UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE INFORMÁTICA

PAULO VICTOR DE OLIVEIRA ANDRADE

O Papel do Security Champion no Desenvolvimento de Software: Desafios, Benefícios e Impacto Organizacional em um Estudo de Replicação

RECIFE

2025

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE INFORMÁTICA

ENGENHARIA DA COMPUTAÇÃO

PAULO VICTOR DE OLIVEIRA ANDRADE

O Papel do Security Champion no Desenvolvimento de Software: Desafios, Benefícios e Impacto Organizacional em um Estudo de Replicação

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia da computação da Universidade Federal de Pernambuco, Centro de informática, como requisito para a obtenção do título de Bacharel em Engenharia da Computação.

Orientador(a): Jéssyka Flavyanne Ferreira Vilela

RECIFE

2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Andrade, Paulo Victor de.
O papel do Security Champion no desenvolvimento de software: desafios, benefícios e impacto organizacional em um estudo de replicação / Paulo Victor de Andrade. - Recife, 2025.
59 p. : il., tab.

Orientador(a): Jéssyka Vilela
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Engenharia da Computação - Bacharelado, 2025.
Inclui referências, apêndices, anexos.

1. Segurança cibernética. 2. Desenvolvimento de software. 3. Metodologias ágeis. 4. Security Champion. 5. Práticas de segurança. 6. Cultura organizacional. I. Vilela, Jéssyka. (Orientação). II. Título.

000 CDD (22.ed.)

TÍTULO DO TRABALHO: O Papel do Security Champion no Desenvolvimento de Software: Desafios, Benefícios e Impacto Organizacional em um Estudo de Replicação

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia da computação da Universidade Federal de Pernambuco, Centro de informática, como requisito para a obtenção do título de Bacharel em Engenharia da Computação.

Aprovado em: 14/04/2025.

BANCA EXAMINADORA

_____

Prof.ª Jéssyka Flavyanne Ferreira Vilela (Orientador)
Universidade Federal de Pernambuco

_____

Prof. Carla Taciana Lima Lourenco Silva (Examinador 1)
Universidade Federal de Pernambuco

_____

Prof.ª Mariana Maia Peixoto (Examinador 2)
Universidade de Pernambuco

AGRADECIMENTOS

A professora, Jéssyka Flavyanne Ferreira Vilela, por ter sido minha orientadora e ter desempenhado tal função com dedicação e paciência.

Aos meus colegas de turma, por compartilharem comigo tantos momentos de descobertas, aprendizado, companheirismo e pela troca de experiências que me permitiram crescer não só como pessoa, mas também como formando.

Aos meus pais, por nunca terem medido esforços para me proporcionar um ensino de qualidade durante todo o meu período escolar.

Quero agradecer a minha namorada, que me apoiou incansavelmente em todas as fases deste trabalho. Sua paciência, compreensão e carinho foram fundamentais para que eu pudesse manter o equilíbrio emocional e alcançar a conclusão deste TCC.

RESUMO

Contexto: A segurança cibernética é um aspecto essencial no desenvolvimento de software, especialmente diante da crescente complexidade das ameaças e da evolução constante da tecnologia. No contexto das metodologias ágeis, garantir a segurança é um desafio, pois os ciclos curtos de desenvolvimento dificultam a implementação de práticas mais detalhadas, como testes aprofundados e revisões rigorosas de código. Para lidar com essa questão, os Security Champions desempenham um papel fundamental ao integrar práticas de segurança ao fluxo de trabalho sem comprometer a agilidade da equipe. **Problema:** Apesar da adoção crescente do Security Champion no desenvolvimento de software, há pouca literatura sobre sua eficácia, desafios e impactos organizacionais. Além disso, faltam estudos sobre sua preparação, dificuldades no Brasil e influência na cultura de segurança. **Objetivo:** Este trabalho busca analisar a percepção desses profissionais sobre suas responsabilidades, sua influência na produtividade e na cultura organizacional, além dos desafios enfrentados na prática no contexto brasileiro. **Método:** Replicou-se a pesquisa de Nguyen-Duc *et al.* (2023) de forma adaptada, aplicando um questionário eletrônico a profissionais da área, coletando dados qualitativos e quantitativos. Neste estudo comparou-se, ainda, os resultados obtidos com os trabalhos anteriores, possibilitando uma visão mais abrangente das melhores práticas e dificuldades na implementação desses programas. **Resultados:** Os achados contribuem para uma melhor compreensão da atuação dos Security Champions e oferecem insights sobre como aprimorar sua participação em empresas que adotam metodologias ágeis, equilibrando eficiência e segurança no desenvolvimento de software. **Conclusões:** Para que o programa de Security Champions funcione de forma mais eficaz, é essencial que as empresas ofereçam um suporte estruturado, incluindo treinamentos contínuos e um alinhamento claro de expectativas, garantindo a incorporação da segurança ao desenvolvimento de software sem comprometer a agilidade exigida pelo mercado.

Palavras-chave: Segurança cibernética; Desenvolvimento de software; Metodologias ágeis; Security Champion; Práticas de segurança; Replicação; Cultura organizacional.

ABSTRACT

Background: Cybersecurity is an essential aspect of software development, especially in the face of the increasing complexity of threats and the constant evolution of technology. In the context of agile methodologies, ensuring security is a challenge, as short development cycles make it difficult to implement more detailed practices, such as in-depth testing and rigorous code reviews. To address this issue, Security Champions play a key role in integrating security practices into the workflow without compromising team agility. **Problem:** Despite the increasing adoption of Security Champion in software development, there is little literature on its effectiveness, challenges, and organizational impacts. In addition, there is a lack of studies on their preparation, difficulties in Brazil and influence on the safety culture. **Objective:** This paper seeks to analyze the perception of these professionals about their responsibilities, their influence on productivity and organizational culture, as well as the challenges faced in practice in the Brazilian context. **Method:** The study replicated the research of Nguyen-Duc *et al*. (2023) in an adapted manner, applying an electronic questionnaire to professionals in the field and collecting both qualitative and quantitative data. Additionally, this study compared the obtained results with previous works, providing a broader perspective on best practices and challenges in implementing these programs. **Results:** The findings contribute to a better understanding of the performance of Security Champions and offer insights on how to improve their participation in companies that adopt agile methodologies, balancing efficiency and security in software development. **Conclusions:** For the Security Champions program to work more effectively, it is essential that companies offer structured support, including continuous training and a clear alignment of expectations, ensuring the incorporation of security into the design

Keywords: Cybersecurity; Software development; Agile methodologies; Security Champion; Security practices; Replication; Organizational culture.

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

A segurança cibernética tem se consolidado como uma preocupação central no desenvolvimento de software, especialmente diante da crescente sofisticação das ameaças digitais e da rápida evolução tecnológica (HUSSAIN, 2020). Empresas de diversos setores enfrentam o desafio de proteger seus produtos e sistemas sem comprometer a eficiência e a velocidade na entrega de novas soluções (FADZISO, *et al.,* 2023). Nesse cenário, torna-se essencial buscar um equilíbrio entre segurança e produtividade, garantindo que medidas protetivas sejam implementadas de forma eficaz e contínua (OBAFEMI; NGEVAO, 2024).

Com a popularização das metodologias ágeis, esse desafio se torna ainda mais evidente. Modelos tradicionais de segurança, que priorizam longas revisões e testes apenas nas fases finais do desenvolvimento, muitas vezes não se mostram compatíveis com a dinâmica acelerada desses processos (OK; ENIOLA, 2025). Dessa forma, a segurança precisa ser integrada desde as etapas iniciais do ciclo de desenvolvimento, tornando-se um componente inerente ao fluxo de trabalho (AKSOY *et al.,* 2024).

1.2 Motivação e Justificativa

Os *Security Champions* emergem como uma estratégia para enfrentar essa questão, atuando como agentes facilitadores da segurança dentro das equipes de desenvolvimento. Seu papel envolve a disseminação de boas práticas, a identificação de riscos e a promoção de uma cultura organizacional mais voltada à segurança, tudo isso sem comprometer a agilidade necessária para a entrega de produtos (SÁNCHEZ-GORDÓN; COLOMO-PALACIOS, 2020). No entanto, a efetividade dessa abordagem está diretamente relacionada a fatores como o suporte institucional oferecido pelas empresas, a clareza das responsabilidades atribuídas a esses profissionais e a compatibilidade de suas funções com outras demandas do time (NGUYEN-DUC *et al.,* 2024).

O trabalho *Towards an Effective Security Champions Program* (AALVIK *et al.* , 2022) oferece uma análise abrangente sobre como esse papel pode ser formalizado nas empresas, apresentando sugestões para a seleção, capacitação, acompanhamento e avaliação contínua desses profissionais. A tese serviu como referência central para a construção do questionário aplicado nesta pesquisa, permitindo uma replicação metodológica e uma posterior comparação dos achados com os do estudo original. Além disso, a pesquisa de Aalvik deu origem ao estudo *Facilitating Security Champions in Software Projects – An Experience Report from Visma* (NGUYEN-DUC et al., 2024), que aplica as diretrizes propostas na tese em um estudo de caso na empresa Visma, explorando os impactos e desafios da implementação prática do programa.

O artigo *Facilitating Security Champions in Software Projects - An Experience Report from Visma* (NGUYEN-DUC *et al*., 2024) investiga o papel dos *Security Champions* no desenvolvimento de software, destacando sua importância na promoção da segurança em equipes ágeis. A pesquisa, baseada em um estudo de caso na empresa Visma, inclui uma análise de 73 profissionais da área e 11 entrevistas, explorando como esses profissionais são recrutados, suas motivações e os desafios enfrentados (NGUYEN-DUC *et al*., 2024).

O estudo identifica diferenças entre *Security Champions* voluntários e designados, destacando que aqueles que assumem o papel voluntariamente demonstram maior engajamento e motivação. Além disso, aborda dificuldades no onboarding, comunicação e treinamentos, sugerindo formas de melhorar o suporte organizacional para esses profissionais (NGUYEN-DUC *et al*., 2024).

Os achados deste estudo reforçam a necessidade de estruturar programas de *Security Champions* com suporte contínuo, garantindo que esses profissionais tenham as ferramentas e o conhecimento necessários para desempenhar suas funções de forma eficaz. Os resultados fornecem insights valiosos para empresas que desejam implementar ou aprimorar programas de *Security Champions*, visando fortalecer a cultura de segurança no desenvolvimento de software (NGUYEN-DUC *et al*., 2024).

Por se tratar de um conceito relativamente recente, ainda há uma escassez de estudos aprofundados sobre o impacto dos *Security Champions* no

desenvolvimento seguro de software. Nesse sentido este artigo busca contribuir para o avanço do conhecimento na área, oferecendo uma base mais sólida para futuras pesquisas e aprimoramentos na implementação desse papel em diferentes contextos organizacionais (NGUYEN-DUC *et al*., 2024).

Este estudo tem como objetivo comparar os resultados da pesquisa *Towards an Effective Security*, 0que analisa os desafios enfrentados pelas organizações ao integrar a segurança desde as fases iniciais do desenvolvimento e propõe abordagens para superar barreiras culturais, organizacionais e técnicas. Enquanto o estudo original analisou o papel dos *Security Champions* dentro de uma única organização, esta pesquisa busca investigar essa função de forma mais abrangente, considerando profissionais que atuam como *Security Champions* em diferentes contextos considerando o cenário Brasileiro.

1.3 Objetivos

Este trabalho tem como objetivo analisar a atuação dos profissionais que desempenham o papel de *Security Champion* no contexto brasileiro, explorando suas percepções sobre responsabilidades, impacto na produtividade, influência na cultura organizacional e os desafios enfrentados na prática.

Como objetivos específicos, espera-se:

- Avaliar a importância do papel de *Security Champion* no fortalecimento da segurança no desenvolvimento de software.
- Identificar os principais desafios enfrentados por profissionais que desempenham essa função, considerando diferentes contextos organizacionais.
- Propor melhorias para a implementação e o desenvolvimento eficaz do *Security Champion* dentro das empresas.
- Comparar os resultados obtidos com os achados do estudo original *Towards an Effective Security Champions Program*.

1.4 Trabalhos relacionados

Nesta seção, são apresentados trabalhos que discutem a inserção da segurança no ciclo de desenvolvimento, abordagens ágeis para segurança e, especificamente, pesquisas que analisam a implementação e eficácia dos *Security Champions*. Além disso, são comparadas metodologias empregadas em estudos anteriores com a abordagem adotada neste trabalho, destacando lacunas existentes e contribuições potenciais da pesquisa.

O estudo base desta pesquisa é a tese *Towards an Effective Security Champions Program* (2022), de Aalvik, que propõe diretrizes e estratégias para estruturar um programa eficiente de *Security Champions* dentro das organizações. Essa abordagem foi posteriormente aplicada em um estudo de caso prático em uma grande empresa de tecnologia, resultando no artigo *Facilitating Security Champions*

in Software Projects – An Experience Report from Visma (2023), o qual relata a experiência de adoção do programa, destacando os desafios enfrentados, as lições aprendidas e os impactos observados na cultura de segurança.

A presente pesquisa se relaciona diretamente com essa linha de estudo ao analisar a atuação dos *Security Champions* em contextos organizacionais diversos, investigando os principais desafios, os benefícios percebidos e o impacto da função na cultura de segurança das empresas. Diferente do estudo de caso mencionado, que aborda uma única organização, esta pesquisa amplia a abordagem ao coletar dados de múltiplas empresas, oferecendo uma visão mais abrangente sobre o papel emergente desses profissionais na promoção da cibersegurança organizacional.

Um dos trabalhos relacionados é o *Security as Culture: A Systematic Literature Review of DevSecOps* (2020), que aborda o papel essencial de uma cultura de segurança no desenvolvimento de software. O estudo apresenta estratégias para disseminação dessa cultura, destacando os *Security Champions* como agentes-chave na propagação de boas práticas entre as equipes. Embora esse trabalho explore o conceito de *Security Champions*, ele não se aprofunda na análise de sua atuação prática, desafios enfrentados ou impacto organizacional. Já esta pesquisa busca preencher essa lacuna ao investigar a percepção dos profissionais que assumem esse papel, suas dificuldades e sua influência na cultura de segurança dentro das empresas, especialmente no contexto brasileiro.

O artigo *Challenges and Solutions When Adopting DevSecOps: A Systematic Review* (2022) realiza uma revisão sistemática da literatura sobre *DevSecOps*, explorando como a segurança é incorporada à cultura organizacional. Ele discute os desafios da adoção do *DevSecOps*, incluindo barreiras culturais, resistência à mudança e a necessidade de maior colaboração entre equipes de desenvolvimento, segurança e operações. Os principais achados indicam que a integração da segurança desde o início do ciclo de desenvolvimento melhora a postura de segurança das empresas e reduz custos e riscos a longo prazo. O estudo também destaca a importância da automação de segurança, do treinamento contínuo e do uso de métricas para avaliar a eficácia das práticas de *DevSecOps*, além de reconhecer o papel dos *Security Champions* como facilitadores dessa cultura. Diferente desse trabalho, que foca na implementação de *DevSecOps* de forma abrangente, esta pesquisa busca compreender especificamente o impacto dos

Security Champions, analisando sua influência na produtividade e nas dinâmicas organizacionais.

