UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO ACADÊMICO DE RECIFE

JOSÉ CLAUDINO DOS SANTOS NETO

A EDUCAÇÃO EM CODIFICAÇÃO SEGURA É NECESSÁRIA NA INDÚSTRIA DE SOFTWARE? Uma investigação por meio de uma pesquisa na indústria local de software.

RECIFE

2023

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO ACADÊMICO DE RECIFE

SISTEMAS DE INFORMAÇÃO

JOSÉ CLAUDINO DOS SANTOS NETO

A EDUCAÇÃO EM CODIFICAÇÃO SEGURA É NECESSÁRIA NA INDÚSTRIA DE SOFTWARE? Uma investigação por meio de uma pesquisa na indústria local de software.

TCC apresentado ao Curso de Sistemas de Informação da Universidade Federal de Pernambuco, Centro Acadêmico de Recife, como requisito para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador(a): Profª. Carla Taciana Lima Lourenço Silva Schuenemann

FICHA CATALOGRÁFICA

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

Santos Neto, José Claudino dos.
A educação em codificação segura é necessária na indústria de software? Uma investigação por meio de uma pesquisa na indústria local de software / José Claudino dos Santos Neto. - Recife, 2023.
114 : il., tab.

Orientador(a): Carla Taciana Lima Lourenço Silva Schuenemann
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Sistemas de Informação - Bacharelado, 2023.
Inclui referências, apêndices, anexos.

1. Desenvolvimento de Software Seguro. 2. Educação em segurança da informação. 3. Codificação segura. 4. Survey. I. Schuenemann, Carla Taciana Lima Lourenço Silva. (Orientação). II. Título.

000 CDD (22.ed.)

JOSÉ CLAUDINO DOS SANTOS NETO

A EDUCAÇÃO EM CODIFICAÇÃO SEGURA É NECESSÁRIA NA INDÚSTRIA DE SOFTWARE? Uma investigação por meio de uma pesquisa na indústria local de software.

TCC apresentado ao Curso de Sistemas de Informação da Universidade Federal de Pernambuco, Centro Acadêmico de Recife, como requisito para a obtenção do título de Bacharel em Sistemas de Informação.

Aprovado em: 26/04/2023.

BANCA EXAMINADORA

_____

Profª. Carla Taciana Lima Lourenço Silva Schuenemann (Orientadora)
Universidade Federal de Pernambuco

_____

Profª. Jéssyka Flavyanne Ferreira Vilela (Examinadora Interna)
Universidade Federal de Pernambuco

DEDICATÓRIA

A memória de Cremilda Daniel, minha querida avó que tanto se dedicou a me apoiar em minha jornada acadêmica, sem a qual eu certamente não estaria onde estou.

A minha querida mãe que me apoiou e incentivou durante o decorrer do processo desde minha matrícula no curso, até esse presente momento.

AGRADECIMENTOS

A Deus, em primeiro lugar, que sempre me deu oportunidades, força de vontade e coragem para superar todos os desafios.

Gostaria de agradecer a minha família por sempre me apoiar nos estudos, me ensinando que só a educação transforma a vida de pessoas pretas, periféricas e pobres. Especialmente a minha mãe Vera que desde criança me apoiou em minha vida de estudante, chegando até assistir aula em um período que estava doente, sem nunca permitir que eu faltasse aula. A minha avó Cremilda, que nunca mediu esforços para nada quando se tratava da minha educação, pagando curso, passagens, cobrando, acompanhando, infelizmente ela não poderá ler esse trabalho ou participar deste momento, mas sei que ela está feliz com essa conquista. A minha irmã Rebeca e meus quatro sobrinhos, que me dão apoio diário, e o Bingo, novo mascote da família que dorme sempre ao meu lado enquanto escrevo este trabalho.

