuários), que interagem de forma colaborativa em torno de uma plataforma tecnológica comum, promovendo flexibilidade, auto-organização e criação conjunta de valor.

[Manikas 2016] classificou ECOS em três tipos: (i) de código proprietário, em que acordos de confidencialidade protegem o código-fonte e outros artefatos produzidos, pois são os produtos que geram receita para o ecossistema, tais como ecossistemas de comércio eletrônico; (ii) de código aberto, em que os atores não participam da obtenção de renda direta de sua atividade no ecossistema, como a Eclipse Foundation e a Apache Foundation; e (iii) híbrido, que combina contribuições de código proprietário e de código aberto. Por exemplo, o iOS adota estratégias de código proprietário, como a loja de aplicativos e o repositório de código-fonte, para sustentar políticas da plataforma, ao mesmo tempo em que utiliza estratégias de código aberto para engajamento da comunidade, como ferramentas, submissões e contribuições de publicação.

2.2. Gerência de riscos

Riscos são normalmente definidos como incertezas ou ameaças que têm um impacto significativo no desempenho de um projeto [Prakash e Viswanathan 2020]. Segundo [Chen e Deng 2022], um risco é um evento ou condição incerta que pode ou não ocorrer e que, caso ocorra, pode gerar impacto positivo ou negativo em um ou mais objetivos do projeto. À medida que os sistemas de software se tornam cada vez mais complexos e integrais às operações comerciais, o potencial para riscos que podem interromper os processos de desenvolvimento, comprometer a segurança ou levar a falhas no projeto tem aumentado [Siddiqui 2024].

A gerência de riscos em projetos de software descreve uma abordagem de engenharia integrada com métodos, processos e artefatos que identificam, analisam, controlam e agregam riscos continuamente, a fim de reduzir o risco de falha do projeto [Pilliang e Munawar 2022]. A gerência de riscos eficaz envolve a identificação, avaliação e priorização de riscos potenciais, seguida da implementação de estratégias para mitigar ou gerenciar seu impacto [Siddiqui 2024]. De acordo com [Siddiqui 2024], ao abordar proativamente esses riscos, as organizações podem evitar atrasos dispendiosos, garantir melhor alocação de recursos e manter a estabilidade do projeto.

2.3. Gerência de riscos em ecossistemas de software

Em ECOS, riscos podem ser definidos como eventos ou condições incertas que, caso ocorram, podem impactar negativamente a saúde, a sustentabilidade e os objetivos estratégicos do ecossistema [Oliveira e Alves 2021, Keshani et al. 2024]. Esses riscos são frequentemente classificados em três dimensões principais: técnica, social e de negócios

[Oliveira e Alves 2021]. Riscos técnicos incluem vulnerabilidades de segurança, falhas de compatibilidade e problemas decorrentes do acúmulo descontrolado de dependências ou de práticas inadequadas de empacotamento de bibliotecas [Oliveira e Alves 2021, Keshani et al. 2024]. Riscos sociais abrangem a rotatividade de colaboradores, conflitos entre atores e declínio da participação comunitária [Oliveira e Alves 2021]. Riscos de negócios podem envolver questões de propriedade intelectual, licenciamento e conformidade regulatória [Oliveira e Alves 2021]. Além disso, estudos recentes destacam que esses riscos são interconectados e podem se reforçar mutuamente, formando cadeias de impacto que afetam todo o ecossistema [Mandych et al. 2023, Schueller e Wachs 2024].

A gerência de riscos em ECOS é um dos fatores que promovem a saúde e a resiliência do ecossistema [Oliveira e Alves 2021]. Portanto, ela deve ser adaptada às características do ecossistema, considerando seu modelo de governança, abertura e complexidade sociotécnica [Oliveira e Alves 2021, Schueller e Wachs 2024]. A literatura também enfatiza a importância de abordagens integradas de gerência de riscos que considerem simultaneamente fatores técnicos e sociais, dada a natureza interdependente desses elementos em ECOS [Schueller e Wachs 2024]. Essa perspectiva dialoga com a Teoria Sociotécnica [Trist 1981], que destaca a necessidade de equilibrar e coordenar os subsistemas técnicos e sociais para manter a estabilidade e o desempenho do sistema.

2.4. Trabalhos relacionados

[Valério et al. 2020] conduziram uma revisão sistemática da literatura (RSL) sobre gerência de riscos em projetos de desenvolvimento de software, visando identificar lacunas, perspectivas e tendências da área. Os resultados apontaram a necessidade de maior envolvimento da equipe, atenção às falhas e alinhamento entre a estratégia de negócios e os modelos de gerência de riscos. Em um recorte focado em ferramentas de apoio, [Luthfiansyah et al. 2024] realizaram uma RSL que identificou e analisou técnicas e ferramentas aplicadas à gerência de riscos em projetos de software. Entre os resultados, destacam-se o uso de *brainstorming*, análise de causa raiz, inteligência artificial e planos de resposta a riscos. Em uma análise para um contexto específico, [Lopes et al. 2020] conduziram um MSL sobre a gerência de riscos em sistemas de sistemas, ressaltando a ausência de abordagens consolidadas para lidar com riscos emergentes da interação entre múltiplas partes interessadas e componentes heterogêneos.

Diferentemente dos estudos anteriores, que focaram em outros contextos de desenvolvimento de software e sistemas, este trabalho se concentra em investigar a gerência de riscos no contexto de ECOS. Nesse sentido, busca-se identificar riscos específicos de ECOS, mapear soluções para gerenciá-los, analisar em que medida essas soluções têm sido avaliadas e apontar os desafios que ainda persistem na gerência de riscos em ECOS.

3. Método de pesquisa

Para este estudo, foi conduzido um MSL entre janeiro e julho de 2025 com o objetivo de analisar o estado da arte sobre a gerência de riscos em ECOS. Um MSL se caracteriza como um estudo que fornece uma visão estruturada e transparente da literatura publicada sobre determinado tema, permitindo identificar padrões, lacunas e tendências de pesquisa [Petersen et al. 2015]. Portanto, este estudo busca responder à seguinte questão de pesquisa (QP) principal: *Como a gerência de riscos tem sido realizada em ECOS?*

A ausência de estudos secundários sobre o tema, somada ao crescimento do volume de publicações, aumenta a necessidade de sistematizar as evidências disponíveis e oferecer uma visão abrangente da área. Além disso, um MSL pode mapear os diferentes resultados dos estudos, terminologias heterogêneas e contextos específicos. Para guiar este estudo, foram seguidas as diretrizes de [Kitchenham e Charters 2007] e [Petersen et al. 2015], que organizam o processo em três fases principais: planejamento, condução e apresentação dos resultados. As etapas da fase de planejamento deste MSL são descritas a seguir.

3.1. Questões de pesquisa

Para atingir os objetivos deste estudo, foram formuladas quatro QP que nortearam a seleção de estudos e a extração e análise dos dados. A Tabela 1 apresenta estas QP.

Tabela 1. Questões de pesquisa

ID	Questão de Pesquisa	Meta
QP1	Quais são os riscos específicos para ECOS?	Essa QP busca identificar os riscos específicos para o contexto de ECOS.
QP2	Quais são as soluções utilizadas na gerência de riscos em ECOS?	Essa QP busca mapear e classificar as soluções propostas (i.e., teorias, modelos, métodos ou técnicas, práticas, ferramentas e *frameworks*) para apoiar a gerência de riscos em ECOS.
QP3	Como essas soluções têm sido avaliadas?	Essa QP visa identificar se e como as soluções identificadas são avaliadas.
QP4	Quais os desafios na gerência de riscos em ECOS?	Essa QP busca evidenciar as limitações e lacunas existentes na gerência de riscos em ECOS.

3.2. Estratégia de busca

Para identificar os estudos primários que abordam as QP, foram utilizadas seis bibliotecas digitais (Tabela 2). As buscas automatizadas foram conduzidas a partir de uma *string* construída com base nos principais termos utilizados na QP principal do estudo. Seguindo as diretrizes de [Kitchenham e Charters 2007], a formulação dessa *string* teve como objetivo recuperar estudos relevantes em diferentes bases de dados. Para isso, foram selecionadas palavras-chave derivadas das QP, delimitando as buscas a trabalhos que investigam ou mencionam a gerência de riscos em ECOS. A *string* de busca utilizada foi: (*"risk"* OR *"risks"*) AND (*"software ecosystem"* OR *"software ecosystems"*).