O artigo *Security Champions Without Support: Results from a Case Study with OWASP SAMM in a Large-Scale E-Commerce Enterprise* (2023) discute os desafios enfrentados pelos *Security Champions* quando não recebem o suporte necessário dentro das organizações. O estudo revela que, sem apoio institucional e sem diretrizes claras, esses profissionais encontram dificuldades para exercer suas funções de forma eficaz. *Security Champions* são descritos como desenvolvedores ou membros de equipe responsáveis por promover práticas de segurança dentro de suas áreas, funcionando como um elo entre a equipe de segurança e o restante da organização. Enquanto esse trabalho se concentra em um estudo de caso específico dentro de uma grande empresa de e-commerce, esta pesquisa adota uma abordagem mais ampla, analisando o papel dos *Security Champions* em diferentes organizações e setores. Além disso, busca entender quais são as principais barreiras para a adoção desse papel no contexto brasileiro, fornecendo um panorama mais abrangente sobre sua aplicação prática.

2 REVISÃO DE LITERATURA

2.1 Segurança Cibernética

O avanço contínuo da tecnologia impulsiona não apenas inovações positivas, mas também o surgimento de novas ameaças cibernéticas (HUSSAIN, 2020). Com o aumento constante do volume de dados e a conectividade global, as empresas se tornam mais expostas a ataques cibernéticos. Por isso, a segurança digital deixou de ser apenas uma necessidade técnica e passou a ser uma estratégia essencial para negócios de todos os setores (GOEL *et al*., 2015). Setores financeiros, governamentais e industriais, por exemplo, são alvos frequentes de ataques devido à criticidade dos dados envolvidos. Nesse contexto, crimes cibernéticos emergem como uma das ameaças mais aceleradas, exigindo medidas de segurança sofisticadas para mitigar seus impactos (HUSSAIN, 2020).

Nesse contexto, a cibersegurança torna-se essencial para garantir a integridade, confidencialidade e disponibilidade das informações. Ela pode ser definida como uma área de pesquisa e desenvolvimento ativo na comunidade de tecnologia da informação, envolvendo participantes de todas as partes do ecossistema de tecnologias da informação e comunicação (ATAKULOV, 2024).

Com o avanço das ameaças, as estratégias de defesa precisam ser continuamente aprimoradas para mitigar riscos e garantir a segurança digital (HUSSAIN, 2020). A evolução dos ataques cibernéticos exige não apenas ferramentas avançadas de proteção, mas também a adoção de processos, métodos e mentalidades que integrem a segurança em todas as operações empresariais (REEGARD *et al*., 2020).

Com a crescente sofisticação de ataques, como ransomware, ameaças persistentes avançadas e ataques que utilizam inteligência artificial e aprendizado de máquina, as empresas enfrentam desafios constantes para mitigar riscos e fortalecer suas defesas (OBAFEMI; NGEVAO, 2024). Diante desse cenário, medidas tradicionais de segurança, como firewalls e antivírus, tornam-se insuficientes caso não sejam continuamente aprimoradas para enfrentar ameaças emergentes (OBAFEMI; NGEVAO, 2024).

2.2 Métodos Ágeis e Cultura Organizacional

A adoção de uma cultura organizacional ágil voltada para a segurança cibernética acaba se tornando essencial para promover práticas proativas de defesa e conscientização (TASHTOUSH, 2021). Para isso, é fundamental compreender a importância da cultura organizacional na consolidação dessas práticas bem como a metodologia ágil pode contribuir nesse processo. A integração da segurança às metodologias ágeis não deve ser vista como um obstáculo ao desenvolvimento, mas sim como um fator que agrega valor ao processo, garantindo a entrega de produtos mais resilientes a ataques (BESSA; DIAS, 2018).

A metodologia ágil surge como uma abordagem voltada para otimizar o desenvolvimento de software, permitindo entregas incrementais e adaptáveis às necessidades do projeto (CAMPANELLI; PARREIRAS, 2015). Diferente do modelo em cascata, que segue um fluxo rígido e sequencial, os métodos ágeis priorizam interações curtas, feedback contínuo e colaboração entre equipes. Essa dinâmica possibilita a entrega de produtos em menor tempo, garantindo maior flexibilidade e capacidade de resposta a mudanças, sem comprometer a qualidade do software (HUO, 2004).

No contexto da segurança cibernética, essa abordagem permite que práticas de proteção sejam incorporadas continuamente ao ciclo de desenvolvimento, garantindo que vulnerabilidades sejam identificadas e corrigidas de forma mais ágil. Em vez de relegar a segurança para as etapas finais do projeto, como ocorre em abordagens tradicionais, os métodos ágeis possibilitam a integração de testes e revisões de segurança ao longo de todo o processo, reduzindo riscos sem impactar a produtividade (TASHTOUSH, 2021).

Além da adoção de metodologias ágeis, a implementação de uma cultura organizacional sólida é essencial para garantir que a segurança cibernética seja integrada à empresa e não apenas uma preocupação isolada (HUSSAIN, 2020). A cultura organizacional pode ser definida como um padrão de pressupostos básicos, desenvolvidos por um grupo à medida que ele aprende a lidar com problemas de adaptação externa e integração interna (SCHEIN, 1990).

A construção de uma cultura forte de segurança passa pelo engajamento de todos os colaboradores, desde a alta gestão até os desenvolvedores, incentivando boas práticas e a atualização constante sobre ameaças emergentes (AKPA;

ASIKHIA; NNEJI, 2021). Nesse contexto, o papel do *Security Champion* emerge como um facilitador dessa transformação.

A consolidação dessa cultura passa por treinamentos regulares, campanhas de conscientização e políticas claras sobre segurança da informação, além de incentivar uma mentalidade de segurança por design, em que a proteção de dados e sistemas é considerada em todas as etapas de desenvolvimento e operação (AKPA; ASIKHIA; NNEJI, 2021). A segurança organizacional depende, portanto, de um esforço contínuo para alinhar processos, tecnologias e pessoas, garantindo que as vulnerabilidades sejam tratadas de maneira eficiente e estratégica (HUSSAIN, 2020). Esse último aspecto é apontado como uma das principais fontes de risco de segurança de um sistema, de acordo com Shouki (2022).

Empresas que cultivam uma cultura organizacional voltada para a segurança tendem a reduzir significativamente o risco de ataques bem-sucedidos, pois os colaboradores se tornam mais alertas e preparados para identificar e reagir rapidamente a ameaças (SCHEIN, 1990).

2.3 Security Champion

Para fortalecer a cultura organizacional de adoção de boas práticas em cibersegurança, surge o papel do *Security Champion*. Esses profissionais atuam como agentes de mudança, promovendo a conscientização sobre ameaças cibernéticas e incentivando boas práticas de segurança dentro de suas equipes (MENGES, 2023).

Seja por escolha própria ou por indicação da organização, eles desempenham um papel essencial na identificação e mitigação de vulnerabilidades desde as fases iniciais dos projetos, garantindo um ambiente mais seguro ao longo do ciclo de desenvolvimento. Além disso, eles servem como pontos de referência para seus colegas, garantindo que as vulnerabilidades sejam identificadas e corrigidas desde as fases iniciais dos projetos, reduzindo riscos ao longo do ciclo de desenvolvimento (MENGES, 2023).

A presença desses profissionais nas organizações facilita a comunicação entre as equipes de desenvolvimento e segurança, promovendo um ambiente mais colaborativo e eficaz na mitigação de riscos. Isso não só fortalece a defesa preventiva contra ataques, mas também aumenta a eficiência operacional, pois as

equipes tornam-se mais auto suficientes na identificação e mitigação de riscos (MENGES, 2023).

4 METODOLOGIA

Foi utilizado o método de pesquisa por replicação do estudo de Aalvik *et al.* (2022) conforme classificação da Tabela 1.

Tabela 1 - Comparação do Design de Pesquisa entre o Estudo Original e o Estudo Replicado

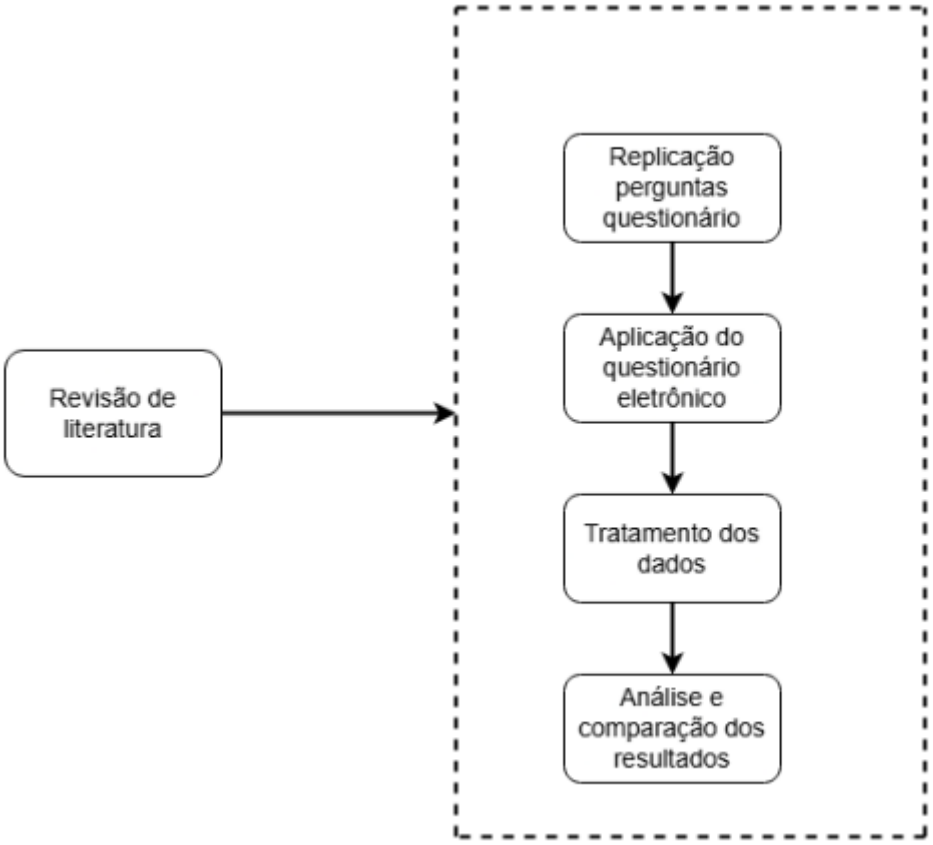
Elemento	**Estudo Original**	**Replicação Atual**	**Justificativa da Alteração**
Objetivo do Estudo	Entender como os *Security Champions* são recrutados e estabelecidos; Compreender como a Visma dá suporte aos que desempenham essa função.	Analisar a atuação dos profissionais que desempenham o papel de *Security Champion* no contexto brasileiro, explorando suas percepções sobre responsabilidades, impacto na produtividade, influência na cultura organizacional e os desafios enfrentados na prática.	Visando avaliar fatores que podem vir a contribuir na atuação do papel de *Security Champion* como um todo.
Participantes	71 Participantes	29 Participantes	Devido à dificuldade de encontrar profissionais atuantes na área de segurança e à limitação de tempo, encerramos o questionário com 29 submissões, embora a expectativa fosse de 30.
Metodologia	Revisão de literatura; Questionário eletrônico; Entrevista	Revisão de literatura; Questionário eletrônico	As perguntas da entrevista foram incorporadas com as do questionário eletrônico
Instrumentos de Coleta	Google Forms	Google Forms	

Fonte: O autor, (2025).

4.1 Etapas do trabalho

A Figura 1 apresenta o diagrama do fluxo do caso de estudo, detalhando as principais etapas da pesquisa.

Figura 1 - Diagrama do fluxo do trabalho



Fonte: O autor, (2025).

4.1.1 Revisão de Literatura

A revisão de literatura desta pesquisa foi fundamental para embasar o estudo sobre o papel dos *Security Champions* no desenvolvimento de software. Foram analisados trabalhos relevantes na área, incluindo *Towards an Effective Security Champions Program* (Aalvik, 2022) e *Facilitating Security Champions in Software Projects - An Experience Report from Visma* (Nguyen-Duc *et al.*, 2023). Esses estudos forneceram um panorama sobre os desafios, benefícios e estratégias para a implementação de *Security Champions*, permitindo uma base teórica sólida para a pesquisa.

4.1.2 Replicação e aplicação das perguntas do questionário

Para garantir a replicação metodológica, parte do questionário foi baseada no estudo de Aalvik (2022), permitindo que os achados desta pesquisa pudessem ser comparados com investigações anteriores. As perguntas abordaram aspectos como responsabilidades dos *Security Champions*, desafios enfrentados e impacto organizacional, assegurando uma continuidade nas investigações sobre o tema. Considerando que o termo *Security Champion* ainda não é amplamente disseminado nas empresas brasileiras, o questionário eletrônico foi direcionado a profissionais que atuam em atividades relacionadas à segurança da informação e que, mesmo sem o título formal, desempenham funções alinhadas às atribuições de um *Security Champion*. Para garantir o entendimento dos participantes, foi incluída no início da pesquisa uma explicação com caráter informativo sobre o conceito e o papel desses profissionais.

4.1.3 Tratamento dos dados

Os dados obtidos foram organizados e tratados no Google Sheets. O questionário continha perguntas objetivas e subjetivas destinadas a analisar a percepção dos participantes sobre o papel de *Security Champion*, garantindo a relevância das questões e a replicação metodológica de estudos anteriores. As perguntas aplicadas no questionário estão disponíveis na Tabela do Apêndice A.

4.1.4 Análise e comparação dos resultados

Por fim, a análise e comparação dos resultados foram conduzidas com base nos achados dos estudos anteriores, buscando verificar similaridades e divergências entre as pesquisas. Essa abordagem possibilitou avaliar como as experiências dos profissionais entrevistados nesta pesquisa se alinham ou diferem das observações feitas em contextos distintos, contribuindo para um entendimento mais amplo sobre a implementação dos Security Champions no desenvolvimento de software.