Um agradecimento aos que me acompanharam durante minha graduação me dando todo apoio emocional necessário, especialmente meus companheiros de curso Gabriel e Navarro, parceiros que levo deste curso para a vida, um trio onde sempre nos apoiamos e incentivamos mutuamente dentro e fora da faculdade. Um agradecimento especial a Pedro por ter me apoiado, motivado e incentivado a finalizar esta etapa da minha vida. A meu amigo Lucas que me deu várias dicas e fiz ler várias versões deste trabalho. E a mim por ser resiliente nessa jornada acadêmica.

A minha orientadora e professora Carla Silva pela paciência, sugestões e melhorias aplicadas no decorrer deste trabalho. E a todos os meus professores, que cada um com seu jeito e conhecimento contribuiu para a minha formação.

Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob o conhecimento de pessoas de má-fé ou concorrentes podem comprometer significativamente não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.10).

RESUMO

O objetivo do trabalho é investigar o estado da educação em segurança da informação na área de desenvolvimento de software local, com base em duas pesquisas aplicadas internacionalmente. Foi adotado o método de pesquisa por survey, onde um questionário foi elaborado e enviado a profissionais da indústria de software local. De acordo com os resultados obtidos, a maioria dos participantes considera a educação em segurança da informação importante para o desenvolvimento de software seguro, no entanto, ainda há uma carência na educação em segurança da informação local. Conclui-se que as empresas devem investir mais em treinamentos adequados e abrangentes sobre o tema, além de incentivar e recompensar os profissionais que priorizam a segurança do software em seus projetos. É fundamental disseminar uma cultura de segurança da informação em toda a organização, desde a alta gestão até os profissionais de desenvolvimento, para conscientizar a todos sobre a importância da segurança da informação e sua responsabilidade em mantê-la. Por fim, destaca-se que os desenvolvedores têm um papel crucial na garantia da segurança do software, sendo responsáveis por buscar conhecimento e aprimorar suas habilidades em codificação segura por meio de treinamentos, leituras e práticas.

Palavras-chave: Desenvolvimento de Software Seguro; Educação em segurança da informação; Codificação segura, Survey.

ABSTRACT

The aim of this work is to investigate the state of education in information security in the local software development industry, based on two internationally conducted surveys. The survey method was adopted, in which a questionnaire was developed and sent to local software industry professionals. According to the results obtained, the majority of the participants consider education in information security important for secure software development, however, there is still a lack of local education in information security. It is concluded that companies should invest more in adequate and comprehensive training on the subject, as well as incentivize and reward professionals who prioritize software security in their projects. It is essential to disseminate a culture of information security throughout the organization, from top management to development professionals, to raise awareness of the importance of information security and their responsibility to maintain it.Finally, it should be noted that developers have a crucial role in ensuring software security, being responsible for seeking knowledge and improving their skills in secure coding through training, reading, and practice.

Keywords: Secure Software Development; Information Security Education; Secure Coding, Survey.

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIAÇÕES

LGPD	Lei Geral de Proteção de Dados
SDLC	Ciclo de vida do desenvolvimento de software *(Systems Development Life Cycle)*
SDL	Ciclo de Vida de Desenvolvimento Seguro *(Security Development Lifecycle)*
TCU	Tribunal de Contas da União
CI	Integração Contínua (*Continuous Integration*)
CD	Entrega Contínua (*Continuous Delivery*)
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

A palavra informação deriva do latim, *informare*, que significa dar forma ou aparência, criar, representar uma ideia ou noção de algo que é colocado em forma, em ordem. Drucker (2000, p.13) define a informação como um “dado investido de propósito”[1].

A Informação é um recurso fundamental para as empresas, uma vez que permeia todas as áreas e atividades organizacionais. Esse papel se deve à mudança de paradigma da sociedade, que saiu da industrialização para uma sociedade da informação, na qual a informação tornou- se o principal ativo na busca pela sobrevivência e competitividade das empresas, atuando como apoio nas decisões executivas. Segundo Stair e Reynolds (2002, p.10), “informação é um conjunto de fatos organizados de modo a terem valor adicional, além do valor dos fatos propriamente ditos”[2].