Tabela 2. Lista das bibliotecas digitais

Biblioteca	Link
Engineering Village	https://www.engineeringvillage.com/
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/
ScienceDirect	https://www.sciencedirect.com/
Scopus	https://www.scopus.com/
Web of Science	https://webofknowledge.com/
Wiley Online Library	https://onlinelibrary.wiley.com/

3.3. Critérios de seleção dos estudos

Para a seleção dos estudos, foram definidos e aplicados critérios de inclusão (CI) e exclusão (CE), apresentados na Tabela 3. Os estudos foram incluídos se atendiam o CI e foram excluídos caso se enquadrassem em pelo menos um dos CE.

Tabela 3. Critérios de seleção

Categoria	ID	Descrição
Critério de Inclusão	CI1	Estudo responde a pelo menos uma QP.
Critérios de Exclusão	CE1	Estudo secundário (e.g., MSL e RSL).
	CE2	Estudo duplicado.
	CE3	Estudo não disponível para download gratuito ou por meio de acesso institucional.
	CE4	Estudo não escrito em inglês.
	CE5	Estudo que seja prefácio, livro, capítulo de livro, resumo, pôster, painel, palestra, *keynote*, tutorial, editorial ou demonstração.
	CE6	Estudo que não atende ao CI.

3.4. Processo de seleção dos estudos

O processo de seleção foi dividido em seis etapas, conforme descrito na Tabela 4. Inicialmente, a *string* de busca foi aplicada nas bases selecionadas para obtenção do conjunto inicial de estudos. Em seguida, o processo foi conduzido por meio de quatro filtros sequenciais, aplicados individualmente por dois pesquisadores (P1 e P2). Ao término de cada filtro, os pesquisadores realizavam reuniões para estabelecer consenso quanto às decisões de CI ou CE. Nos casos em que persistiam divergências, outros dois pesquisadores (P3 e P4), ambos com maior experiência, eram acionados para revisar as discordâncias e assegurar a consistência dos estudos selecionados e da extração de dados.

Tabela 4. Processo de seleção dos estudos

Etapa	Descrição
Etapa 1	Aplicação da *string* de busca nas bibliotecas digitais para obter o conjunto de estudos recuperados.
Etapa 2	Aplicação do 1º filtro (remoção de duplicatas).
Etapa 3	Aplicação do 2º filtro (aplicação dos CI e CE após a leitura do título, resumo e palavras-chave).
Etapa 4	Aplicação do 3º filtro (aplicação dos CI e CE após a leitura da introdução e conclusão).
Etapa 5	Aplicação do 4º filtro (aplicação do CI e CE após a leitura completa).
Etapa 6	Extração e síntese dos dados dos estudos selecionados da Etapa 5.

3.5. Extração de dados e síntese

A extração dos dados também foi conduzida por dois pesquisadores (P1 e P2), com posterior verificação dos resultados realizada por outros dois pesquisadores (P3 e P4) com maior experiência. O processo foi realizado de maneira sistemática, utilizando-se a ferramenta Microsoft Excel para registrar e organizar as informações necessárias. Foi utilizado um formulário estruturado contendo os seguintes campos: (1) identificador do estudo (ID); (2) título; (3) autores; (4) ano de publicação; (5) país de afiliação do primeiro autor; e (6) as QP abordadas.

Para responder às QP, adotou-se uma abordagem qualitativa, de caráter descritivo. A síntese dos dados seguiu as diretrizes de [Kitchenham e Charters 2007] e [Petersen et al. 2015], enquanto a análise foi orientada pelo processo de codificação qualitativa proposto por [Charmaz 2006]. Esse processo envolve atribuir códigos próximos aos dados, de modo a captar ações e significados, evoluindo gradualmente da codificação inicial para a focalizada e depois para a axial, em que os códigos são organizados em categorias mais amplas [Charmaz 2006].

No presente estudo, a aplicação do processo de codificação começou com a **codificação inicial**, que consistiu na leitura integral dos estudos e na segmentação do material em unidades coerentes (frases ou parágrafos), às quais foram atribuídos códigos próximos aos dados. Em seguida, realizou-se a **codificação focalizada**, na qual os códigos

mais significativos e recorrentes foram revistos iterativamente, com renomeações quando necessário. Por fim, aplicou-se a **codificação axial**, utilizada para organizar e agrupar os códigos em categorias. A Tabela 5 apresenta exemplos de codificações e o processo de codificação completo está disponível no material suplementar [Campos et al. 2025].

Tabela 5. Ilustração do processo de codificação

Exemplo 1 - Unidade: *"In recent years, the software supply chain has become a critical vector for cybersecurity threats, particularly within web-based software ecosystems."* (E02)			
Código	**Código focado**	**Categoria**	**Subcategoria**
Aumento da complexidade e interconexão dos ECOS eleva o risco de ataques à cadeia de suprimentos.	Comprometimento da cadeia de suprimentos de software	Risco	Técnico
Exemplo 2 - Unidade: *"We present a methodological framework to measure risk in software ecosystems as a function of both dependencies and developers."* (E08)			
Código	**Código focado**	**Categoria**	**Subcategoria**
Framework metodológico para modelagem de riscos sistêmicos em ECOS (riscos sociotécnicos).	*Framework* para modelagem de riscos sociotécnicos em ECOS.	Solução	*Framework*
Exemplo 3 - Unidade: *"The risk to using third-party libraries in a software application is that much needed maintenance is solely carried out by library maintainers."* (E12)			
Código	**Código focado**	**Categoria**	**Subcategoria**
Coordenar múltiplos atores no processo de correção e evolução, pois envolve tanto a dependência de poucos mantenedores quanto a necessidade de integrar contribuições externas.	Coordenar múltiplos atores no processo de correção e evolução, incluindo desafios organizacionais e culturais em larga escala.	Desafio	–

4. Resultados

O MSL foi conduzido com o objetivo de identificar o maior número possível de estudos relevantes relacionados à gerência de riscos em ECOS. Para garantir uma cobertura ampla e representativa da literatura científica sobre o tema, não foram aplicadas restrições quanto ao ano de publicação, permitindo a inclusão de todos os trabalhos disponíveis até fevereiro de 2025. A Figura 1 mostra o processo de seleção do MSL.

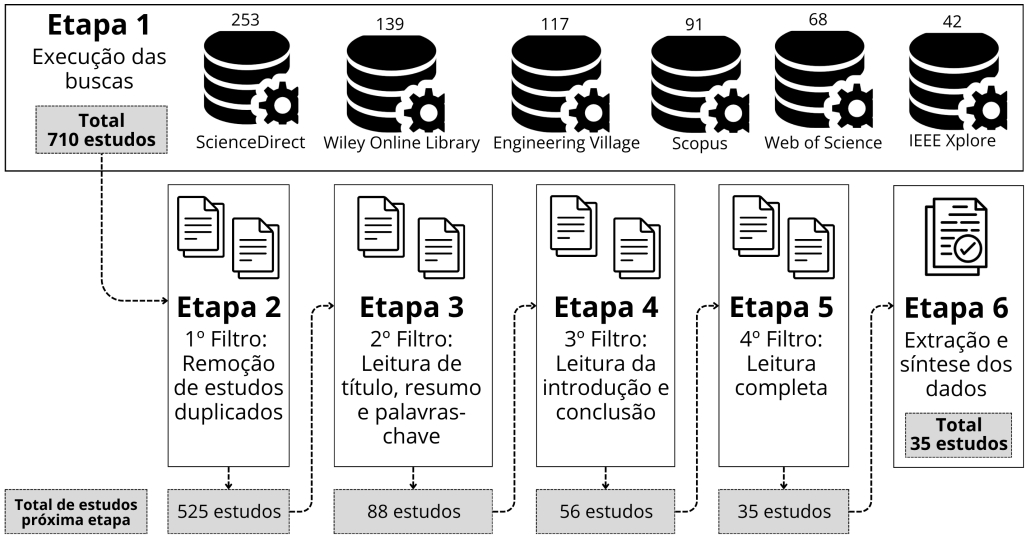

Figura 1. Resultado do processo de seleção de estudos

Ao final do processo de seleção, foram selecionados 35 estudos para extração e síntese dos dados. A Tabela 6 apresenta esses estudos em ordem decrescente por ano de publicação, acompanhados de identificadores numéricos (E1–E35) utilizados para referenciar os estudos nas próximas seções. Devido à limitação de espaço, a listagem dos

estudos selecionados com suas referências e todas as etapas necessárias à reprodução da pesquisa estão disponíveis no material suplementar [Campos et al. 2025].