5 RESULTADOS E DISCUSSÃO

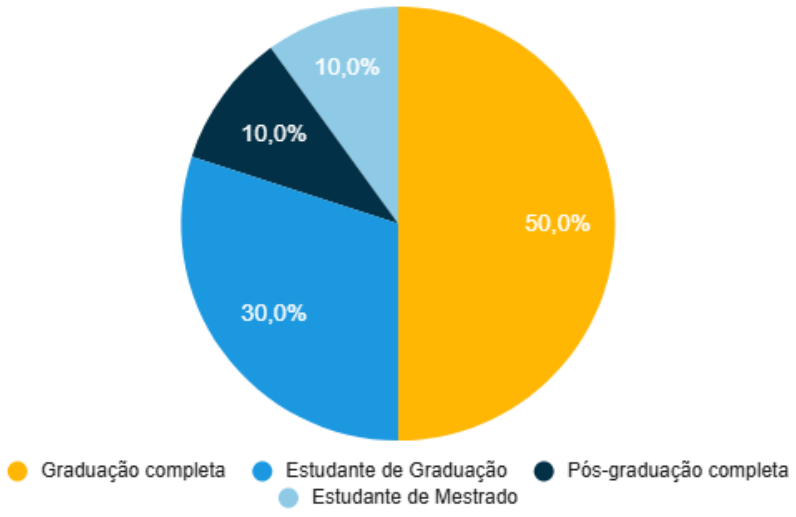
5.1 Estudo Comparativo: Resultados do Original e da Replicação

Esta seção apresenta os resultados obtidos a partir do questionário eletrônico que foi aplicado aos participantes. Os dados são discutidos e comparados com o estudo prévio de Aalvik *et al.* (2023).

5.1.1 Perfil dos participantes

O Gráfico 1 apresenta o nível de formação dos participantes desta pesquisa, observa-se que a metade destes (50%) possui graduação completa, seguido por 30% que ainda são estudantes de graduação. Esses resultados destacam a importância do conhecimento técnico na atuação dos *Security Champions*, sugerindo uma correlação entre áreas específicas de especialização e o desempenho nessa função.

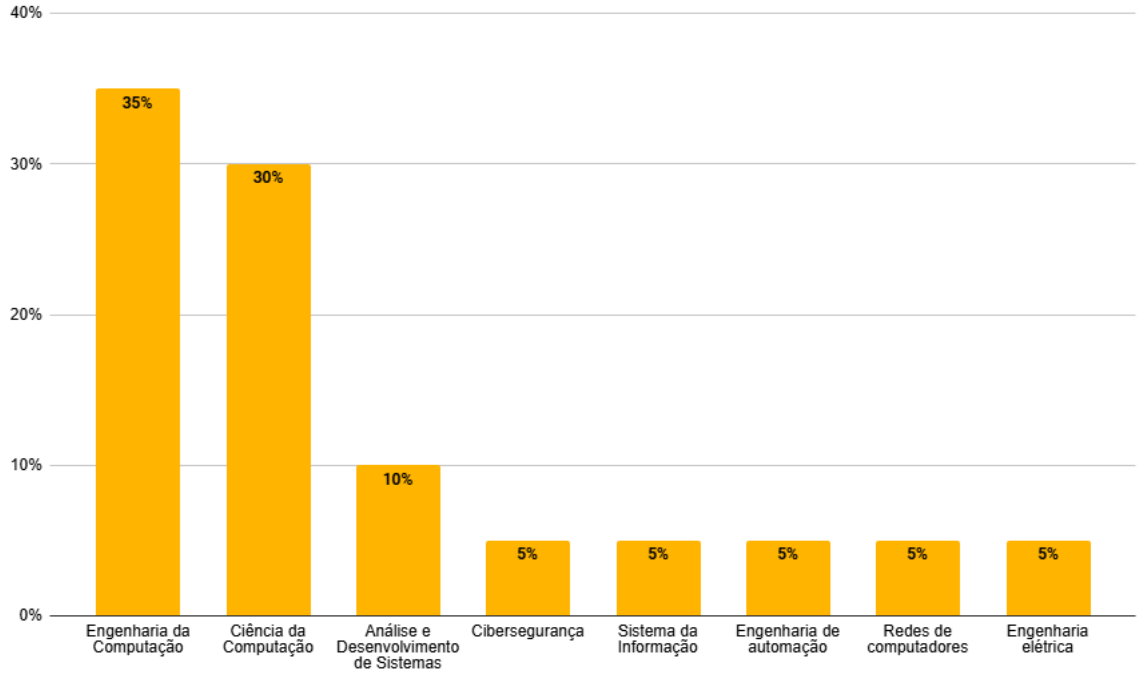
Gráfico 1 - Nível de formação



Fonte: O autor, (2025).

Ainda sobre o perfil dos participantes da pesquisa, observa-se que a maioria possui formação acadêmica na área de tecnologia, com destaque para os cursos de Engenharia da Computação e Ciência da Computação, como observado no Gráfico 2, que juntos representam 65% dos respondentes.

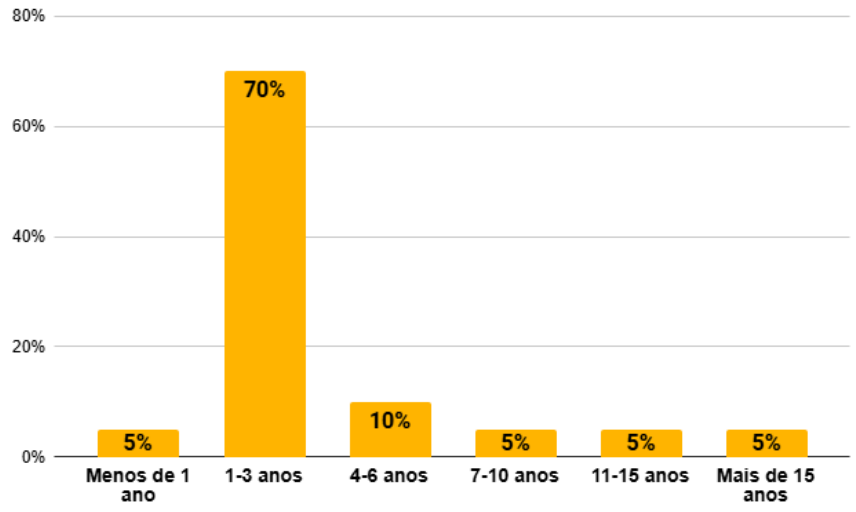
Gráfico 2 - Curso de graduação



Fonte: O autor, (2025).

O Gráfico 3 indica que a maioria dos profissionais deste estudo possui entre 1 e 3 anos de experiência em atuações relacionadas à cibersegurança, reforçando a ideia de que o papel de *Security Champion* é relativamente recente e tem se difundido mais amplamente apenas nos últimos anos.

Gráfico 3 - Tempo de atuação com segurança

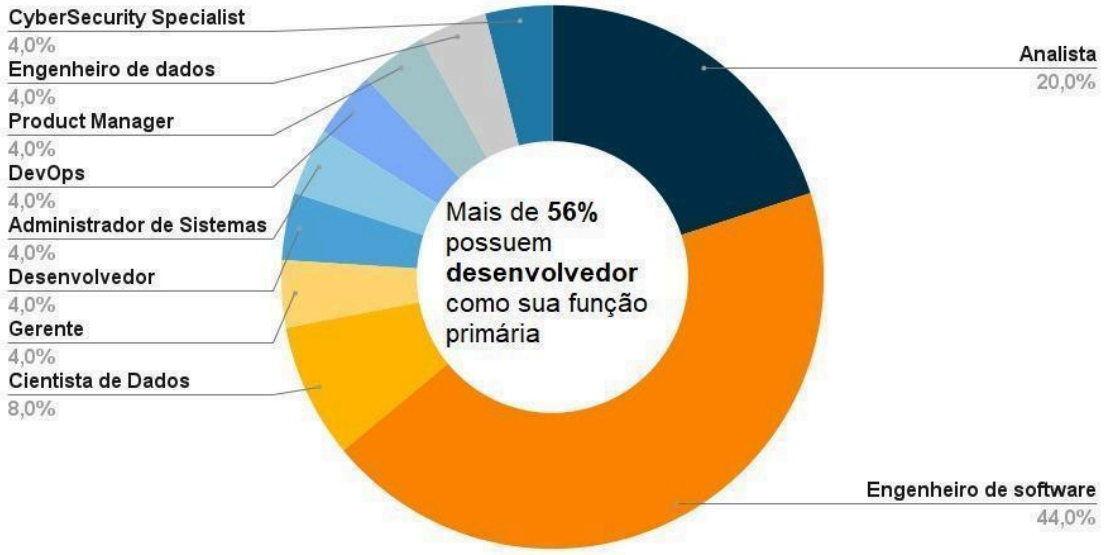


Fonte: O autor, (2025).

5.1.2 Nomeação e Designação dos Security Champions

Conforme ilustrado no Gráfico 4, a função mais comum entre os profissionais que atuam como *Security Champion* é a de desenvolvedor, representando mais de 56% dos participantes desta pesquisa. É possível ver uma correlação entre desenvolvedores e *Security Champions*, o que sugere que as empresas estão priorizando a segurança dentro das próprias equipes de desenvolvimento.

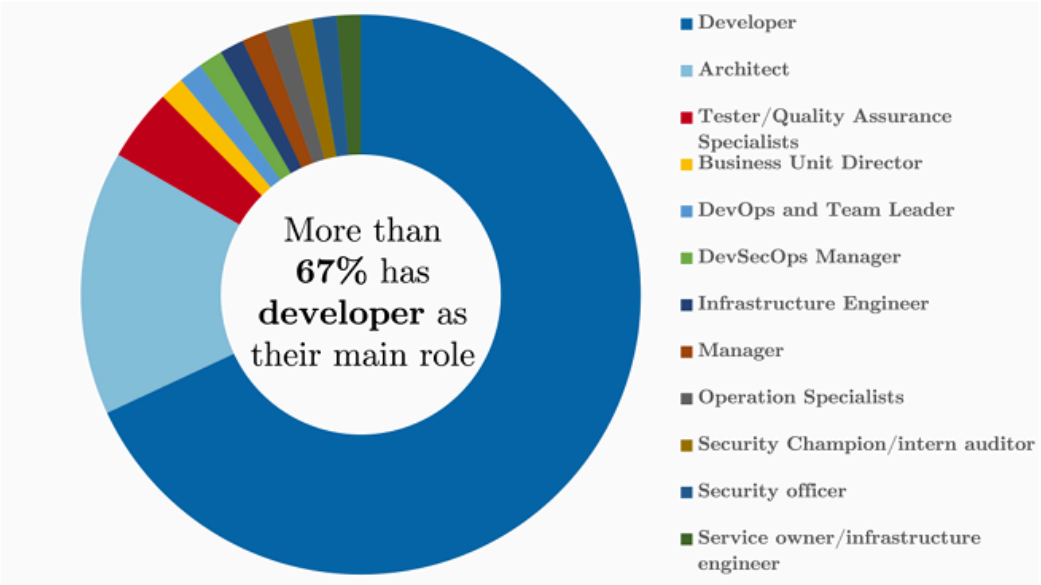
Gráfico 4 - Função primária dos participantes



Fonte: O autor, (2025).

Essa tendência também é observada no estudo original, conforme evidenciado na Figura 2, em que mais de 67% dos Security Champions entrevistados também atuavam como desenvolvedores. A semelhança entre os resultados reforça a associação entre o papel de *Security Champion* e profissionais da área de desenvolvimento, destacando que, em diferentes contextos organizacionais, a escolha por esse perfil técnico tem sido uma prática recorrente.

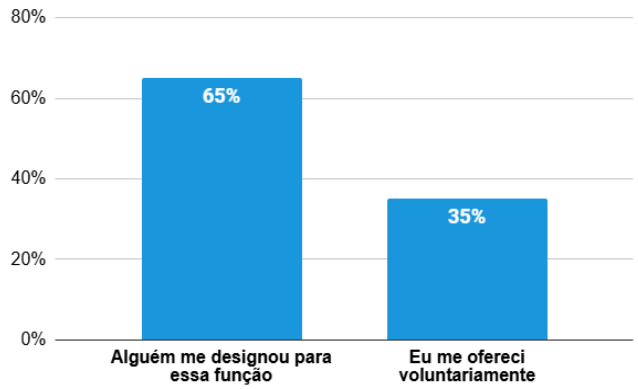
Figura 2 - Função primária dos participantes



Fonte: Aalvik (2022).

Observa-se no Gráfico 5 que, nesta pesquisa, a maioria dos participantes foi designada para atuar como Security Champion. Isso pode indicar que as empresas estão reconhecendo a necessidade formal de incorporar *Security Champions* às suas equipes, em vez de depender apenas do interesse individual dos colaboradores.

Gráfico 5 - Designação laboral

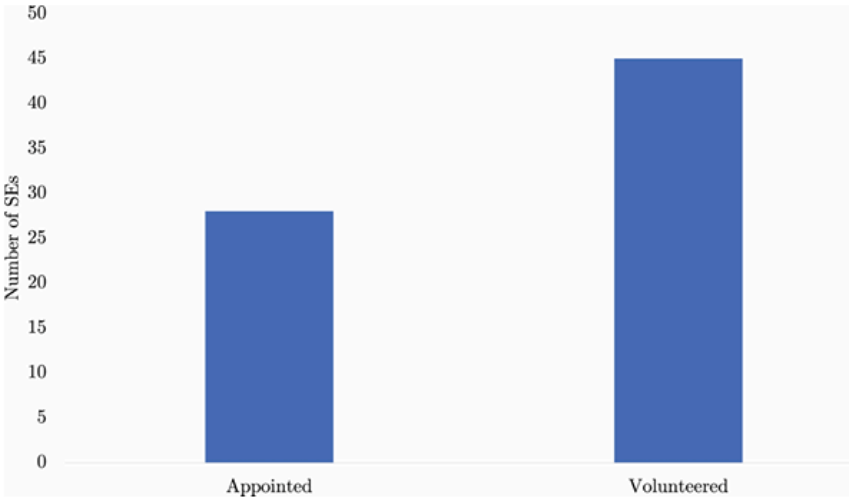


Fonte: O autor, (2025).

Em contraste, a Figura 3 do estudo original mostra que a maioria dos participantes se voluntariaram para exercer a função de *Security Champion*. Isso

indica que, naquele contexto, o engajamento partiu mais da motivação pessoal dos profissionais do que de uma estratégia organizacional formal. A comparação entre os dois estudos evidencia uma possível mudança de abordagem, com as empresas passando a estruturar e definir de forma mais clara esse papel em suas equipes.