Com o avanço constante da tecnologia, a segurança da informação se tornou um assunto de grande relevância para empresas e organizações em todo o mundo. A cada dia, a quantidade de informações armazenadas e compartilhadas digitalmente cresce exponencialmente, o que faz com que seja cada vez mais necessária a presença de profissionais especializados em segurança da informação. Conforme Nakamura e Geus (2002, p.9), “a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida”[3].

A segurança da informação é um tema de extrema importância na era da tecnologia e da informação sempre constante. Essa indústria de *software* está em constante evolução e crescimento, com novas tecnologias e ferramentas surgindo a cada dia e com isso a crescente dependência de sistemas e tecnologias de informação em todos os setores da sociedade, a necessidade de garantir os três pilares da segurança da informação; confidencialidade, integridade e disponibilidade das informações é cada vez mais importante. A segurança da informação envolve a implementação de medidas para proteger as informações contra ameaças, sejam

elas, externas ou internas, tais como *hackers*, *malwares*, usurpadores de identidade, *phishing*, entre outras.

De acordo com Peixoto (2006, p. 37), “O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade”[4].

A importância da segurança da informação não pode ser subestimada. A divulgação não autorizada ou perda de informações pode ter consequências de grande impacto na empresa, incluindo danos financeiros, dano na reputação, violação da privacidade e até mesmo riscos à segurança física. Além disso, as empresas precisam cumprir leis e regulamentações que exigem proteção adequada das informações, como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil [5], que passaram a ser vigente com sanções administrativas cabíveis em 1.º de agosto de 2018, nos termos da Lei n.º 13.709/2018.

Há uma concordância entre (2009) [6] e Mitnick e Simon (2003) [7] de que os incidentes de segurança da informação são, em grande parte, causados pelo homem. Alexandria (2009) [6] ressalta que um erro comum é não levar em conta os fatores humanos e sociais envolvidos na construção da segurança da informação.

1.2 Delimitação do tema estudado

Nesse contexto, a formação e treinamento de profissionais de segurança da informação torna-se essencial para garantir a proteção de dados e sistemas, bem como a privacidade e segurança de informações sensíveis. A codificação segura envolve a prática de desenvolver códigos de *software* para garantir que sejam robustos e resistentes a ameaças de segurança. Porém, a complexidade desse campo requer uma formação sólida e contínua, que acompanhe as mudanças constantes e evolução das tecnologias.

Além disso, as regulamentações de proteção de dados, exigem que as empresas protejam as informações pessoais dos usuários e clientes, e a codificação segura é uma das principais medidas para atender a esses requisitos. Então, a educação em codificação segura é fundamental para que os desenvolvedores e

profissionais de tecnologia entendam as ameaças de segurança, aprendam as melhores práticas de codificação segura e implementá-las em seus projetos de *software*. Isso ajudará a garantir a segurança dos dados, a proteção da privacidade e a mitigação de riscos cibernéticos para as empresas e seus usuários.

1.3 Objetivos da pesquisa

Os desenvolvedores estão no centro do desenvolvimento de sistemas, nem mesmo o surgimento de tecnologias com Inteligência Artificial e o aprimoramento do aprendizado de máquina conseguiram tirar o protagonismo dos seres humanos. Pois os seres humanos estão por trás de todo esse mecanismo projetando e implementando esse mecanismo.

Para se ter proatividade na implementação de código seguro desde o início do Ciclo de vida do desenvolvimento de *software*(SDLC), um desenvolvedor deve ter as habilidades e capacidades necessárias para escrever código de forma segura e mantê-lo em mente desde o design até o desenvolvimento e a implantação, conhecido *security by design*. Mas todos envolvidos na equipe de desenvolvimento acham difícil de fazer isso, a dificuldade, no entanto, não está em implementar a segurança necessária, mas em aprender como fazer quando os programas e métodos de treinamentos não são relevantes para o trabalho dos desenvolvedores.