Tabela 6. Lista de estudos selecionados

ID	Título	Ano
E01	Strategic Patterns to Foster the Evolution of Emerging Software Ecosystems	2025
E02	A Graph-Based Approach for Software Functionality Classification on the Web	2025
E03	Understanding Abandonment and Slowdown Dynamics in the Maven Ecosystem	2025
E04	Impact of Minimum Viable Product on Software Ecosystem Failure	2025
E05	OSS Malicious Package Analysis in the Wild	2025
E06	A Framework for Software Vendor Selection by Applying Inconsistency and Conflict Removal (ICR) Method	2024
E07	A Cast of Thousands: How the IDEAS Productivity Project Has Advanced Software Productivity and Sustainability	2024
E08	Modeling Interconnected Social and Technical Risks in Open Source Software Ecosystems	2024
E09	Maven Unzipped: Exploring the Impact of Library Packaging on the Ecosystem	2024
E10	Lessons from the Long Tail: Analysing Unsafe Dependency Updates across Software Ecosystems	2023
E11	On the Discoverability of NPM Vulnerabilities in Node.js Projects	2023
E12	Understanding the Role of External Pull Requests in the NPM Ecosystem	2023
E13	Vulnerability Management in Linux Distributions: An Empirical Study on Debian and Fedora	2023
E14	Maintenance Cost of Software Ecosystem Updates	2023
E15	An Empirical Study of Artifacts and Security Risks in the Pre-trained Model Supply Chain	2022
E16	smartPip: A Smart Approach to Resolving Python Dependency Conflict Issues	2022
E17	Goals within Trust-based Digital Ecosystems	2021
E18	Software Ecosystems Governance - An Analysis of SAP and GNOME Platforms	2021
E19	TrustSECO: A Distributed Infrastructure for Providing Trust in the Software Ecosystem	2021
E20	Technical Leverage in a Software Ecosystem: Development Opportunities and Security Risks	2021
E21	Do Scaling Agile Frameworks Address Global Software Development Risks? An Empirical Study	2021
E22	Software Reuse Cuts Both Ways: An Empirical Analysis of Its Relationship with Security Vulnerabilities	2021
E23	Open Source Software Supply Chain for Reliability Assurance of Operating Systems	2020
E24	An Empirical Comparison of Dependency Network Evolution in Seven Software Packaging Ecosystems	2019
E25	Risks and Assets: A Qualitative Study of a Software Ecosystem in the Mining Industry	2019
E26	Which Factors Affect the Evangelist's Support During Training Sessions in Mobile Software Ecosystems?	2018
E27	An Exploratory Study on Library Aging by Monitoring Client Usage in a Software Ecosystem	2017
E28	Towards a Multi-criteria Decision Support Method for Consumer Electronics Software Ecosystems	2016
E29	The Influence of Developer Multi-homing on Competition between Software Ecosystems	2016
E30	Intelligently Transparent Software Ecosystems	2016
E31	Tracing Known Security Vulnerabilities in Software Repositories – A Semantic Web Enabled Modeling Approach	2016
E32	On Using Markov Decision Processes to Model Integration Solutions for Disparate Resources in Software Ecosystems	2015
E33	Variability Mechanisms in Software Ecosystems	2014
E34	Software Ecosystems Risks	2013
E35	Analyses of Two End-user Software Vulnerability Exposure Metrics	2013

A Figura 2 ilustra a distribuição dos estudos selecionados ao longo dos anos. Entre 2013 e 2019 foram publicados 12 estudos, enquanto 23 estudo foram publicados entre 2020 e o início de 2025, indicando um aumento recente no interesse pelo tema. A Figura 3 apresenta a distribuição dos países dos estudos selecionados, considerando apenas o país do primeiro autor. Estados Unidos e Canadá destacam-se com o maior número de publicações (5 estudos cada).

4.1. QP1: Quais são os riscos específicos para ECOS?

Esta QP buscou identificar os riscos específicos para ECOS presentes nos estudos selecionados. De acordo com [Oliveira e Alves 2021], os riscos em ECOS podem ser classificados em três dimensões principais: (i) riscos técnicos, (ii) riscos sociais e (iii) riscos de negócios. Essa classificação foi adotada neste estudo para organizar os riscos identificados. Para garantir maior representatividade e clareza na apresentação, riscos com significados semelhantes foram agrupados em um único código. O risco com maior evidência entre os estudos selecionados foi *comprometimento da cadeia de suprimentos de software*,

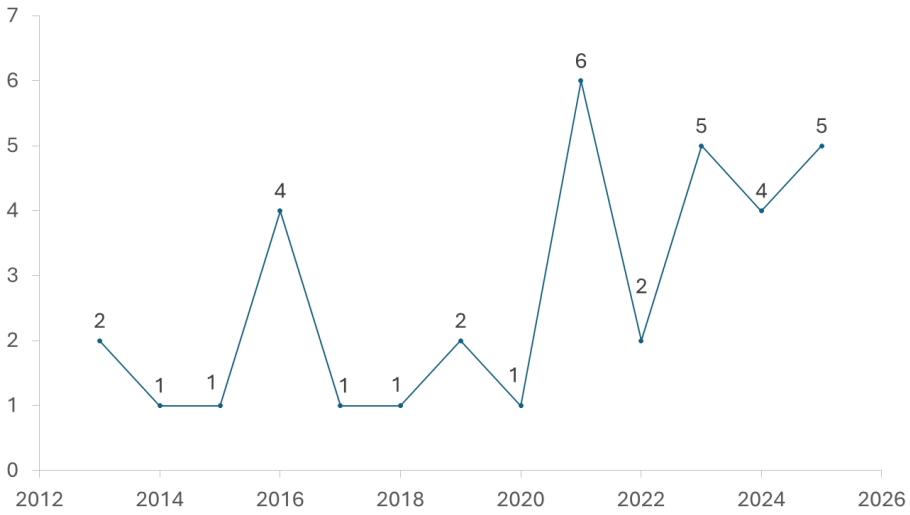

Figura 2. Número de estudos por ano

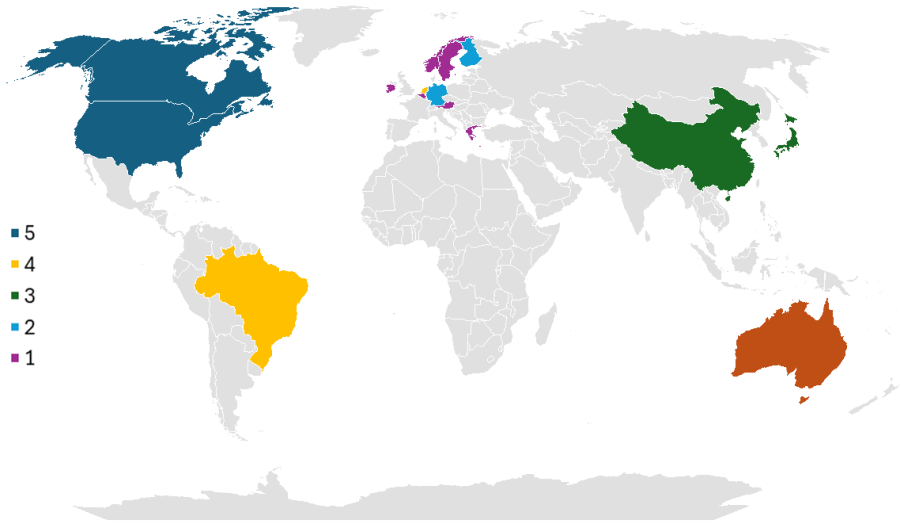

Figura 3. Número de estudos por país

descrito em seis estudos (E02, E05, E08, E10, E15, E19). A Tabela 7 apresenta todos os riscos identificados. Em seguida, esses riscos são descritos por dimensão.