Figura 3 - Número de participantes voluntariados e designados

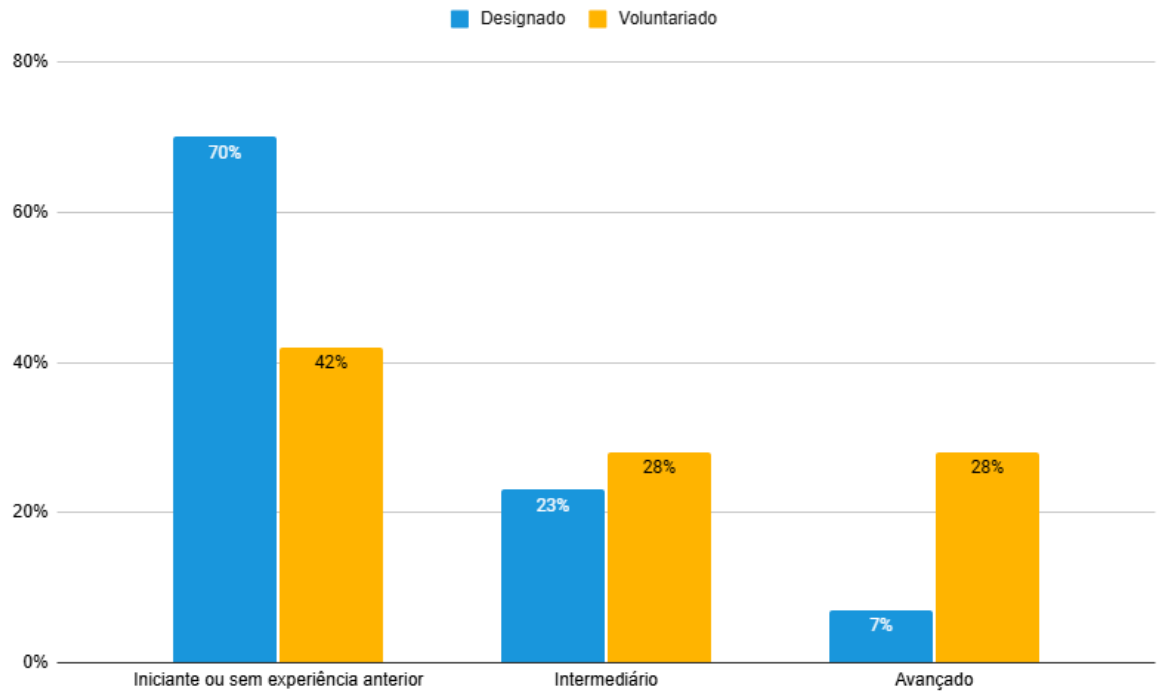


Fonte: Aalvik (2022).

5.1.3 Experiência e Clareza das Expectativas

O Gráfico 6 apresenta o nível de conhecimento em segurança dos participantes da pesquisa. Os dados mostram que muitos profissionais iniciam suas atividades com pouca ou nenhuma experiência prévia na área, sendo essa a realidade para 70% dos designados e 42% dos voluntários. Isso indica que o setor depende fortemente de aprendizado prático e treinamento no trabalho. Além disso, a diferença entre os designados (70%) e os voluntários (42%) sugere que aqueles que entram na área por imposição (designados) tendem a ter menos experiência inicial do que aqueles que escolhem atuar voluntariamente, possivelmente porque os voluntários já possuem algum interesse ou preparo prévio. Isso reforça a importância de programas de capacitação para garantir a qualificação dos profissionais de segurança.

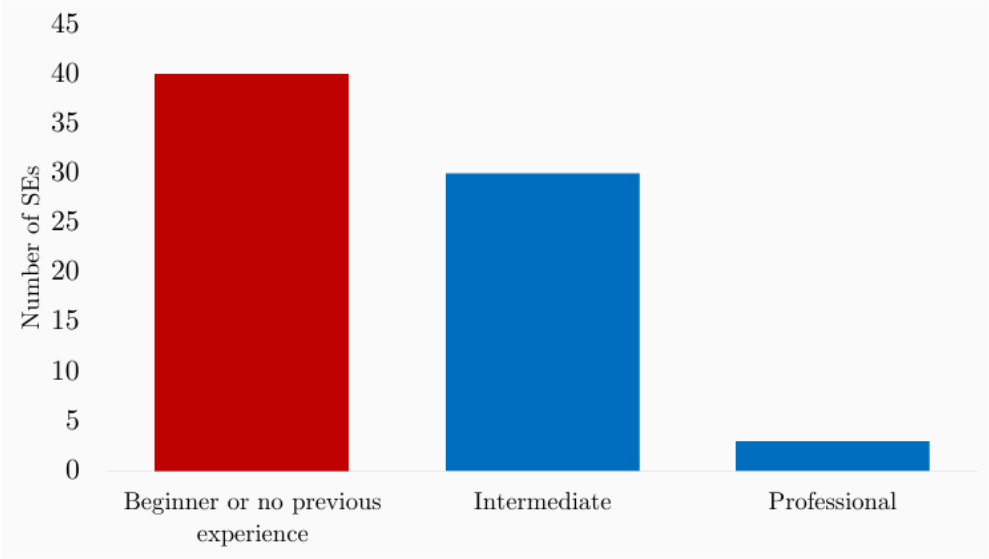
Gráfico 6 - Nível de Competência em segurança antes de assumir a função



Fonte: O autor, (2025).

De forma semelhante, a Figura 4 do estudo original de Aalvik *et al.* (2023) também demonstra que muitos Security Champions começaram com pouco ou nenhum conhecimento prévio em segurança. Embora o estudo original não distinga os grupos entre voluntários e designados, os dados corroboram a constatação de que o ingresso na função geralmente ocorre com uma base limitada, o que destaca a relevância de ações estruturadas de onboarding e capacitação. A comparação entre os dois estudos evidencia um padrão comum e a necessidade recorrente de preparar melhor os profissionais desde o início de sua atuação em segurança.

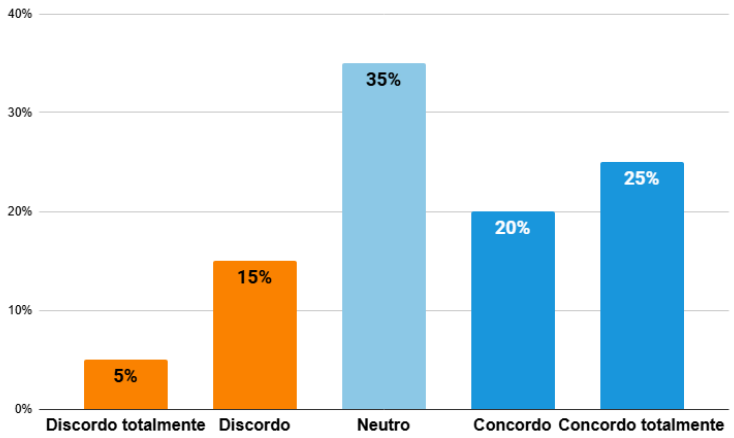
Figura 4 - Nível de Competência em segurança antes de assumir a função



Fonte: Aalvik (2022).

Quando os participantes desta pesquisa foram questionados sobre a clareza das expectativas antes de assumirem a função de *Security Champion*, os dados do Gráfico 7 indicam que 45% consideram ter recebido uma visão clara, enquanto 20% discordam e 35% permaneceram neutros. Esses números revelam que, embora uma parte significativa tenha se sentido orientada, ainda há uma parcela relevante de profissionais que ingressam na função sem um entendimento pleno das suas responsabilidades, demonstrando a necessidade de um melhor alinhamento comunicacional por parte das organizações ao designar alguém para esse papel.

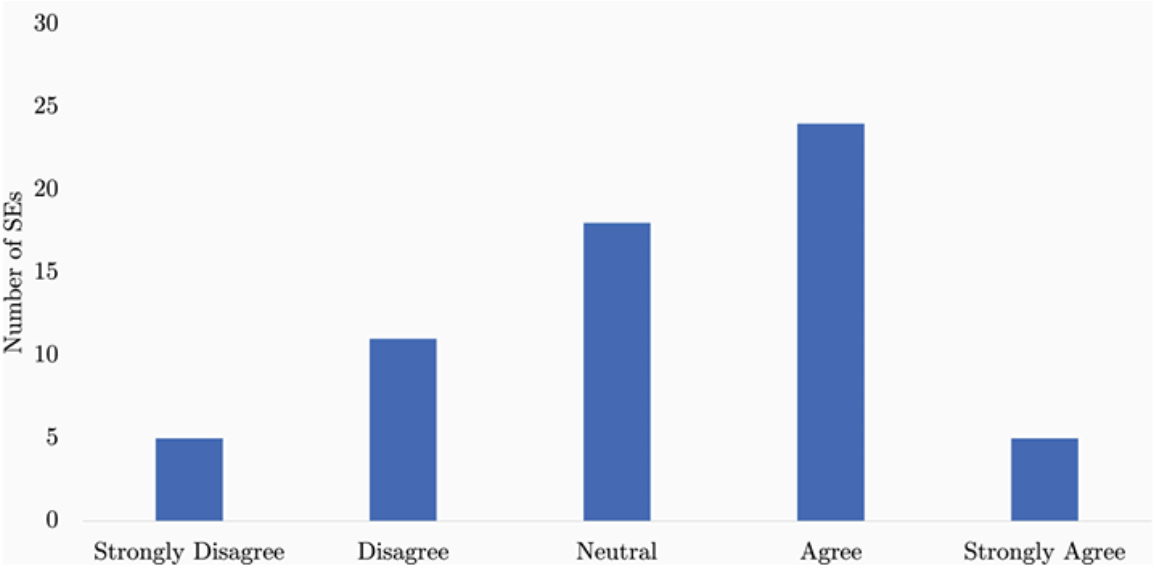
Gráfico 7 - Visão clara das expectativas antes de assumir a função



Fonte: O autor, (2025).

De forma semelhante, a Figura 5, oriunda do estudo de Aalvik (2022), também aponta que muitos dos participantes relataram ter uma visão clara das expectativas antes de iniciarem suas atividades como *Security Champions*. No entanto, apesar do tom mais positivo, o estudo original não detalha os percentuais de discordância ou neutralidade, dificultando uma comparação mais precisa. Ainda assim, os dois estudos convergem ao indicar que a clareza nas responsabilidades é um aspecto essencial, embora ainda não plenamente resolvido, o que reforça a importância de processos de onboarding mais estruturados e comunicativos.

Figura 5 - Visão clara das expectativas antes de assumir a função



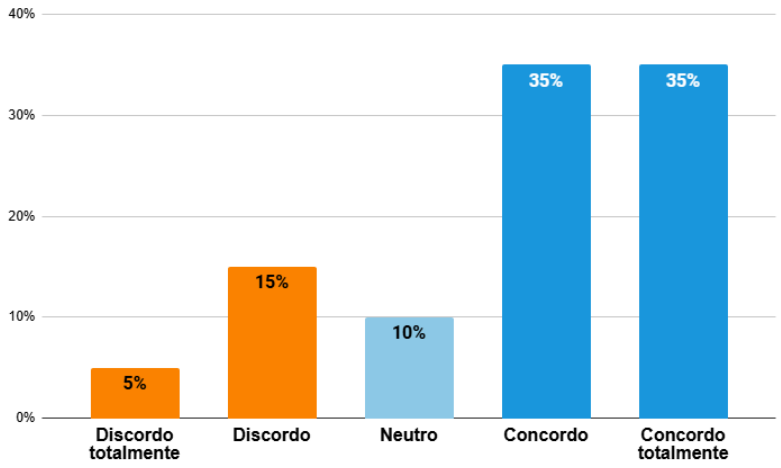
Fonte: Aalvik (2022).

5.1.4 Conflitos com Outras Funções e Alocação de Tempo

Além das responsabilidades técnicas e organizacionais, é importante compreender como a atuação como *Security Champion* se articula com as demais funções exercidas pelos profissionais. Um dos pontos investigados nesta pesquisa foi justamente se há sobreposição ou conflito entre essas atividades.

Quando questionados sobre possíveis conflitos entre a atuação como *Security Champion* e outras funções, como apresentado no Gráfico 8, 70% dos participantes desta pesquisa afirmaram não enfrentar dificuldades nesse sentido. Sugerindo que as e os profissionais têm conseguido estruturar e atuar nessa função de forma equilibrada dentro das atividades diárias.

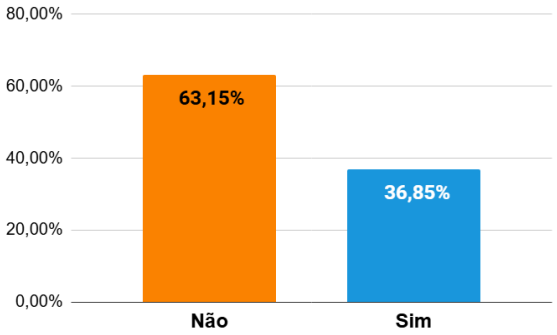
Gráfico 8 - Não tenho conflitos entre este papel e outras funções que desempenho



Fonte: O autor, (2025).

O Gráfico 9 indica que 63,15% dos profissionais não possuem horas pré-alocadas para tarefas de segurança. Como observado anteriormente, por não enfrentarem conflitos com suas outras funções, isso sugere que não há sobrecarga em relação às demandas. Dessa forma, os profissionais conseguem gerenciar seu próprio tempo para conciliar as atividades de segurança com suas demais responsabilidades.

Gráfico 9 - Profissionais que possuem horas pré-alocadas

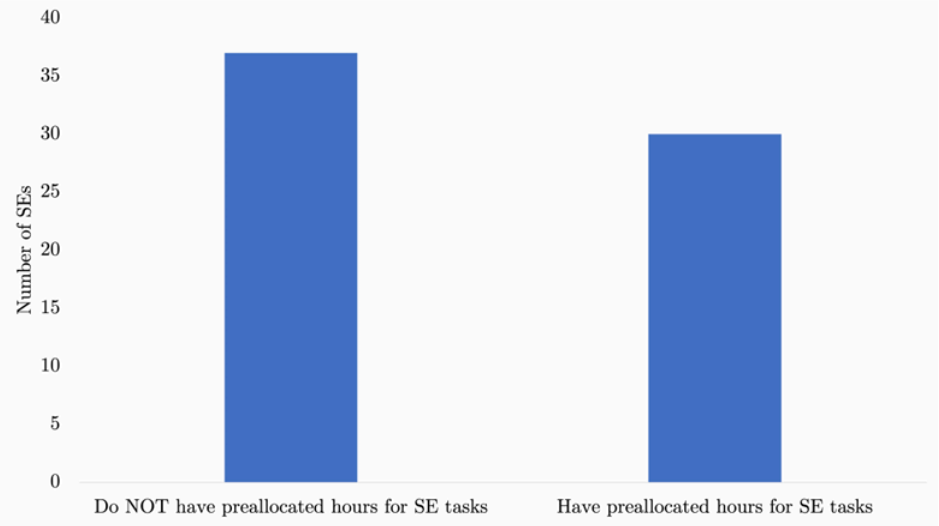


Fonte: O autor, (2025).