A falta de compreensão sobre por que os desenvolvedores de software não seguem os padrões de codificação segura e práticas recomendadas já estabelecidas (algumas são citadas no item 2.9 deste documento), é um problema recorrente na indústria. Embora a segurança de software seja amplamente discutida, existem poucos resultados empíricos que explicam esse fenômeno no contexto local da indústria de *software*. Vários estudos têm destacado a importância da segurança de software, mas poucos se concentram nos fatores que levam os desenvolvedores a ignorar ou desconhecer padrões conhecidos de segurança de *software*. Nesse sentido, a coleta de dados foi realizada para responder à seguinte questão de pesquisa: A educação em codificação segura é necessária na indústria de *software* local?

Conforme o Gartner, em 2023 estima-se que os investimentos em TI alcançarão US $4,5 trilhões, um aumento em relação a 2022 de 2,4%. Neste mesmo

estudo verificou-se que 66% dos CIOs disseram que o plano era aumentar os investimentos em segurança, provando que proteger as empresas contra ameaças cibernéticas se mantém como prioridade [8].

Já segundo um relatório da MarketsandMarkets o mercado de segurança vai alcançar no ano de 2027 um faturamento anual em torno de US $266,2 bilhões [9]. Alguns fatores impulsionam esse crescimento do mercado de segurança cibernética, como o aumento do volume de ataques, conforme um mapeamento da Statista só no primeiro semestre de 2022 ocorreu 2,8 bilhões de ataques de *malware* em um contexto global [10], além de 236,1 milhões de ataques de tipo *ransomware* [11].

As consequências de ataques assim podem ser angustiantes para as vítimas, caso o ataque coloque em risco vidas humanas e são potencialmente caras para as empresas. O custo médio de uma violação de dados é de cerca de US $3,86 milhões, mas esse valor varia bastante entre região, tamanho e setor da empresa. Um exemplo é no setor de saúde que o custo médio de uma violação de dados pode chegar a US $7,13 milhões [12].

O objetivo desta pesquisa foi resumido da seguinte forma: gerar conhecimento por meio da análise de fatores pessoais, comportamentais e ambientais relacionados ao conhecimento dos desenvolvedores e suas equipes sobre codificação segura, bem como a forma como direcionam seus esforços para fazer código seguro e o suporte que recebem da indústria para isso.

1.4 Justificativa da pesquisa

Neste cenário de um mundo hiper conectado e digitalizado, e com crescimento de vulnerabilidades nos *softwares* desenvolvidos, se o desenvolvedor tiver problema de falta de conhecimento em codificação segura, as empresas de *software* podem sofrer prejuízos quando os sistemas são comprometidos, o que pode levar à perda de dados confidenciais, interrupção de serviços, violação de privacidade, entre outros problemas.

A indústria de *software* local, assim como a global, precisa investir em programas de treinamento e capacitação em codificação segura para seus desenvolvedores. A pesquisa deste trabalho de conclusão de curso pode ajudar a

destacar a importância desse treinamento, bem como os principais sentimentos que devem ser abordados com os desenvolvedores na criação de programas de treinamento em codificação segura.

Essa pesquisa é baseada em duas outras pesquisas, a primeira realizada entre março e setembro de 2020 em desenvolvedores da indústria, distribuídos em 3 empresas, com 194 participantes. Pesquisa disponível no artigo "*Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey*" de maio de 2021. [13]

A outra pesquisa foi aplicada com desenvolvedores de *software* da América do Norte, com 123 respostas. Pesquisa disponível no artigo "*Think secure from the beginning: A Survey with Software Developers*", de 2019. [14].

Por conta dessas pesquisas terem sido realizadas em um cenário externo, tornou-se importante conhecer o cenário local e comparar os resultados entre os estudos. Com base no objetivo da pesquisa, foram desenvolvidas as seguintes questões de pesquisa (RQs):

Quadro 1 – Questões e motivações da pesquisa.