Riscos técnicos. R01 refere-se ao comprometimento da cadeia de suprimentos de software em ECOS. E02 destaca que essa cadeia se tornou um vetor crítico para ameaças de cibersegurança, enquanto E05 mostra que ataques desse tipo em ECOS de código aberto frequentemente envolvem a injeção de código malicioso durante o desenvolvimento e a distribuição de artefatos. Além disso, E08 evidencia como falhas introduzidas em dependências *upstream* podem comprometer todo o ecossistema, exemplificado pela violação de dados da Equifax em 2017, decorrente de falha no Apache Struts, e pelo *bug* Heartbleed no OpenSSL.

R02 trata da exposição contínua a vulnerabilidades no ecossistema. Esse risco está associado ao atraso na aplicação de correções, muitas vezes causado pelo fenômeno do *Transitive Growth*, em que o número crescente de dependências amplia a superfície

Tabela 7. Riscos específicos identificados em ECOS

ID	Risco	Categoria	Estudos
R01	Comprometimento da cadeia de suprimentos de software	Técnico	E02, E05, E08, E10, E15, E19
R02	Exposição contínua a vulnerabilidades em múltiplos componentes do ECOS	Técnico	E09, E11, E13, E35
R03	Vulnerabilidades em dependências transitivas de bibliotecas	Técnico	E11, E31
R04	Incompatibilidade entre versões de bibliotecas interdependentes	Técnico	E12, E22, E30, E31
R05	Ataques direcionados à infraestrutura e aos pacotes do ecossistema	Técnico	E03, E09, E12, E13, E22
R06	Injeção de código malicioso em pacotes distribuídos pelo ecossistema	Técnico	E05, E19
R07	Atualizações inseguras de dependências em bibliotecas compartilhadas	Técnico	E05, E10, E24
R08	Propagação de *bugs* não resolvidos entre projetos do ecossistema	Técnico	E03, E08
R09	Abandono de bibliotecas essenciais do ecossistema	Técnico	E03, E08
R10	Envelhecimento de bibliotecas abertas amplamente utilizadas	Técnico	E01, E27
R11	Fragilidades na infraestrutura compartilhada de desenvolvimento	Técnico	E34
R12	Perda de confiança devido a pacotes maliciosos ou enganosos no ecossistema	Social	E02, E13, E19
R13	Conflitos de interesse na governança do ecossistema (*moral hazard*)	Social	E20
R14	Falhas de comunicação entre os múltiplos atores do ecossistema	Social	E07, E21
R15	Ausência de mecanismos formais de governança no ecossistema	Social	E09, E18
R16	Sobrecarga de mantenedores de múltiplos pacotes críticos	Social	E12
R17	Dependência crítica de poucos mantenedores (*Truck Factor*)	Social	E08
R18	Ameaças de *insiders* maliciosos no ecossistema	Social	E19
R19	Ausência ou deficiência de documentação das plataformas	Negócio	E09, E15, E18, E28
R20	Altos custos de manutenção e risco de migração para plataformas concorrentes	Negócio	E01, E29
R21	Percepção de valor insuficiente para adesão e permanência no ecossistema	Negócio	E04, E06
R22	Perda de controle da plataforma ou fragmentação do ecossistema	Negócio	E25, E28
R23	Fracasso em fases iniciais de implantação do ECOS	Negócio	E04
R24	Descontinuidade ou morte do ecossistema	Negócio	E18

de ataque, como apontado em E09. E11 mostra que muitas aplicações permanecem expostas a falhas conhecidas mesmo após a disponibilização de correções, enquanto E13 evidencia que desenvolvedores podem levar anos para atualizar dependências, permitindo que vulnerabilidades se propaguem entre ecossistemas. No mesmo contexto, R03 aborda vulnerabilidades presentes em dependências, especialmente transitivas, que estão além do controle dos desenvolvedores. E31 evidencia que a disseminação global do código aberto intensifica o problema, ampliando a propagação de falhas em múltiplos ecossistemas.

R04 aborda a incompatibilidade entre versões de bibliotecas no ecossistema. Embora também esteja ligado às dependências, distingue-se do R03 por não tratar de vulnerabilidades de segurança, mas de falhas de manutenção e evolução. E12 mostra que redes extensas de bibliotecas ampliam a chance de incompatibilidades, enquanto E22 aponta que a utilização de versões desatualizadas agrava o risco. E31 acrescenta que esses problemas podem gerar impactos em cascata (*rippling impact*), comprometendo múltiplos projetos interdependentes no ECOS.

R05 está relacionado a ataques direcionados à segurança de ECOS. E03 mostra que o aumento da superfície de ataque impacta diretamente a proteção dos sistemas, enquanto E09 evidencia que a ampla disponibilidade de software de código aberto, como no ecossistema Maven, amplia as possibilidades de exploração. Complementarmente, R06 aborda um vetor específico desses ataques, a injeção de código malicioso em pacotes. E05 e E19 descrevem como invasores podem comprometer bibliotecas e mostram a variedade de vetores explorados para propagar esse tipo de ataque.

R07 refere-se a atualizações inseguras de dependências em ECOS. Nesse caso, segundo E10, o risco surge quando o processo de atualização introduz falhas, como *pull requests* que executam código não verificado. R08, por sua vez, apresenta a situação

oposta, a ausência de atualização. *Bugs* não resolvidos em pacotes *upstream* podem se propagar por toda a rede, como evidenciado por E03 e E08, comprometendo em larga escala bibliotecas e sistemas dependentes. Assim, enquanto R07 está ligado ao risco de atualizar de forma insegura, R08 está ligado ao risco de não atualizar, ambos refletindo desafios complementares no gerenciamento de dependências.

R09 trata do abandono de bibliotecas em ECOS. E03 destaca que a descontinuidade de projetos pode comprometer gravemente sistemas dependentes, enquanto E08 mostra que a dependência de mantenedores voluntários amplia a vulnerabilidade a esse risco. E08 ainda aponta que mais da metade das bibliotecas do ecossistema NPM (*Node Package Manager*) depende, de forma transitiva, de pelo menos uma biblioteca abandonada. Nesse mesmo contexto, R10 refere-se ao envelhecimento de bibliotecas abertas em ECOS. E27 evidencia que a ausência de manutenção aumenta a exposição a falhas e vulnerabilidades, ampliando os riscos para sistemas dependentes dessas bibliotecas. R11, por sua vez, está associado a fragilidades no processo de desenvolvimento em ECOS. E34 aponta que a ausência de modelos de processo padronizados, as dificuldades na coleta de requisitos e a incerteza em manter padrões de qualidade comprometem a confiabilidade e aumentam a probabilidade de falhas.

Riscos sociais. R12 está relacionado à perda de confiança entre os múltiplos atores do ECOS. E02 mostra como pacotes podem ser rotulados de forma enganosa para ocultar funcionalidades prejudiciais, comprometendo a credibilidade dos provedores. De forma semelhante, E13 aponta que vulnerabilidades podem resultar não apenas em perdas financeiras, mas também em danos à reputação e à relação de confiança com os usuários. Esse risco se intensifica à medida que os ecossistemas crescem e a confiança passa a ser distribuída entre múltiplos atores. R13 refere-se a conflitos de interesse entre atores do ecossistema. E20 discute o fenômeno de *moral hazard*, no qual desenvolvedores se beneficiam da reutilização de bibliotecas, mas transferem os riscos associados ao seu uso para os usuários finais. Diferentemente do R12, o foco do R13 não está na quebra da confiança percebida, mas na assimetria de incentivos que compromete a sustentabilidade do ECOS.

R14 diz respeito a falhas de comunicação entre os participantes do ecossistema. E07 evidencia que equipes com opiniões divergentes e sem coordenação clara enfrentam dificuldades em atingir objetivos comuns. Em complemento, E21 mostra que a ausência de diálogo pode resultar em problemas típicos de má gestão, como inexperiência das equipes e planejamento deficiente. R15, por sua vez, envolve a ausência de governança adequada nos ecossistemas. E09 e E18 demonstram que a inexistência de regras ou estruturas de governança formais, principalmente em ECOS de código aberto, gera riscos difíceis de controlar e impacta diretamente a sustentabilidade e a segurança do ecossistema.