De forma semelhante, a Figura 6, referente ao estudo original de Aalvik (2022), mostra que mais da metade dos profissionais também não possuíam horas pré-alocadas para atividades de segurança. Esse dado reforça a tendência observada de que a atuação como *Security Champion*, embora importante, ainda é

frequentemente exercida de maneira informal, exigindo dos profissionais autonomia no gerenciamento de tempo, mas também apontando para a necessidade de uma estrutura mais consolidada para a função.

Figura 6 - Profissionais que possuem horas pré-alocadas

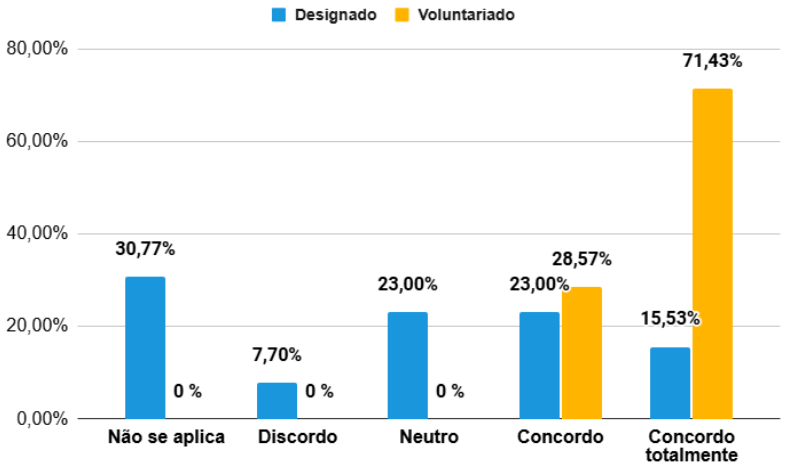


Fonte: Aalvik (2022).

5.1.5 Motivação para Atuar na Função

No Gráfico 10 é possível observar que 100% dos participantes desta pesquisa que se voluntariaram para atuarem como *Security Champion* afirmaram estarem motivados para desempenhar suas funções de segurança. Enquanto apenas 38,53% dos que foram designados afirmaram estar motivados.

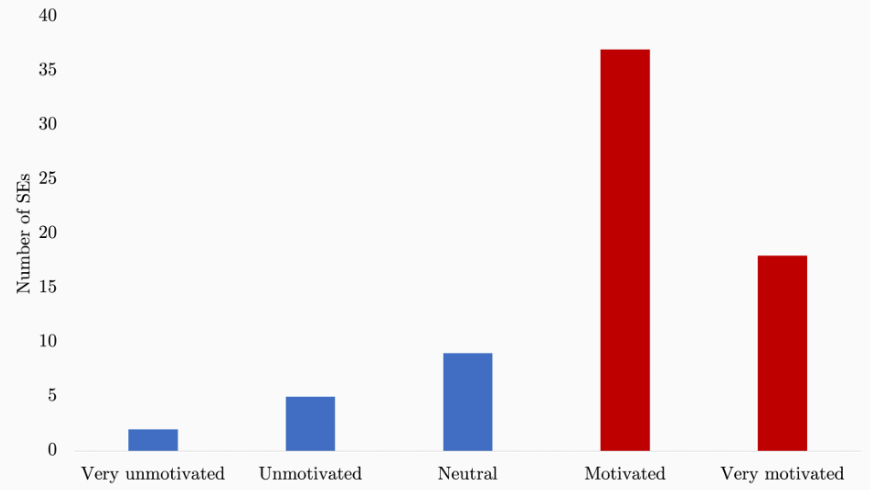
Gráfico 10 - Motivação com a função



Fonte: O autor, (2025).

Esse achado se alinha ao observado na Figura 7, do estudo original de Aalvik (2022), em que a maioria dos participantes também se declarou motivada para exercer o papel de *Security Champion*. No entanto, o estudo original não detalha a motivação por tipo de nomeação, o que torna os resultados desta pesquisa relevantes por evidenciar que o fator "voluntariedade" pode ter impacto direto no engajamento e satisfação com a função.

Figura 7 - Motivação com a função



Fonte: Aalvik (2022).

5.1.6 Treinamento e Onboarding

Quando questionados em relação ao suporte e satisfação, descritos no Gráfico 11, 90% dos entrevistados afirmam que as ferramentas e os canais de suporte, adotados por suas empresas, são eficazes em suas atuações. Reforçando a importância de um canal aberto de suporte e comunicação.

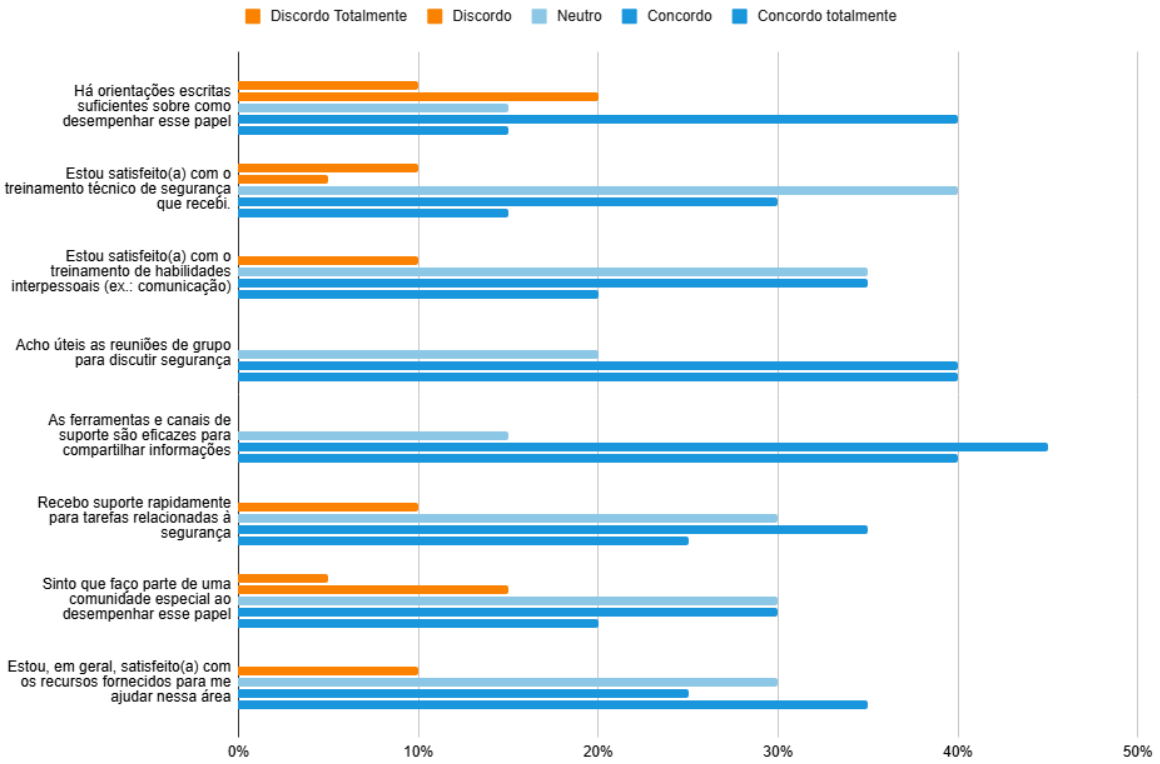
Em relação ao treinamento técnico, 45% dos participantes afirmaram ter recebido uma boa capacitação, o que pode indicar uma necessidade de melhores treinamentos e capacitações para atuações de segurança.

No que diz respeito ao sentimento de pertencimento, 52,58% dos entrevistados afirmaram sentir-se parte de uma comunidade especial ao desempenhar suas funções, evidenciando um nível considerável de engajamento. No entanto, 21,1% expressaram discordância, enquanto 26,32% permaneceram neutros, indicando que há espaço para melhorias na promoção de um ambiente mais acolhedor.

Sobre as habilidades interpessoais, 55% dos participantes desta pesquisa afirmaram estar satisfeitos com o treinamento recebido nessa área.

Por fim, quando questionados sobre a satisfação geral com os recursos fornecidos para auxiliá-los no desempenho de suas funções, 61,11% dos participantes manifestaram contentamento, enquanto 27,78% permaneceram neutros e 11,11% demonstraram insatisfação.

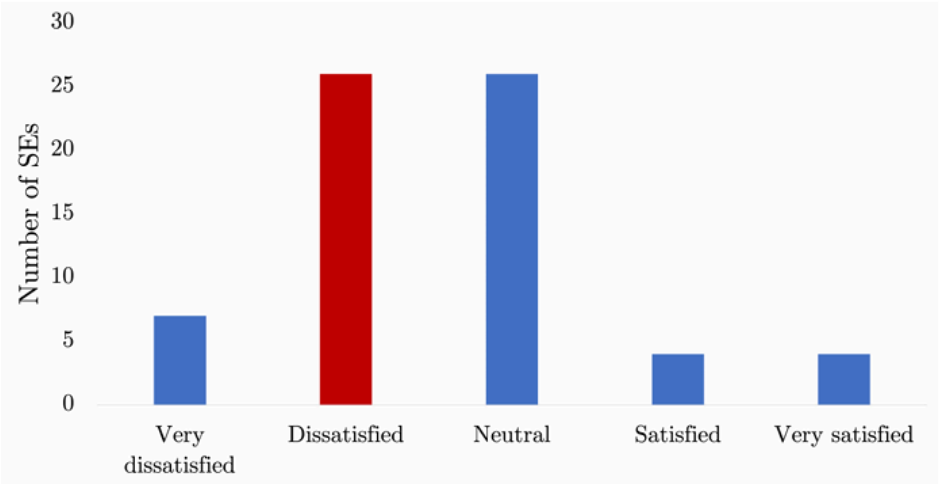
Gráfico 11 - Satisfação dos participantes sobre suporte, recursos e treinamentos



Fonte: O autor, (2025).

Esses achados dialogam com os dados apresentados na Figura 8 do estudo original de Aalvik (2022), onde a maior parte dos participantes também relatou insatisfação com o treinamento técnico recebido. Isso reforça uma tendência observada em ambos os estudos: embora os *Security Champions* reconheçam a relevância do suporte e recursos disponíveis, a efetividade dos treinamentos técnicos ainda se mostra um ponto crítico a ser aprimorado para garantir uma atuação mais eficaz e segura.

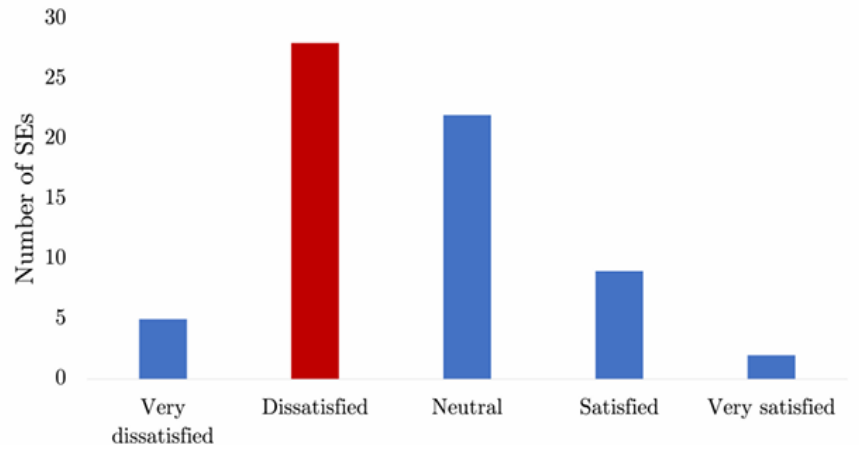
Figura 8 - Satisfação com o treinamento de segurança



Fonte: Aalvik (2022).

Seguindo com as comparações deste trabalho com o estudo original, grande parte dos participantes, ao serem questionados sobre seu nível de satisfação com o treinamento de *soft skills* demonstraram neutralidade ou discordância, conforme pode ser observado na Figura 9. Esse aspecto pode indicar uma oportunidade de melhoria, considerando que uma das atribuições de um *Security Champio*n é transmitir conhecimento.

Figura 9 - Satisfação com o treinamento de soft skills

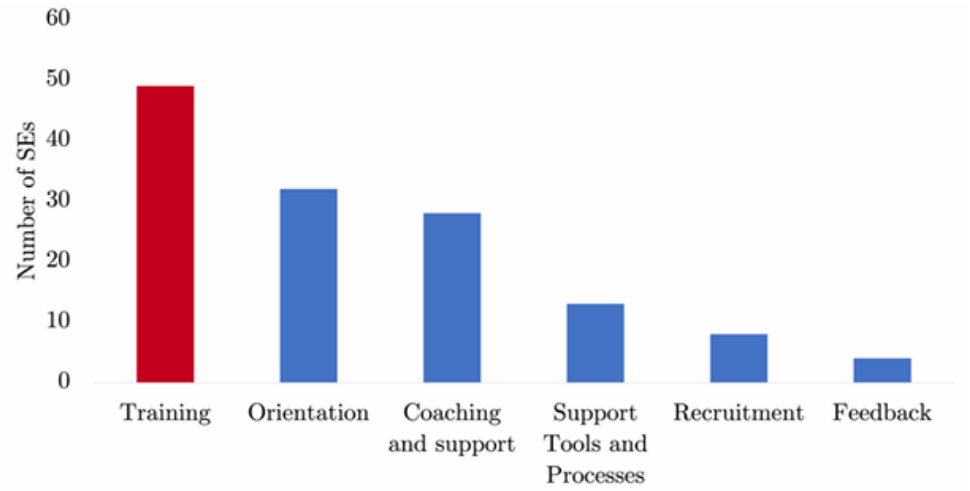


Fonte: Aalvik (2022).

Na Figura 10, observa-se que o treinamento e a orientação inicial foram os aspectos mais votados pelos participantes para aperfeiçoamento, seguidos por coaching e suporte contínuo, recrutamento e feedback, respectivamente. Isso

demonstra que os profissionais têm uma preocupação com a estruturação e o suporte inicial da função.

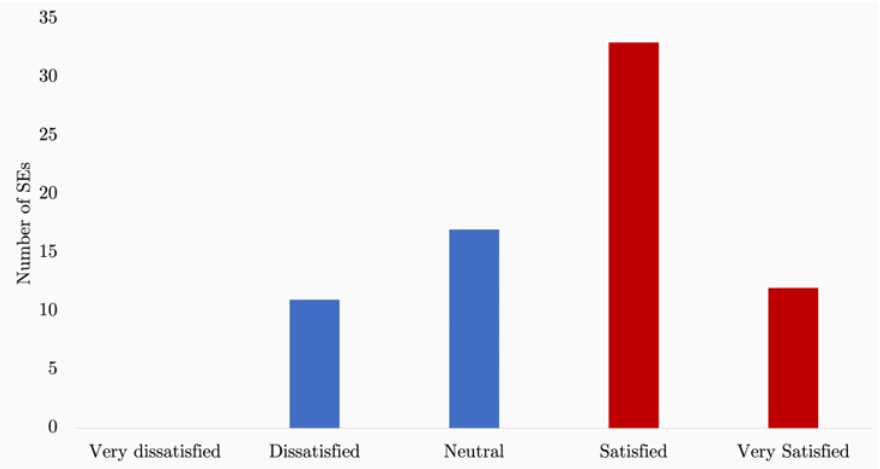
Figura 10 - Partes do onboarding que precisam de melhorias



Fonte: Aalvik (2022).

Quando questionados sobre a satisfação geral com os recursos fornecidos para auxiliá-los no desempenho de suas funções, a maioria de seus participantes manifestaram contentamento, como pode ser visualizado na Figura 11. Indicando que possuem ferramentas e meios para exercerem suas funções adequadamente.

Figura 11 - Nível de satisfação com os recursos fornecidos

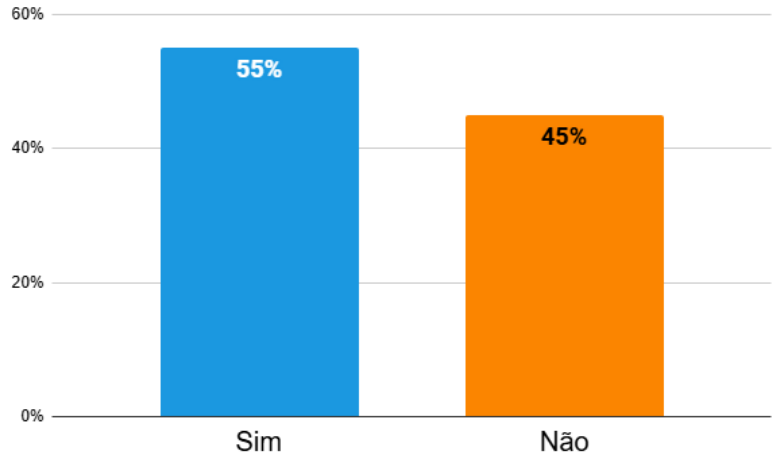


Fonte: Aalvik (2022).

O Gráfico 12 demonstra que, embora a maioria dos participantes (55%) tenha indicado que teve um mentor no início de suas carreiras, 45% afirmaram não ter recebido essa orientação. Esse dado sugere uma falta de suporte e direcionamento

nas atribuições de segurança, o que pode impactar negativamente a curva de aprendizado dos profissionais que estão iniciando na área.

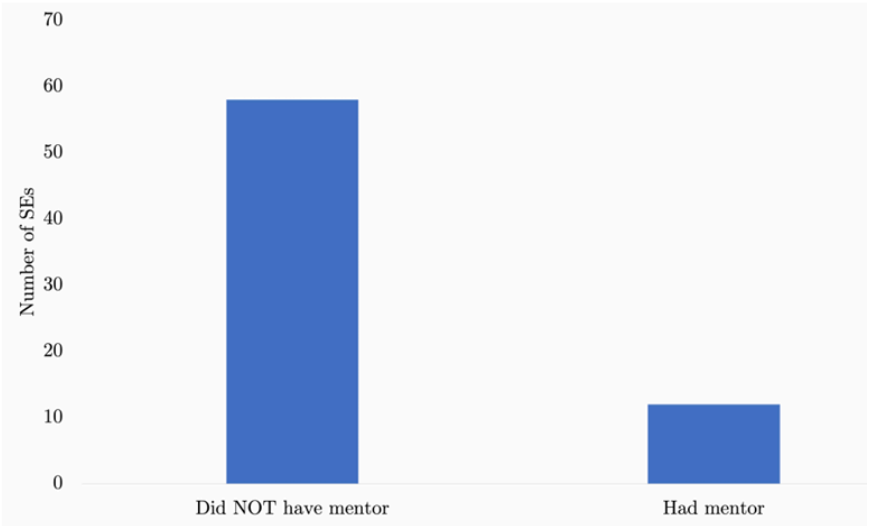
Gráfico 12 - Profissionais que tiveram um mentor



Fonte: O autor, (2025).

Esse achado dialoga com os resultados da Figura 12, do estudo original de Aalvik (2022), onde a maioria dos participantes relatou não ter tido um mentor em sua trajetória. A semelhança entre os estudos reforça que a ausência de orientação inicial é uma lacuna recorrente em diferentes contextos organizacionais, indicando a necessidade de estruturar programas de mentoria como parte integrante do processo de *onboarding* dos *Security Champions*.

Figura 12 - Profissionais que tiveram um mentor



Fonte: Aalvik (2022).

5.1.7 Suporte e Feedback

O Gráfico 13 retrata a percepção dos participantes desta pesquisa sobre diferentes aspectos do retorno que recebem ao exercer o papel de Security Champion. Mais de 75% dos participantes afirmaram que recebem feedback sobre suas atuações e estão satisfeitos com a quantidade de retornos recebidos, o que reflete um cenário positivo de comunicação e acompanhamento.

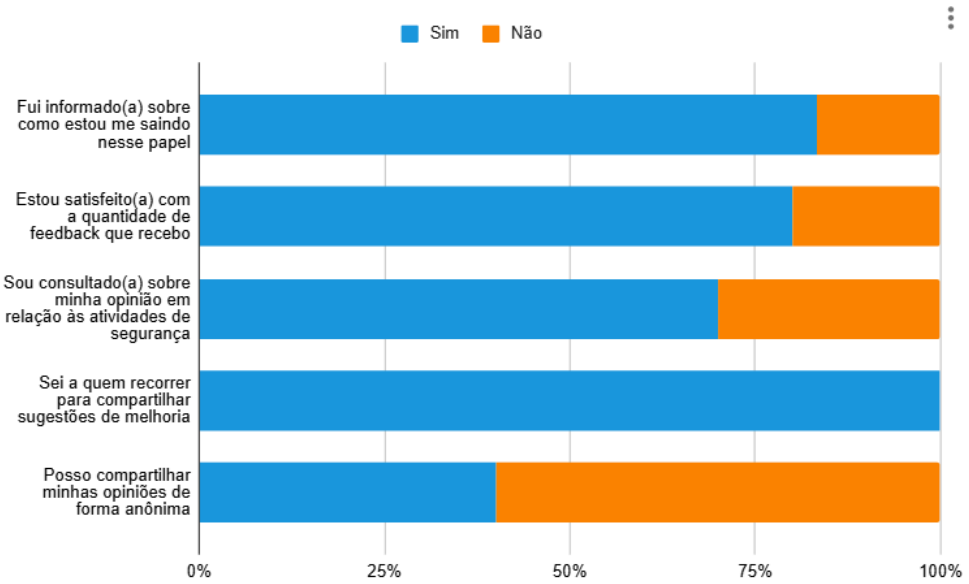
No entanto, ao analisarmos a consulta de opiniões, pouco mais da metade declarou ser consultada sobre atividades de segurança, o que indica uma atuação ativa, mas com espaço para ampliação da escuta e inclusão nas decisões. A esse respeito, os dados mostram uma tendência semelhante à observada no estudo original (Figura 13), em que parte dos participantes também relatou não se sentir plenamente ouvida, evidenciando que esse é um ponto a ser aprimorado em diferentes contextos.

Outro ponto abordado no gráfico diz respeito ao conhecimento sobre a quem recorrer para sugestões de melhoria, no qual os participantes foram unânimes ao afirmar que sabem como e com quem se comunicar. Esse achado reforça a clareza dos canais de suporte, em consonância com os resultados de Aalvik (2022), onde a maioria também declarou ter clareza sobre os canais disponíveis para feedback.

Já quanto à possibilidade de compartilhar opiniões de forma anônima, os dados da presente pesquisa revelam que mais de 50% dos participantes relataram não possuir essa possibilidade, o que também foi identificado no estudo original, onde menos da metade dos respondentes afirmou poder emitir feedbacks anonimamente. Ambos os resultados sugerem uma limitação importante na criação de um ambiente seguro para críticas construtivas, que pode afetar a transparência e a sinceridade dos retornos.

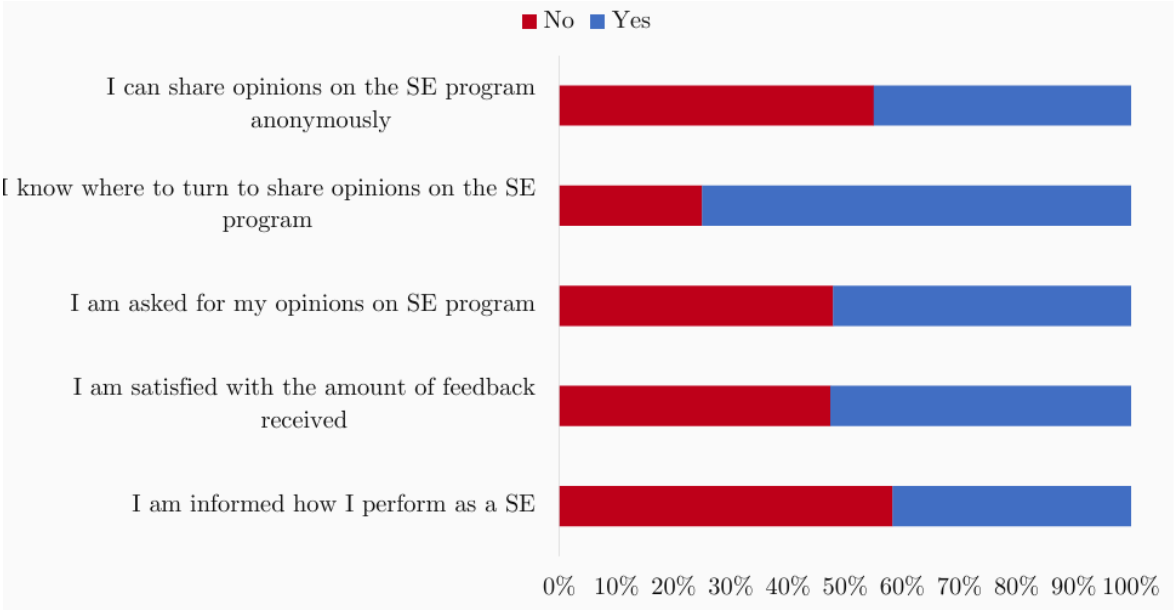
Por fim, a pesquisa de Aalvik destacou que apenas metade dos participantes se sentia devidamente informada sobre seu desempenho como *Security Champion*. Embora os dados da presente pesquisa apontem uma taxa maior de feedbacks e satisfação, essa lacuna de reconhecimento individual ainda pode estar presente de forma mais sutil, reforçando a necessidade de melhorar a estrutura de retorno e valorização desses profissionais.

Gráfico 13 - Feedbacks



Fonte: O autor, (2025).

Figura 13 - Feedbacks

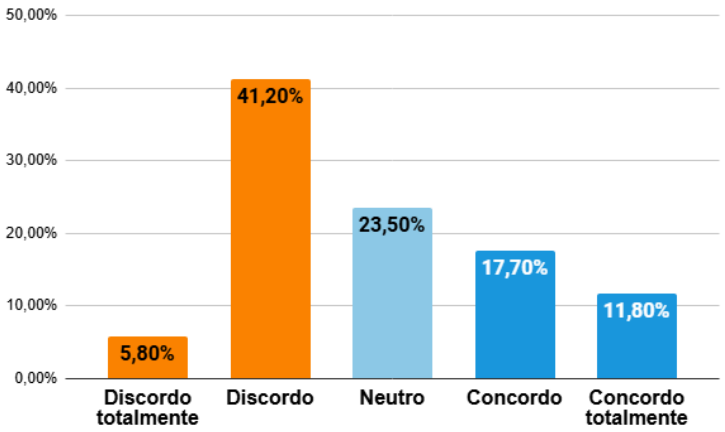


Fonte: Aalvik (2022).

5.1.8 Sentimentos de Pertencimento e Engajamento

Embora a maioria dos participantes (55%) afirme ter uma noção geral sobre suas atribuições na área de segurança, os dados do Gráfico 14 indicam que o processo de onboarding ainda é deficiente, oferecendo pouca orientação para essas atividades.

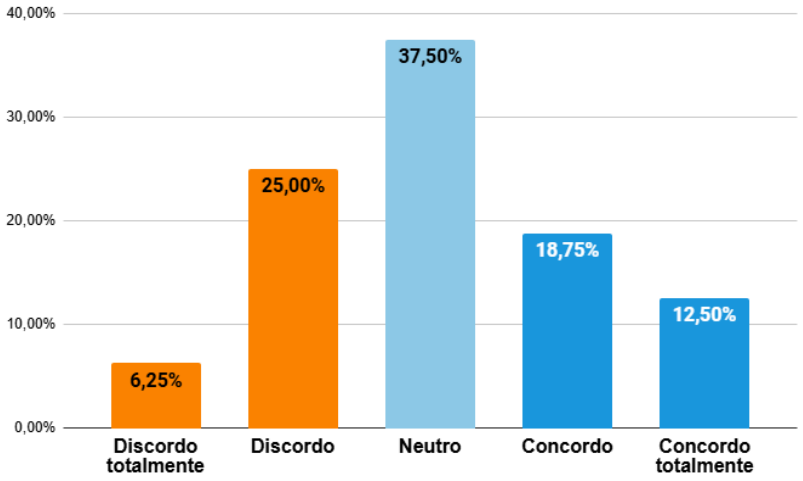
Gráfico 14 - Existe um processo claro de *onboarding* para quem começa a atuar com segurança



Fonte: O autor, (2025).

Essa limitação é reforçada pelo Gráfico 15, que mostra que apenas 31,25% dos participantes consideram o onboarding útil para seu desempenho, enquanto 68,75% expressam neutralidade ou discordam dessa afirmação.

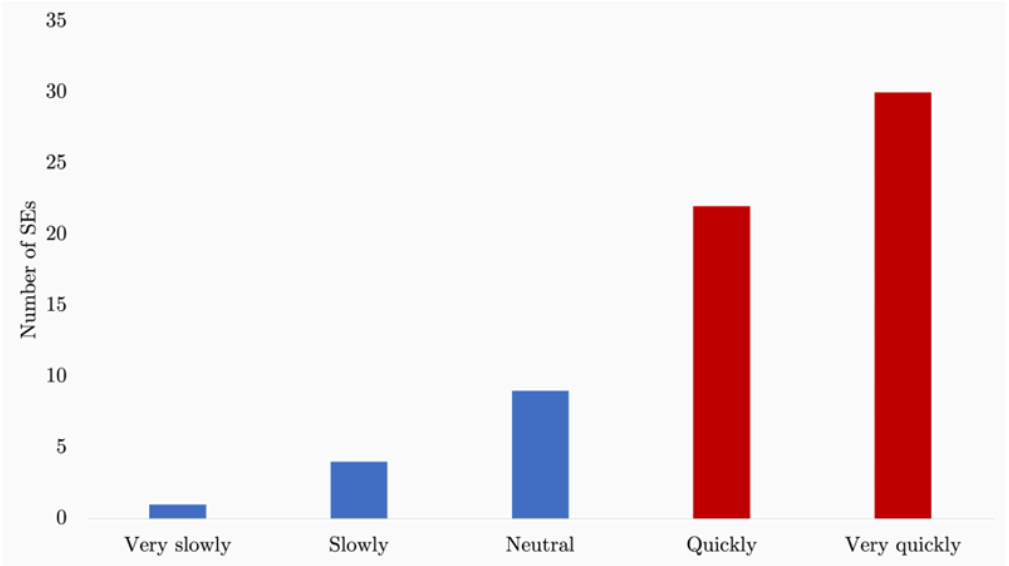
Gráfico 15 - O processo de onboarding me fez sentir mais eficiente nesse papel



Fonte: O autor, (2025).