R16 está ligado à sobrecarga de mantenedores em ECOS. E12 demonstra que a ausência de remuneração e de processos formais para gerenciar contribuições externas aumenta significativamente a carga de trabalho desses atores, colocando em risco a continuidade dos projetos. Esse cenário compromete a motivação dos colaboradores e amplia a possibilidade de falhas decorrentes de sobrecarga. Relacionado a esse contexto, R17 refere-se à dependência crítica de poucos mantenedores, conhecida como *Truck Factor*. E08 destaca que quando o conhecimento essencial está concentrado em poucos indivíduos, o abandono ou a indisponibilidade desses colaboradores pode gerar falhas em cascata em bibliotecas dependentes, ameaçando todo o ecossistema. R18 aborda a ameaça

de *insiders* maliciosos nos ECOS. E19 descreve casos em que desenvolvedores insatisfeitos ou mal-intencionados comprometem deliberadamente pacotes de software, criando vulnerabilidades intencionais. De acordo com E19, esse risco se diferencia dos ataques externos por envolver atores internos com acesso privilegiado e conhecimento específico do projeto, o que o torna especialmente difícil de detectar e mitigar.

Riscos de negócios. R19 refere-se à ausência ou deficiência de documentação em plataformas de ECOS. E09 mostra que muitas bibliotecas não possuem arquivos obrigatórios, como código-fonte e documentação (*javadoc*), dificultando o trabalho dos desenvolvedores. De forma semelhante, E15 aponta que a falta de documentação adequada reduz a percepção de riscos pelos usuários e facilita a inserção de modelos maliciosos, como *EvilModels*. Além disso, E18 e E28 destacam que documentações incompletas ou pouco claras comprometem a validação de propostas e podem gerar falhas de segurança. Relacionado a esse contexto, R20 está ligado aos altos custos de manutenção e ao risco de migração para plataformas concorrentes. E01 e E29 evidenciam que a perda de clientes para soluções alternativas é um risco significativo, geralmente associado à ausência de suporte ou manutenção. Neste cenário, o provedor da plataforma (*keystone*) deve gerenciar a fidelização do cliente e aumentar os custos de mudança.

R21 diz respeito à percepção de valor insuficiente para adesão e permanência no ECOS. E04 mostra que ECOS falham quando não conseguem oferecer valor claro para seus participantes, levando ao abandono. Em complemento, E06 ressalta que, mesmo quando as organizações reconhecem algum valor, o processo de decisão sobre investimentos em parcerias ainda é pouco compreendido, aumentando a incerteza quanto à realização do valor esperado. R22, por sua vez, envolve a perda de controle da plataforma ou sua fragmentação. E25 mostra que a falha em um único serviço pode paralisar toda a operação, dificultando a identificação da causa raiz, que pode estar em diferentes fornecedores. E28 aponta que o risco de perda de controle é ampliado em ECOS de código aberto, pois desenvolvedores externos podem modificar diretamente a plataforma, gerando fragmentação.

R23 está relacionado ao fracasso em fases iniciais de implantação de ECOS. E04 evidencia que falhas no design do produto mínimo viável, quando mal definido, reduzem a atratividade para clientes e comprometem o engajamento dos participantes, aumentando as chances de insucesso. R24, de maneira complementar, refere-se à descontinuidade ou morte do ecossistema. E18 destaca que a ausência de conhecimento sobre as peculiaridades dos ECOS, aliada à falta de mecanismos de governança, pode levar à obsolescência e, em última instância, à extinção do ECOS.

4.2. QP2 – Quais são as soluções utilizadas na gerência de riscos em ECOS?

Esta QP teve como propósito identificar e descrever as soluções utilizadas na gerência de riscos em ECOS. Para classificar essas soluções, foi adotada a taxonomia proposta por [Shaw 2003], que organiza contribuições em diferentes níveis: (i) teoria, entendida como um conjunto de ideias voltado a explicar determinado fenômeno; (ii) modelo, que corresponde a uma estrutura ou taxonomia direcionada a um domínio de problema; (iii) método ou técnica, que representa um procedimento específico para realizar uma atividade; (iv) prática, que se refere a uma nova ou aprimorada forma de executar uma tarefa; (v) ferramenta, caracterizada como um artefato que implementa uma técnica; e (vi) *framework*, definido como uma estrutura de suporte que auxilia na execução de tarefas.

A Tabela 8 apresenta o conjunto de soluções identificadas e sua classificação, conforme [Shaw 2003]. A categoria mais recorrente foi a de ***frameworks***, com 7 soluções (E02, E06, E08, E19, E30, E31, E33), seguida da de **modelos**, com 6 soluções (E17, E18, E20, E22, E27, E32). Também foram identificadas **práticas**, presentes em 3 soluções (E01, E15, E25), além de **ferramentas**, presentes em 2 soluções (E11, E16). Por fim, a categoria de **métodos** foi observada em 2 soluções (E23, E28).

Tabela 8. Soluções identificadas (agrupadas por categoria)

ID	Soluções	Classificação	Estudos
S01	*Framework* baseado em HIN e Metapath2Vec para classificação de pacotes	*Framework*	E02
S02	*Framework* para seleção de fornecedores de software em ECOS	*Framework*	E06
S03	*Framework* para modelagem de riscos socio-técnicos em ECOS	*Framework*	E08
S04	*Framework* conceitual de mecanismos de variabilidade em ECOS	*Framework*	E33
S05	*Framework* distribuído TrustSECO para registrar e calcular fatos de confiança	*Framework*	E19
S06	*Intelligent Software Assurance and Monitoring* (ISAM)	*Framework*	E30
S07	*Framework* SE-GPS baseado em Web Semântica para rastreamento de vulnerabilidades	*Framework*	E31
S08	Modelo de representação de metas e anti-metas baseadas em confiança	Modelo	E17
S09	Modelo conceitual de governança de ECOS para mitigar riscos	Modelo	E18
S10	Modelo de *technical leverage* para avaliar riscos de dependências em ECOS	Modelo	E20
S11	Modelo teórico sobre relação entre reutilização de software e riscos de segurança em ECOS	Modelo	E22
S12	Modelo de envelhecimento de bibliotecas baseado em uso de clientes (*library usage*)	Modelo	E27
S13	Modelo baseado em processos de decisão de Markov para identificar riscos	Modelo	E32
S14	Assegurar a robustez da plataforma para mitigar riscos no ECOS	Prática	E01
S15	Atrair, manter e apoiar atores para mitigar riscos de engajamento, conflitos e permanência	Prática	E01
S16	Adotar mecanismos de segurança em hubs de modelos pré-treinados	Prática	E15
S17	Usar *Service Level Agreements* (SLA) como prática de gerência de riscos	Prática	E25
S18	Ferramenta *DepReveal* para descoberta e análise de vulnerabilidades em projetos NPM	Ferramenta	E11
S19	Ferramenta *smartPip* para mitigar conflitos de dependências em ECOS Python	Ferramenta	E16
S20	Método de gerenciamento da confiabilidade da cadeia de suprimentos de software	Método	E23
S21	Método multicritério para selecionar tipos de ECOS e e decisões estratégicas	Método	E28

***Frameworks*.** E02 demonstra que a aplicação de um *framework* baseado em HIN e Metapath2Vec (S01) em pacotes NPM reduz a exposição a bibliotecas maliciosas e fortalece a cadeia de suprimentos em ECOS. Em seguida, E06 destaca que a utilização de um *framework* para seleção de fornecedores (S02) permite estruturar critérios de decisão, aumentando a transparência e reduzindo riscos técnicos e organizacionais em ECOS. Complementando essa perspectiva, E08 mostra que a integração entre riscos técnicos e sociais em um *framework* de riscos socio-técnicos (S03) possibilita identificar pontos críticos e propor cenários de intervenção no contexto de ECOS.