Ao avaliar a rapidez com que a equipe de segurança fornece suporte, observa-se na Figura 14 que a maioria dos participantes concorda que o suporte é rápido ou muito rápido. Isso reforça a importância da equipe de segurança na existência e manutenção da função de *Security Champion,* uma vez que esse profissional atua como uma ponte essencial para facilitar a comunicação e o acesso às informações de segurança.

Figura 14 - Recebo suporte rapidamente para tarefas relacionadas à segurança

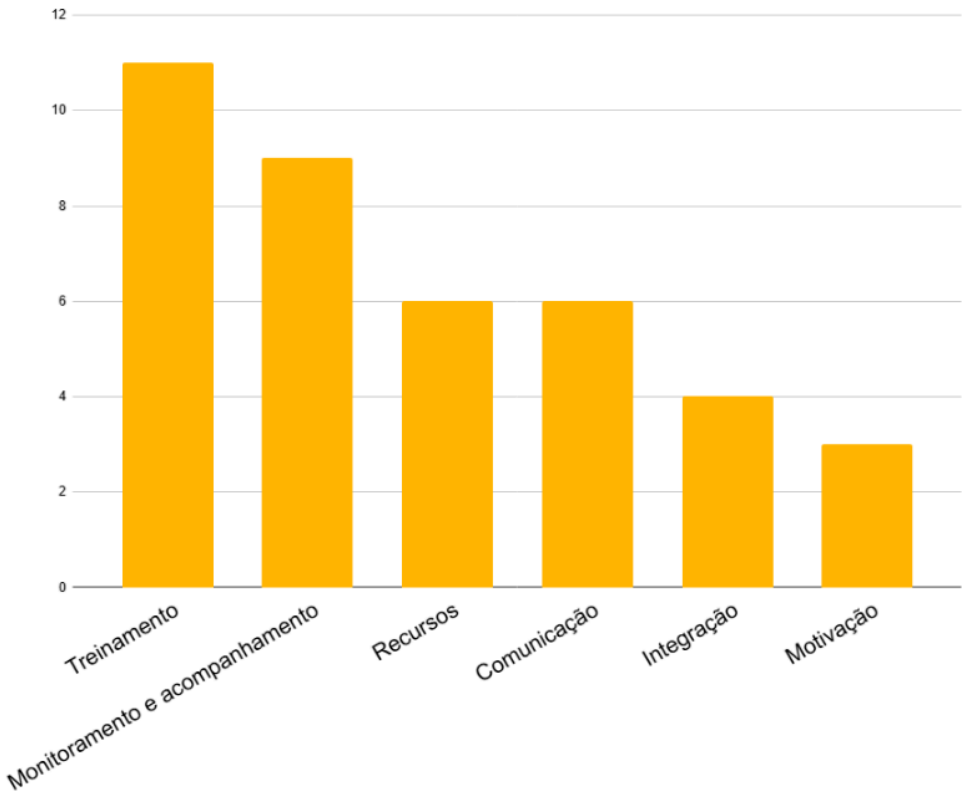


Fonte: Aalvik (2022).

5.1.9 Principais Áreas de Melhoria

Quando questionados sobre melhorias voltadas para a atuação como *Security Champion*, a maioria dos participantes destacou a necessidade de aprimoramento no treinamento, conforme mostrado no Gráfico 16. Em seguida, o monitoramento e acompanhamento também foram apontados como aspectos cruciais, evidenciando a importância de um suporte contínuo para o desempenho da função.

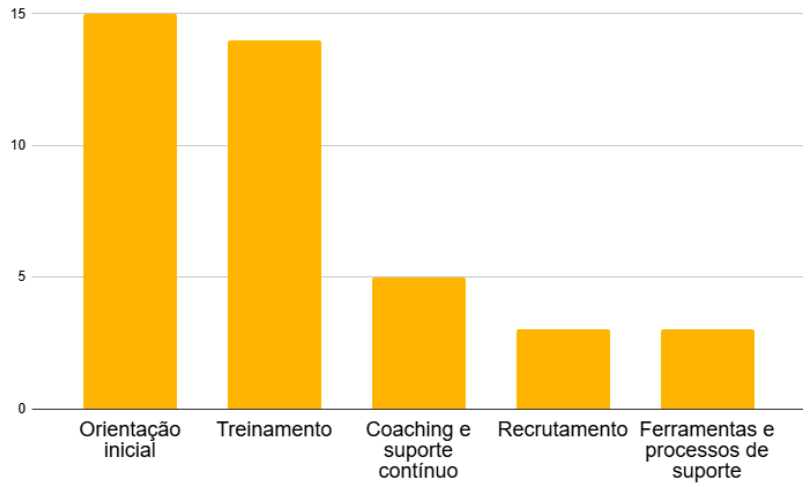
Gráfico 16 - Partes que podem ser melhoradas



Fonte: O autor, (2025).

De forma semelhante, ao se tratar especificamente do processo de seleção e onboarding, o Gráfico 17 reforça essa percepção: a orientação inicial e o treinamento foram os itens mais votados como pontos de melhoria, seguidos por coaching, suporte contínuo, recrutamento e ferramentas de apoio.

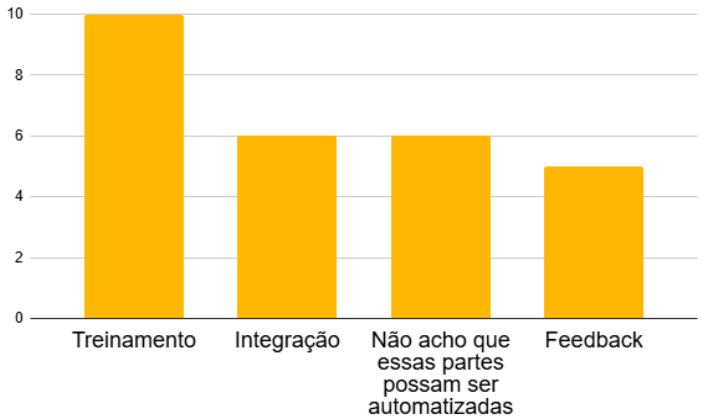
Gráfico 17 - Eu melhoraria as seguintes funções do processo de seleção e onboarding



Fonte: O autor, (2025).

Já no Gráfico 18, a predominância do treinamento continua evidente como o aspecto mais crítico, além da integração e do feedback também se destacarem como áreas que demandam ajustes.

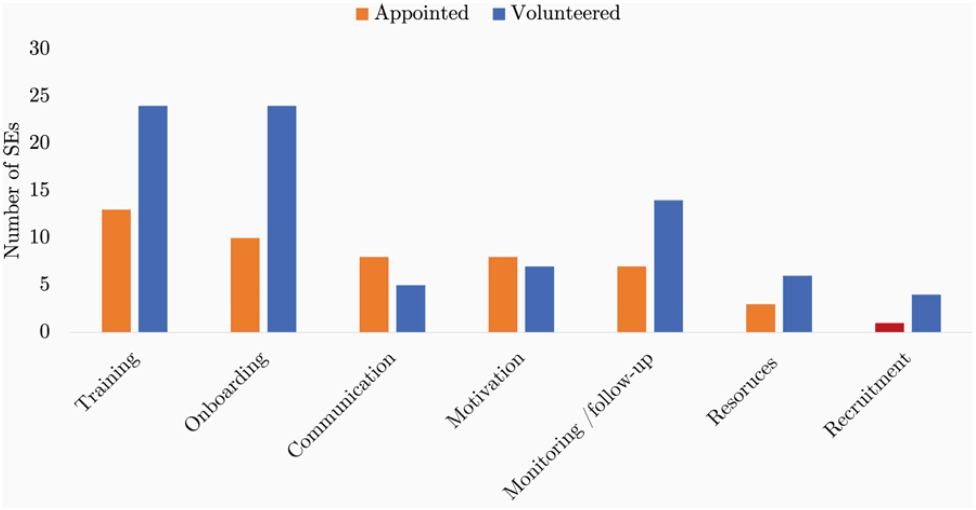
Gráfico 18 - Eu melhoraria as seguintes funções do processo de seleção e onboarding



Fonte: O autor, (2025).

Esses resultados se alinham ao que foi encontrado no estudo original de Aalvik (2022). Na Figura 15, os participantes, tanto voluntários quanto designados, também apontaram treinamento e *onboarding* como os elementos que mais necessitavam de melhorias. Isso sugere uma percepção comum entre os estudos sobre a importância de um início bem estruturado e com capacitações adequadas para garantir a eficácia do papel.

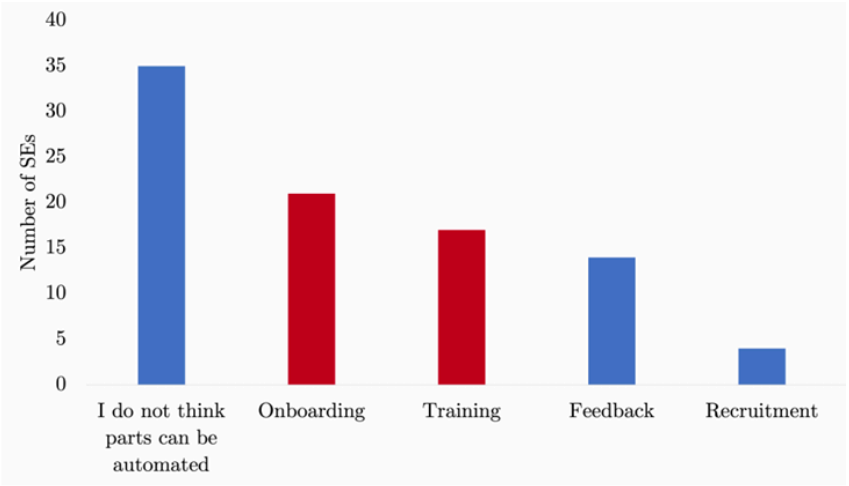
Figura 15 - Eu melhoraria as seguintes funções do programa de segurança da empresa



Fonte: Aalvik (2022).

No entanto, a Figura 16 do estudo de Aalvik revela um cenário interessante: apesar das críticas, a maior parte dos participantes afirmou que não vê necessidade de mudanças no programa. Ainda assim, entre os que sugeriram melhorias, os mesmos tópicos apareceram com destaque, onboarding, treinamento e feedback, reforçando que, mesmo em programas considerados funcionais, há espaço para aprimorar a integração de novos membros e a capacitação contínua.

Figura 16 - Partes que podem ser melhoradas



Fonte: Aalvik (2022).

5.2 Síntese Comparativa entre os Estudos

Esta seção tem como objetivo sintetizar as comparações entre o estudo original e esta pesquisa de replicação, reunindo os principais achados de ambos os trabalhos. São destacados pontos de convergência e divergência em aspectos como a forma de nomeação dos *Security Champions*, o nível de experiência prévia dos participantes, a clareza nas atribuições do papel, os desafios enfrentados, a motivação, bem como a efetividade do treinamento e do processo de onboarding. A partir dessa análise comparativa, são discutidas tendências observadas nos dois contextos e apontadas oportunidades de melhoria para a consolidação do papel do *Security Champion* nas organizações.

Tabela 2 - COMPARAÇÃO DOS RESULTADOS DO ESTUDO ORIGINAL E O ESTUDO REPLICADO

Elemento	**Estudo Original**	**Replicação Atual**
Nomeação e Designação dos Security Champions	A maioria dos participantes foi voluntária para atuar como Security Champion, indicando que as empresas dependiam principalmente do interesse espontâneo dos colaboradores.	A maioria dos participantes foi designada para atuar como *Security Champion*, indicando uma mudança na abordagem das empresas para institucionalizar essa função.
Experiência e Clareza das Expectativas	Grande parte começou com pouco ou nenhum conhecimento prévio, mas a maioria afirmava ter uma visão clara do papel antes de assumi-lo.	A maioria começou com pouco ou nenhum conhecimento prévio. Embora muitos tenham tido uma visão clara do papel antes de assumi-lo, 55% permaneceram neutros ou discordaram, sugerindo falhas na comunicação das responsabilidades.
Conflitos com Outras Funções e Alocação de Tempo	A maioria dos Security Champions consegue equilibrar suas funções de segurança com outras atribuições, o que sugere um bom gerenciamento de tempo por parte dos	A maioria dos Security Champions equilibra bem suas funções de segurança com outras atribuições. A ausência de horas pré-alocadas pode indicar tanto uma boa gestão de

	profissionais.	tempo quanto a falta de uma estrutura formal para a função.
Motivação para Atuar na Função	Profissionais voluntários demonstraram maior motivação. No estudo original, a maioria relatou estar motivada, independentemente da forma de nomeação.	Profissionais voluntários demonstram maior motivação, com 100% deles engajados, enquanto apenas 38,53% dos designados relataram o mesmo.
Treinamento e Onboarding	A maioria dos participantes sentiu falta de uma capacitação adequada, reforçando que a introdução e preparação para a função ainda são deficientes.	Apenas 31,25% dos participantes consideraram o onboarding útil, reforçando que a introdução e preparação para a função ainda são deficientes.
Suporte e Feedback	A maioria estava satisfeita com os recursos fornecidos, mas treinamento e onboarding foram identificados como as principais áreas de melhoria.	O estudo destaca que treinamento e onboarding são as principais áreas de melhoria, além de ressaltar a importância do suporte e do monitoramento contínuo.
Sentimento de Pertencimento e Engajamento	O estudo original indicava que os Security Champions tinham um papel relevante dentro das equipes, mas careciam de um ambiente estruturado para troca de experiências.	No estudo de replicação, 52,58% dos participantes relataram sentir-se parte de uma comunidade especial, demonstrando um nível considerável de engajamento.
Principais Áreas de Melhoria	Treinamento e onboarding foram apontados como os principais pontos a serem aprimorados, com a maioria dos participantes sugerindo mais capacitações para melhor desempenhar a função.	O treinamento e o onboarding foram apontados como as maiores necessidades de aprimoramento, seguidos pelo monitoramento e acompanhamento contínuo.