E33 analisa mecanismos de variabilidade (S04) em diferentes ECOS e demonstra que eles ajudam a reduzir riscos de *lock-in*, inconsistências e fragmentação. Na área de confiança e segurança, E19 apresenta o TrustSECO (S05), um *framework* distribuído baseado em *Distributed Ledger Technology* (DLT) capaz de registrar e calcular fatos de confiança, apoiando tanto a detecção de vulnerabilidades quanto a reconfiguração de sistemas em ECOS. Outros trabalhos avançam no uso de dados para prever e mitigar riscos. E30 propõe o *ISAM* (S06), que combina informações sociais e técnicas para antecipar falhas e reduzir riscos em ECOS. Por sua vez, E31 descreve o SE-GPS (S07), mostrando que a integração de repositórios de vulnerabilidades e software amplia a visibilidade sobre riscos de dependência em ECOS e contribui para diminuir o tempo de exposição.

Modelos. E17 organiza preocupações de confiança em diferentes níveis com um modelo de metas e anti-metas (S08), favorecendo a análise de riscos ligados a motivações maliciosas ou falhas intencionais de atores em ECOS. No mesmo campo, E18 evidencia que a ausência de mecanismos formais compromete a sustentabilidade do ECOS e que um

modelo conceitual de governança (S09) pode contribuir para mitigar riscos. E20 introduz o conceito de *technical leverage* (S10), que quantifica a proporção de código herdado e indica projetos mais expostos a falhas de segurança no ECOS. E22 discute um modelo teórico de reutilização de software (S11), argumentando que a prática pode reduzir riscos ao apoiar-se em bibliotecas maduras, mas também ampliá-los ao aumentar a superfície de ataque em ECOS.

E27 propõe um modelo de envelhecimento de bibliotecas (S12), mostrando que prever a obsolescência a partir do uso por clientes permite planejar atualizações e reduzir riscos de manutenção e segurança em ECOS. E32 aplica um modelo baseado em processos de decisão de Markov (S13) para simular cenários de integração no ecossistema, identificando gargalos e apoiando a mitigação de riscos de desempenho e robustez.

Práticas. E01 ressalta a importância da robustez da arquitetura, do planejamento da evolução e da validação de terceiros como formas de mitigar vulnerabilidades estruturais em ECOS, caracterizando uma prática de mitigação de riscos ligados à plataforma (S14). E01 também evidencia que práticas de governança voltadas a atrair e reter participantes (S15) são fundamentais para mitigar conflitos, engajamento insuficiente e problemas de *multihoming*. Em outra perspectiva, E15 aponta que a adoção de mecanismos de segurança em hubs de modelos pré-treinados (S16), como auditoria, controle de permissões e varredura de *malware*, contribui para prevenir *uploads* maliciosos e aumentar a rastreabilidade em ECOS. De modo relacionado, E25 destaca que o uso de SLA (S17) em contextos *as-a-service* auxilia na redução de riscos técnicos e organizacionais.

Ferramentas. E11 descreve a ferramenta *DepReveal* (S18), mostrando como sua aplicação em projetos NPM identifica vulnerabilidades e classifica *advisories*, o que reduz o tempo de exposição a ataques e fortalece a resposta a incidentes em ECOS. Em complemento, E16 apresenta a ferramenta *smartPip* (S19), demonstrando que a resolução de conflitos de dependência por meio de restrições lógicas e otimização de bibliotecas em ambientes virtuais previne falhas de instalação e reduz custos de manutenção em ECOS.

Métodos. E23 propõe um método para gerenciar a confiabilidade da cadeia de suprimentos (S20), utilizando grafos de conhecimento para identificar vulnerabilidades, calcular escores de confiabilidade e recomendar ações de mitigação em ECOS. Complementarmente, E28 apresenta um método multicritério para seleção de tipos de ECOS em eletrônicos de consumo (S21), no qual a análise conjunta de requisitos de mercado e de engenharia com diferentes tipos de ecossistemas permite antecipar riscos de integração e evolução, além de apoiar decisões estratégicas mais seguras.

4.3. QP3 – Como essas soluções têm sido avaliadas?

Esta questão buscou identificar de que forma as soluções para a gerência de riscos em ECOS foram avaliadas e em quais contextos esses estudos foram conduzidos. Das 21 soluções identificadas, 15 apresentaram algum tipo de avaliação, enquanto 6 não tiveram avaliação formal reportada. As abordagens identificadas mostraram diversidade de métodos e cenários de aplicação.

A categoria de avaliação mais recorrente foi a de **estudos de caso**, presente em sete soluções (S02, S04, S08, S10, S13, S14, S17), aplicados em contextos que vão desde ECOS de código aberto, como GNOME e Maven, até ECOS de código proprietário, como SAP. Em seguida, destacam-se os **estudos experimentais**, empregados em três

soluções (S01, S20, S21), abrangendo desde experimentos com milhares de pacotes em repositórios até a validação de protótipos em sistemas reais. Também foram identificadas avaliações baseadas em **mineração de repositórios** (S05, S11), além de abordagens qualitativas como **entrevistas** (S15, S16) e **pesquisa de opinião e grupo focal** (S18), que ampliam a diversidade de perspectivas.

No conjunto analisado, seis soluções (S03, S06, S07, S09, S12, S19) não apresentaram qualquer forma de avaliação formal, evidenciando lacunas na validação prática de determinadas propostas. Por outro lado, algumas soluções recorreram a métodos mistos, combinando entrevistas, mineração de dados, estudos de caso e experimentos (como em S08, S13 e S17), o que enriquece a análise e amplia a confiabilidade dos resultados. A Tabela 9 apresenta o panorama detalhado das avaliações identificadas.

Tabela 9. Avaliação das soluções identificadas

ID	Avaliada?	Tipo de Estudo	Contexto
S01	Sim	Estudo Experimental	Avaliação no ECOS NPM com 17.067 pacotes para classificação binária e 1.500 pacotes em 10 classes funcionais, comparando com DeepWalk e Node2Vec
S02	Sim	Estudo de caso	Avaliação considerando 2 fornecedores (Vendor X e Y) e 2 tomadores de decisão, aplicando o método ICR para seleção de software
S03	Não	-	-
S04	Sim	Estudo de caso	Avaliação em cinco ECOS (eCos, Linux, Debian, Eclipse, Android) com análise qualitativa e quantitativa
S05	Sim	Mineração de repositórios + Estudo de caso	Avaliação em 4.500 projetos clientes, 1.500 versões de bibliotecas e 852.322 dependências no Maven
S06	Não	-	-
S07	Não	-	-
S08	Sim	Estudo Experimental + Estudo de caso	Avaliação no ECOS Maven (92.989 projetos e 795.311 versões), incluindo 3 estudos de caso e comparação com OWASP Dependency-Check
S09	Não	-	-
S10	Sim	Estudo de caso	Avaliação nos ECOS SAP e GNOME por análise documental da governança
S11	Sim	Mineração de repositórios	Avaliação no ECOS Maven (8.464 bibliotecas Java), aplicando métricas de alavancagem técnica, evolução e vulnerabilidades
S12	Não	-	-
S13	Sim	Estudo Experimental + Estudo de caso	Avaliação no ECOS Maven com 1.500 bibliotecas, incluindo análise quantitativa de modelos de envelhecimento e 2 estudos de caso
S14	Sim	Estudo de caso	Avaliação em cenário simulado de processamento de pedidos em um ECOS empresarial
S15	Sim	Entrevista	Avaliação com 6 profissionais em 3 ecossistemas emergentes, confirmando a estratégia de assegurar a robustez da plataforma
S16	Sim	Entrevista	Avaliação com 6 profissionais em 3 ecossistemas emergentes, confirmando a estratégia de atrair, manter e apoiar atores
S17	Sim	Mineração de repositórios + Estudo de caso	Avaliação em 8 hubs de modelos pré-treinados, com estudo de caso no ECOS Hugging Face e medições de riscos (discrepâncias e alcance de mantenedores)
S18	Sim	Pesquisa de opinião + Grupo focal	Avaliação com 41 organizações de diferentes setores e grupo focal com 5 empresas do ECOS PIMM DMA
S19	Não	-	-
S20	Sim	Estudo Experimental	Avaliação em 3 datasets de projetos Python (WatchMan, HG2.9K, AAAI 2021), comparando com pip, Conda e venv
S21	Sim	Estudo Experimental	Avaliação com 24 participantes (pesquisadores, profissionais e mestrandos) e protótipo testado em um sistema operacional Linux/RISC-V

4.4. QP4 – Quais são os desafios da gerência de riscos em ECOS?

Esta QP buscou identificar os principais desafios discutidos na literatura sobre gerência de riscos em ECOS. A análise mostrou que muitos estudos abordam problemas semelhantes sob diferentes perspectivas. Assim, os desafios foram consolidados para evitar redundâncias e destacar apenas aqueles claramente definidos. Ao todo, foram identificados 14 desafios, refletindo preocupações recorrentes nas dimensões técnica, social e de negócios. A Tabela 10 sintetiza esses desafios.

Tabela 10. Desafios identificados na gerência de riscos em ECOS

ID	Desafio	Estudos
D01	Coordenar múltiplos atores no processo de correção e evolução, incluindo desafios organizacionais e culturais em larga escala.	E07, E12, E13, E26
D02	Reduzir a exposição prolongada a vulnerabilidades, afetada por atrasos na atualização de dependências e na aplicação de *patches*.	E11, E13, E35
D03	Estruturar mecanismos eficazes de governança que alinhem aspectos sociais, técnicos e de negócio, evitando *lock-in* e promovendo sustentabilidade.	E18, E25
D04	Conciliar reaproveitamento técnico e reutilização de software, equilibrando benefícios de qualidade com riscos de segurança e aumento da superfície de ataque.	E20, E22
D05	Tratar da insuficiência de mecanismos de defesa em hubs e registries, bem como da ausência de ferramentas de auditoria e escaneamento abrangentes.	E15, E19
D06	Reduzir limitações metodológicas ligadas ao uso de *release notes* e ausência de validação em ECOS reais, que comprometem a generalização de resultados.	E14
D07	Monitorar sinais de abandono e inatividade em bibliotecas para antecipar riscos de manutenção.	E03
D08	Superar dificuldades na resolução de conflitos de dependência, evitando falhas de instalação e custos de manutenção.	E16
D09	Lidar com a complexidade da análise e evolução de pacotes maliciosos, considerando múltiplos ecossistemas OSS e diferentes estratégias de ataque.	E05
D10	Enfrentar más práticas de empacotamento que comprometem segurança, manutenção e escalabilidade dos ECOS.	E09
D11	Integrar riscos sociais e técnicos, considerando sua interdependência na propagação de vulnerabilidades e fragilidade de comunidades.	E08
D12	Definir metas, anti-metas e prioridades claras para apoiar a análise de confiança e reduzir riscos de motivações maliciosas.	E17
D13	Melhorar a integração de informações dispersas em múltiplos repositórios de software e vulnerabilidades, ampliando a rastreabilidade da cadeia de suprimentos.	E31
D14	Antecipar riscos de desempenho e robustez em cenários de integração complexa, por meio de simulações e modelos de decisão.	E32

Entre os desafios identificados, destacam-se a coordenação de múltiplos atores (D01) e a redução de exposições prolongadas a vulnerabilidades (D02). Esses achados indicam que a dimensão social permanece crítica para a sustentabilidade dos ECOS, evidenciando que, apesar dos avanços técnicos, a integração entre comunidades, processos decisórios e governança ainda constitui um obstáculo central à gerência de riscos.

5. Discussão

Este estudo identificou riscos, soluções e desafios voltados à gerência de riscos em ECOS, mapeando *frameworks*, modelos, práticas, ferramentas e métodos. A partir da análise dos 710 estudos recuperados, 35 atenderam ao CI e não se enquadraram nos CE, sendo selecionados para avaliação detalhada e compondo a base de evidências deste MSL.

Em resposta à QP, os resultados indicam que a gerência de riscos em ECOS tem sido conduzida por soluções técnicas voltadas ao controle de dependências e vulnerabilidades (E02, E11, E15, E16, E20, E23, E27, E31), acompanhadas por iniciativas de governança pontuais e pouco estruturadas (E01, E08, E18). A análise também mostra lacunas na relação entre riscos, soluções e desafios: (i) riscos críticos, como o *comprometimento da cadeia de suprimentos* (R01) e a *exposição contínua a vulnerabilidades* (R02), ainda não possuem soluções validadas em contextos reais; (ii) algumas soluções, como *frameworks* de governança (S02, S10), abordam parcialmente os desafios de *coordenação entre múltiplos atores* (D01) e de *integração de riscos sociais e técnicos* (D09); e (iii) desafios recorrentes, como a *ausência de mecanismos eficazes de governança* (D11), permanecem sem respostas consolidadas, indicando distância entre propostas conceituais e práticas de adoção.

Outro aspecto crítico é que, embora 15 das 21 soluções identificadas apresentem

algum tipo de avaliação, observa-se que muitas dessas avaliações são restritas a *estudos de caso* em contextos limitados (e.g., ECOS específicos como GNOME ou SAP), comprometendo a generalização dos resultados. Esse cenário evidencia a importância de investigações que explorem diferentes métodos e contextos, de modo a ampliar a compreensão sobre a aplicabilidade prática das soluções propostas em ecossistemas de diferentes naturezas (i.e., de código aberto, de código proprietário e híbrido).

A RSL de [Valério et al. 2020], que investigou a gerência de riscos em projetos de software em geral, apontou a importância do alinhamento entre estratégia de negócios e práticas de gerência de riscos. Os resultados deste estudo mostram que esse desafio é ainda mais complexo em ECOS, refletido em riscos de governança (R15) e, de forma particular, no desafio D08, que trata das dificuldades na resolução de conflitos de dependências. Esse ponto mostra que mesmo soluções conceituais, como o *framework* de seleção de fornecedores (S02), ainda não oferecem mecanismos eficazes de alinhamento entre decisões técnicas e de negócios, deixando lacunas na gerência integrada de riscos.

De forma complementar, a RSL de [Luthfiansyah et al. 2024], centrada em técnicas e ferramentas de apoio à gerência de riscos, destacou práticas tradicionais como *brainstorming* e análise de causa raiz. Embora relevantes, tais abordagens não se mostram suficientes para lidar com riscos específicos de ECOS, como a *propagação de vulnerabilidades em dependências transitivas* (R03). Esse cenário explica o surgimento de soluções mais direcionadas, como o *framework* TrustSECO (S11) e a ferramenta DepReveal (S19). De modo semelhante, o MSL de [Lopes et al. 2020] em sistemas de sistemas ressaltou a ausência de abordagens consolidadas para lidar com riscos oriundos da interação de múltiplas partes interessadas. Esse problema também se manifesta em ECOS, refletido em riscos sociais como a *sobrecarga de mantenedores* (R16) e o *Truck Factor* (R17), que se relacionam diretamente aos desafios de *coordenação* (D07) e *integração de dimensões sociais e técnicas* (D03).

À luz da Teoria Sociotécnica [Trist 1981], que reconhece a interdependência entre componentes técnicos e sociais, os achados reforçam que riscos em ECOS não podem ser compreendidos apenas como falhas técnicas isoladas. Eles emergem da interdependência entre componentes técnicos, sociais e de negócios e podem gerar efeitos em cascata quando não tratados de forma integrada. Assim, intervenções restritas a apenas uma dessas dimensões tendem a produzir ganhos limitados, como ocorre em processos de governança sem métricas de qualidade. A gerência de riscos em ECOS exige, portanto, estratégias integradas que combinem monitoramento técnico, práticas de governança e coordenação social, fortalecendo a resiliência e a sustentabilidade do ecossistema.