Fonte: O autor, (2025).

5.2.1 Reconhecimento e Institucionalização da Função

No estudo original, a maioria dos participantes se voluntariou para a função, indicando um interesse pessoal dos profissionais na área. Já no estudo de replicação, a maioria foi designada para atuar como *Security Champion*. Essa diferença sugere uma tendência à institucionalização da função nas empresas mais recentemente, reconhecendo a importância do papel e formalizando sua atuação.

A pesquisa original também indicava que os *Security Champions* tinham um papel relevante dentro das equipes, mas careciam de um ambiente estruturado para troca de experiências. No estudo de replicação, 52,58% dos participantes relataram sentir-se parte de uma comunidade especial, indicando um nível considerável de engajamento. No entanto, 21,1% discordaram e 26,32% permaneceram neutros, o que reforça que nem todos se sentem plenamente integrados.

5.2.2 Deficiência em Estrutura de Suporte

Os dois estudos apontam deficiências no treinamento e no processo de onboarding. No estudo original, a maioria dos participantes sentia falta de capacitação adequada. No estudo de replicação, apenas 31,25% consideraram o onboarding útil, e 68,75% expressaram neutralidade ou discordância. Essa similaridade indica que a introdução dos *Security Champions* ao papel ainda é falha, prejudicando sua preparação.

Além disso, no estudo de replicação, o treinamento técnico foi considerado satisfatório por apenas 45% dos participantes, reforçando a necessidade de aprimoramento na formação desses profissionais. Ambos os estudos indicam que o suporte e o monitoramento contínuo são aspectos cruciais para o sucesso do programa. Outro ponto em comum é que, apesar de muitos participantes receberem feedback, como apontado por 75% dos respondentes no estudo de replicação, mais de 50% afirmaram não se sentir confortáveis para compartilhar opiniões de forma anônima. Esse dado evidencia que ainda há carência de um ambiente seguro e transparente para o feedback.

5.2.3 Desafíos Enfrentados

Os dois estudos indicam que muitos *Security Champions* têm experiência limitada na área de cibersegurança. No estudo original, grande parte começou sem conhecimento prévio, reforçando a importância do treinamento. Já no estudo de replicação, a maioria tem entre 1 e 3 anos de experiência, o que sugere uma possível evolução na maturidade da função.

Sobre a clareza das expectativas, no estudo original, grande parte dos participantes afirmava ter uma visão clara do papel antes de assumi-lo. No estudo de replicação, 45% dos participantes concordaram com essa afirmação, 35% permaneceram neutros e 20% discordaram, mostrando que ainda há espaço para aprimoramento na comunicação sobre as responsabilidades desta função.

Ambos os estudos revelam que a maioria dos *Security Champions* não enfrenta dificuldades para equilibrar suas funções de segurança com suas demais atribuições. No entanto, o estudo de replicação mostra que 63,15% dos participantes não possuem horas pré-alocadas para tarefas de segurança, reforçando que a gestão de tempo continua sendo um desafio. Enquanto no estudo original isso foi interpretado como um sinal de um bom gerenciamento por parte dos profissionais, no estudo de replicação, a ausência de alocação formal de horas pode indicar que as empresas ainda não integram essa função de maneira estruturada em suas rotinas.

5.2.4 Motivação dos Profissionais

Nos dois estudos, os voluntários demonstraram maior motivação do que aqueles que foram designados. No estudo original, a maioria dos participantes afirmava estar motivada, independentemente da forma de nomeação. Já no estudo de replicação, 100% dos voluntários estavam motivados, enquanto apenas 38,53% dos designados relataram o mesmo. Esse dado sugere que a imposição da função pode impactar negativamente o engajamento, reforçando a importância de iniciativas para incentivar os profissionais.

6 CONCLUSÃO

Este estudo teve como objetivo analisar o papel do *Security Champion* no desenvolvimento de software, identificando seus desafios, benefícios e impacto organizacional. Os resultados obtidos tanto no estudo original quanto na sua replicação revelam que, apesar do crescente reconhecimento dessa função, ainda existem aspectos que precisam ser aprimorados para garantir sua eficácia.

Observou-se uma tendência à institucionalização do *Security Champion* dentro das empresas, com uma maioria significativa dos participantes sendo formalmente designada para o papel. No entanto, ainda há desafios relacionados à clareza das expectativas e à estrutura de suporte disponível para esses profissionais. O treinamento e o onboarding foram consistentemente apontados como as principais lacunas, sugerindo a necessidade de investimentos mais robustos em capacitação e suporte contínuo.

Embora a maioria dos *Security Champions* consiga equilibrar suas funções de segurança com suas demais atribuições, a falta de horas pré-alocadas levanta questionamentos sobre a formalização dessa atividade dentro das organizações. Ademais, verificou-se que os profissionais que se voluntariaram para a função demonstram maior motivação em comparação aos que foram designados, o que pode impactar diretamente a eficácia do programa.

Outro achado relevante foi o papel do *Security Champion* como elo entre as equipes de desenvolvimento e segurança. Apesar disso, nem todos os profissionais se sentem plenamente consultados sobre questões de segurança, o que evidencia a necessidade de aprimoramento na integração dessa função dentro da cultura organizacional.

Por fim, o estudo destaca que, para que o programa de *Security Champions* seja efetivo, é fundamental aprimorar os processos de seleção, treinamento e acompanhamento. O desenvolvimento de um ambiente colaborativo, com feedback estruturado e canais de suporte eficientes, pode contribuir significativamente para o fortalecimento desse papel e para a disseminação de boas práticas de segurança dentro das organizações.

Em suma, os achados reforçam a importância da função do *Security Champion* e indicam direções estratégicas para seu aperfeiçoamento, visando uma segurança integrada e mais eficiente no desenvolvimento de software.

REFERÊNCIAS

ADEWALE OBAFEMI, O.; NGEVAO, T.; ADEWALE, O. **Cyber Security: Emerging Threats, Challenges, and Future Directions**. [s.l: s.n.].

AKPA, V.; ASIKHIA, O.; NNEJI, N. **Organizational Culture and Organizational Performance: A Review of Literature**. International Journal of Advances in Engineering and Management (IJAEM), v. 3, p. 361, 2021.

AKSOY, C. **BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS**. İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, v. 7, n. 1, p. 96–110, 19 jan. 2024.

BESSA, T.; DIAS, D. **Metodologias ágeis para o desenvolvimento de softwares Agile methodologies for software development**. [s.l: s.n.].

CAMPANELLI, A. S.; PARREIRAS, F. S. **Agile methods tailoring - A systematic literature review**. Journal of Systems and Software, v. 110, p. 85–100, 1 dez. 2015.

EBAD, S. A. **Exploring How to Apply Secure Software Design Principles**. IEEE Access, v. 10, p. 128983–128993, 2022.

FADZISO, T. et al. **Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat**. 2023.

GOEL, J. N.; MEHTRE, B. M. **Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology**. Procedia Computer Science. **Anais**...Elsevier, 2015.

GUTFLEISCH, M. et al. **Security Champions Without Support: Results from a Case Study with OWASP SAMM in a Large-Scale E-Commerce Enterprise**. ACM International Conference Proceeding Series. **Anais**...Association for Computing Machinery, 16 out. 2023.

AALVIK, H. **Towards an Effective Security Champions Program**. [s.l: s.n.].

HUO, M. et al. **Software Quality and Agile Methods**. [s.l: s.n.].

HUSSAIN, A.; MOHAMED, A.; RAZALI, S. **A Review on Cybersecurity: Challenges & Emerging Threats**. ACM International Conference Proceeding Series. **Anais**...Association for Computing Machinery, 31 mar. 2020.

MENGES, U. et al. **Caring Not Scaring - An Evaluation of a Workshop to Train Apprentices as Security Champions**. ACM International Conference Proceeding Series. **Anais**...Association for Computing Machinery, 16 out. 2023.

NGUYEN-DUC, A. et al. **Facilitating Security Champions in Software Projects - An Experience Report from Visma**. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). **Anais**...Springer Science and Business Media Deutschland GmbH, 2024.

O‘G‘LI, A. B. A. **Cybersecurity: threats, challenges, solutions**. International Journal of Law And Criminology, v. 5, n. 1, p. 5–8, 1 jan. 2025.

OK, E.; ENIOLA, J. **Best Practices for Cybersecurity Risk Management in Agile Software Development**. [s.l: s.n.].

RAJAPAKSE, R. N. et al. **Challenges and solutions when adopting DevSecOps: A systematic review**. **Information and Software Technology** Elsevier B.V., , 1 jan. 2022.

REEGÅRD, K.; BLACKETT, C.; KATTA, V. **The Concept of Cybersecurity Culture**. Research Publishing Services, 23 jan. 2020.

SÁNCHEZ-GORDÓN, M.; COLOMO-PALACIOS, R. **Security as Culture: A Systematic Literature Review of DevSecOps**. Proceedings - 2020 IEEE/ACM 42nd International Conference on Software Engineering Workshops, ICSEW 2020. **Anais**...Association for Computing Machinery, Inc, 27 jun. 2020.

SCHEIN, E. H. **Organizational Culture**. [s.l: s.n.].

TASHTOUSH, Y. M. et al. **Agile Approaches for Cybersecurity Systems, IoT and Intelligent Transportation**. IEEE Access, v. 10, p. 1360–1375, 2022.

APÊNDICE A – TABELA DE PERGUNTAS DO QUESTIONÁRIO ELETRÔNICO

ID	Pergunta	Opções de Resposta
1	Qual o seu nível de formação?	Estudante de Graduação; Graduação completa; Pós-graduação lato sensu (Especialização); Estudante de mestrado; Mestrado completo; Estudante de doutorado; Doutorado completo
2	Qual é/Qual foi o seu curso de graduação ?	Análise e Desenvolvimento de Sistemas; Ciência da computação; Engenharia da computação; Engenharia de Software; Outro
3	Como você começou a atuar em atividades relacionadas à segurança? (Ex.: Code review, mitigação de vulnerabilidades, consultoria, desenvolvimento seguro e etc.)	Não atuo com segurança; Alguem de designou para essa fumção; Eu me ofereci voluntariamente
4	Qual é sua função principal na empresa, além das atividades de segurança?	Engenheiro de software; Arquiteto(a); Testador(a) ou Especialista em Garantia de Qualidade; Analista; Outro
5	Sua organização é de qual porte?	Pequena (<100 funcionários); Média (100-500 funcionários); Grande (>500 funcionários)
6	Qual a área de atuação da empresa?	Financeiro; Sistemas de Varejo; Educalçao; Bigdata; Outro
7	Como você descreveria seu conhecimento sobre segurança antes de assumir esse papel de *Security Champion*?	Iniciante ou sem experiência anterior; Intermediário; Avançado
8	Há quanto tempo você desempenha atividades relacionadas à segurança em sua equipe?	Menos de 1 ano; 1-3 anos; 4-6 anos; 7-10 anos; 11-15 anos; Mais de 15 anos

9	Recebi uma visão clara das expectativas antes de assumir esse papel	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
10	Não tenho conflitos entre este papel e outras funções que desempenho	Discordo Totalmente; Discordo; Neutro; Concordo; oncordo Totalmente
11	Estou satisfeito(a) com o suporte inicial que recebi para atuar nessa área	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
12	Estou satisfeito(a) com meu desempenho nas atividades de segurança	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
13	Tenho horas previamente alocadas para tarefas relacionadas à segurança	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
14	Recebi um treinamento/orientação formal sobre como atuar nesse papel	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
15	Recebi informações sobre os programas de segurança da empresa.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
16	Tive um mentor ou suporte direto durante o início da minha atuação.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
17	Estou familiarizado(a) com as seguintes atividades de suporte oferecidas pela equipe de segurança:	Reuniões de grupo para discutir segurança; Sessões de conscientização sobre segurança; Canal de comunicação específico para segurança (ex.: Slack); Contato direto com a equipe de segurança da empresa; Plataformas de treinamento em segurança, como o Secure Code Warrior; Nenhuma das opções acima
18	Eu me comunico com outras pessoas que também desempenham este papel de security champion por meio de:	Conversas presenciais no escritório; Email; Teams; Telefone; Slack; Não me comunico com outros colegas nessa área; Outro

19	Há orientações escritas suficientes sobre como desempenhar esse papel.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
20	Estou satisfeito(a) com o treinamento técnico de segurança que recebi.	Discordo Totalmente; Discordo; Neutro; Concordo; oncordo Totalmente
21	Estou satisfeito(a) com o treinamento de habilidades interpessoais (ex.: comunicação).	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
22	Acho úteis as reuniões de grupo para discutir segurança.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
23	As ferramentas e canais de suporte são eficazes para compartilhar informações.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
24	Recebo suporte rapidamente para tarefas relacionadas à segurança.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
25	Sinto que faço parte de uma comunidade especial ao desempenhar esse papel.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
26	Estou, em geral, satisfeito(a) com os recursos fornecidos para me ajudar nessa área.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
27	Fui informado(a) sobre como estou me saindo nesse papel.	Sim; Não; Não se aplica
28	Estou satisfeito(a) com a quantidade de feedback que recebo	Sim; Não; Não se aplica
29	Sou consultado(a) sobre minha opinião em relação às atividades de segurança.	Sim; Não; Não se aplica
30	Sei a quem recorrer para compartilhar sugestões de melhoria.	Sim; Não; Não se aplica
31	Posso compartilhar minhas opiniões de forma anônima.	Sim; Não; Não se aplica
32	Existe um processo claro de onboarding para quem começa a atuar com segurança.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
33	O processo de onboarding me fez sentir	Discordo Totalmente;

	mais eficiente nesse papel.	Discordo; Neutro; Concordo; Concordo Totalmente
34	O processo de onboarding me deixou mais confiante para desempenhar essa função.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
35	O onboarding me ajudou a entender a importância desse papel na empresa.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
36	Estou motivado(a) a continuar trabalhando com segurança.	Discordo Totalmente; Discordo; Neutro; Concordo; Concordo Totalmente
37	Eu melhoraria as seguintes funções do processo de seleção e onboarding:	Recrutamento; Orientação inicial; Treinamento; Ferramentas e processos de suporte; Coaching e suporte contínuo
38	Eu melhoraria as seguintes funções do programa de segurança da empresa:	Recrutamento; Integração; Comunicação; Recursos; Treinamento; Monitoramento e acompanhamento; Motivação; Outro
39	Acho que as seguintes partes do programa de segurança poderiam ser automatizadas:	Recrutamento; Integração; Treinamento; Feedback; Não acho que partes possam ser automatizadas; Outro
40	Deseja realizar algum comentário adicional ?	Subjetiva

APÊNDICE B - LINK DO QUESTIONÁRIO ELETRÔNICO APLICADO NA PESQUISA

Research on the role of security champions performed by developers in companies