6. Ameaças à validade

Durante a execução deste estudo, buscou-se minimizar a influência de possíveis ameaças à validade e reduzir seus potenciais impactos. **Validade descritiva**: as principais ameaças incluem erros na codificação e divergências na extração. Para minimizá-las, utilizou-se um formulário de extração padronizado, preenchido por dois pesquisadores e revisado por outros dois, assegurando qualidade e reduzindo vieses individuais. **Validade teórica**: as ameaças referem-se à definição da *string* de busca e ao risco de omissão de estudos relevantes. Para mitigá-las, os estudos foram selecionados com base em CI e CE previamente definidos. Além disso, a *string* de busca foi elaborada de forma ampla e aplicada sem

restrições quanto ao período de publicação, sendo fundamentada em estudos relacionados e em recomendações metodológicas consolidadas. **Validade interpretativa**: as ameaças incluem divergências de interpretação tanto na seleção dos estudos quanto na extração dos dados. Para mitigar o viés, as dúvidas surgidas durante essas etapas foram discutidas coletivamente e as divergências foram analisadas e resolvidas por consenso entre os pesquisadores envolvidos. **Generalização:** as ameaças relacionam-se à delimitação das bases de dados selecionadas. Para mitigá-las, foram adotados os protocolos propostos por [Kitchenham e Charters 2007] e [Petersen et al. 2015], o que favorece a replicação do estudo. Além disso, os resultados refletem os trabalhos disponíveis nas bibliotecas digitais consideradas e podem não abranger produções fora do escopo definido, limitando a abrangência, mas sem comprometer a análise do estado da arte.

7. Conclusão

Este estudo buscou responder à QP: *Como a gerência de riscos tem sido realizada em ECOS?* Para isso, foi conduzido um MSL com 35 estudos primários. Os resultados evidenciam que a gerência de riscos em ECOS possui especificidades em relação a outros contextos de desenvolvimento de software, demandando soluções que considerem a interdependência entre aspectos técnicos, sociais e organizacionais. Foram identificados 24 riscos específicos de ECOS (QP1), 21 soluções propostas (QP2) e 14 desafios consolidados (QP4). Entre as soluções, 15 apresentaram avaliação experimental em diferentes contextos (QP3), o que representa avanços relevantes, mas ainda evidencia lacunas quanto à validação em cenários amplos e reais.

Sob a perspectiva da Teoria Sociotécnica [Trist 1981], os achados mostram que riscos em ECOS emergem da interação entre tecnologia, processos e pessoas, o que exige estratégias integradas que combinem monitoramento técnico, mecanismos de governança e práticas de colaboração. A principal contribuição científica deste estudo está em oferecer a primeira visão sistemática sobre a gerência de riscos em ECOS, consolidando evidências dispersas em categorias de riscos, soluções e desafios. Para a prática, os resultados podem apoiar pesquisadores e profissionais na adoção de estratégias mais consistentes para identificar, monitorar e mitigar riscos em ECOS.

Como trabalhos futuros, recomenda-se expandir o MSL para aprofundar a análise comparativa entre diferentes tipos de ECOS, como os de código proprietário e de código aberto. Outra direção relevante é a estruturação de taxonomias e *frameworks* conceituais a partir dos resultados sintetizados, com o objetivo de apoiar pesquisas futuras e a formulação de métodos mais consistentes de gerência de riscos em ECOS. Essas iniciativas podem fortalecer a compreensão da gerência de riscos e contribuir para a resiliência e sustentabilidade dos ECOS em um cenário de software cada vez mais complexo.

Disponibilidade de artefatos

Os dados e os procedimentos do estudo estão disponíveis no material suplementar, acessível em https://doi.org/10.5281/zenodo.17261825.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001, CNPq (Proc. 316510/2023-8), FAPERJ (Proc. E-26/204.404/2024), UNIRIO e UFRA.

Referências

Bilousiva, L., Gryzun, L., Zhytienova, N. e Pikalova, V. (2023). Issues of formalization of risk management process in software design. In *4th International Workshop on Intelligent Information Technologies and Systems of Information Security*, pages 48–57.

Boscarioli, C., Araujo, R. M. e Maciel, R. S. P., editors (2017). *I GranDSI-BR – Grand Research Challenges in Information Systems in Brazil 2016–2026*. SBC, Porto Alegre, Brazil.

Campos, G. d. S. S. d., Silva, F. I. R. d., Malcher, P. e Santos, R. P. d. (2025). Material suplementar do artigo "challenges and solutions of risk management in software ecosystems"'. https://doi.org/10.5281/zenodo.17261825.

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage.

Chen, X. e Deng, Y. (2022). An evidential software risk evaluation model. *Mathematics*, 10(13).

Damian, D., Linåker, J., Johnson, D., Clear, T. e Blincoe, K. (2021). Challenges and strategies for managing requirements selection in software ecosystems. *IEEE Software*, 38(6):76–87.

Hou, F. e Jansen, S. (2024). A survey of the state-of-the-art approaches for evaluating trust in software ecosystems. *Journal of Software: Evolution and Process*, 36(10):e2695.

Jansen, S. (2020). A focus area maturity model for software ecosystem governance. *Information and Software Technology*, 118:106219.

Keshani, M., Bot, G., Rungta, P., Izadi, M., Van Deursen, A. e Proksch, S. (2024). Maven unzipped: Exploring the impact of library packaging on the ecosystem. In *2024 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, pages 50–62.

Kitchenham, B. e Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical report, Evidence-Based Software Engineering (EBSE) Project.

Lopes, S. d. S., Vargas, I. G., Oliveira, A. L. d. e Braga, R. T. V. (2020). Risk management for system of systems: A systematic mapping study. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, pages 258–265. IEEE.

Luthfiansyah, F., Prasetyo, A. e Raharjo, T. (2024). A systematic review of risk management tools and techniques in software projects. *The Indonesian Journal of Computer Science*, 13(1).

Manalif, E., Capretz, L. F. e Ho, D. (2013). Software ecosystems risks. In *8th International Conference on Software Engineering and Applications*, pages 417–422.

Mandych, O., Zaika, S., Zaika, O., Zhyliakova, O., Blyzniuk, et al. (2023). Risk management of innovation activities in the digital ecosystem. *INNOVATIONS IN THE SCIENTIFIC, TECHNICAL AND SOCIAL ECOSYSTEMS*, 1(6):24–45.

Manikas, K. (2016). Revisiting software ecosystems research: A longitudinal literature study. *Journal of Systems and Software*, 117:84–103.

Menezes Jr, J., Gusmão, C. e Moura, H. (2019). Risk factors in software development projects: a systematic literature review. *Software Quality Journal*, 27(3):1149–1174.

Mens, T. e Roover, C. d. (2023). *An Introduction to Software Ecosystems*, pages 1–29. Springer International Publishing, Cham.

Messerschmitt, D. G. e Szyperski, C. (2003). *Software Ecosystem: Understanding an Indispensable Technology and Industry*. MIT press.

Oliveira, J. e Alves, C. (2021). Software ecosystems governance – an analysis of sap and gnome platforms. In *2021 47th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, pages 296–299.

Olsson, T. e Franke, U. (2019). Risks and assets: a qualitative study of a software ecosystem in the mining industry. In *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ESEC/FSE 2019, page 895–904, New York, NY, USA. Association for Computing Machinery.

Petersen, K., Vakkalanka, S. e Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and software technology*, 64:1–18.

Pilliang, M. e Munawar, M. (2022). Risk management in software development projects: A systematic literature review. *Khazanah Informatika: Jurnal Ilmu Komputer dan Informatika*, 8(2).

PMI (2021). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition and The Standard for Project Management*. Project Management Institute, Newtown Square, PA, 7 edition.

Prakash, B. e Viswanathan, V. (2020). A comparative study of meta-heuristic optimisation techniques for prioritisation of risks in agile software development. *International Journal of Computer Applications in Technology*, 62(2):175–188.

Schueller, W. e Wachs, J. (2024). Modeling interconnected social and technical risks in open source software ecosystems. *Collective Intelligence*, 3(1):26339137241231912.

Shaw, M. (2003). Writing good software engineering research papers. In *25th International Conference on Software Engineering*, pages 726–736. IEEE.

Siddiqui, A. T. (2024). Importance of risk management in software engineering. *Asian Journal of Technology & Management Research (AJTMR) ISSN*, 2249(0892).

Trist, E. L. (1981). *The evolution of socio-technical systems*, volume 2. Ontario Quality of Working Life Centre Toronto.

Valério, K. G. O., da Silva, C. E. S. e Neves, S. M. (2020). Risk management in software development projects: systematic review of the state of the art literature. *International Journal of Open Source Software and Processes (IJOSSP)*, 11(1):1–22.