Item	**Motivação**
RQ1: Até que ponto os desenvolvedores de *software* estão cientes das diretrizes de codificação segura?	Verificar até onde os desenvolvedores têm conhecimento sobre padrões de segurança de *software*.
RQ2: O tamanho da empresa ou a adoção de técnicas/métodos/ferramentas específicas influenciam na segurança.	Verificar as implicações do contexto da empresa, na questão de segurança.
RQ3: Quais fatores levam os desenvolvedores de *software* a seguirem ou ignorarem as diretrizes de codificação segura?	Identificar quais são os fatores internos e/ou externos que afetam os desenvolvedores na codificação segura de *softwares*.
RQ4: Até que ponto a educação sobre codificação segura é necessária?	Verificar a importância da necessidade de uma educação voltada para a segurança do ponto de vista da

	indústria de *software* local.

1.5 Metodologia adotada na pesquisa

Este estudo é classificado como uma pesquisa quantitativa, caracterizada pelo uso de técnicas estatísticas para análise dos dados coletados. O objetivo é identificar as opiniões e percepções de profissionais da indústria de *software* sobre a necessidade de ensino de codificação segura. As perguntas foram elaboradas concisamente, utilizando linguagem acessível e evitando jargões técnicos que dificultem o entendimento por parte dos respondentes. O *Survey* terá questões sobre o perfil do respondente, a importância da segurança no desenvolvimento de software e a necessidade de treinamento em codificação segura.

1.6 Estrutura do trabalho

O trabalho de conclusão de curso estrutura-se em quatro seções, apresentando-se na primeira uma introdução contextualizando informação, segurança da informação e a importância de ter uma equipe preparada para criar sistemas seguros. Na segunda seção, faço a revisão de literatura, trazendo breve discussão sobre trabalhos anteriores relacionados ao tema. Na seção seguinte trago a metodologia utilizada na pesquisa e uma visão geral da construção da pesquisa. A quarta seção, abordará uma visão dos resultados mais importantes da análise da pesquisa e na seção seguinte, uma breve discussão sobre ações a serem tomadas conforme a análise dos resultados, essas duas seções constituem a parte central do trabalho. Finalmente, a sexta seção conclui esse trabalho com uma visão geral do estudo.

2 REVISÃO DE LITERATURA

Na seção que se segue, serão explorados diversos conceitos relevantes e interligados ao campo de estudo abordado neste artigo. Além disso, na última subseção, serão apresentados e discutidos alguns trabalhos correlatos que se relacionam com o tema em questão. É importante salientar que o entendimento e a análise desses conceitos e trabalhos auxiliarão na compreensão e na contextualização do estudo aqui apresentado.

2.1 Segurança da informação

A segurança da informação é um tema amplamente estudado e discutido em diversas pesquisas. Segundo Kizza (2015) [15], à segurança da informação é um conjunto de medidas que visam garantir a proteção dos dados e informações importantes em sistemas de informação. Essas medidas incluem a utilização de criptografia, autenticação, controle de acesso, *backups*, entre outros.

Conforme Sêmola (2014, p.43) [16], os conceitos-chave da segurança da informação são os seguintes:

- Confidencialidade: A informação deve ser protegida conforme seu grau de sigilo, a fim de limitar seu acesso e uso somente às pessoas autorizadas.
- Integridade: A informação deve ser mantida em seu estado original, sem sofrer alterações indevidas, intencionais ou acidentais.
- Disponibilidade: A informação gerada ou obtida por uma pessoa, ou instituição deve estar acessível aos seus usuários no momento em que precisarem dela, para qualquer finalidade.

Segundo o Tribunal de Contas da União (TCU), a confidencialidade

> consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.9) [17]

Ainda seguindo o entendimento do TCU, a integridade é definida da seguinte forma:

> A integridade consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.9) [17]

E por último o TCU define o último pilar da tríade, da seguinte forma:

> garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.10) [17]

É totalmente concebível pensar que a violação de qualquer um dos três pilares da tríade CIA — confidencialidade, integridade e disponibilidade — afeta negativamente uma organização. É importante ressaltar não haver consenso na literatura sobre a importância relativa de cada pilar, uma vez que todos são essenciais para alcançar a segurança.

Para Beal (2012, p.52) [18], além dos pilares já descritos, a autora considera os seguintes requisitos:

- Autenticidade: Garantia de que a informação seja proveniente da fonte à qual ela é atribuída.
- Irretratabilidade da comunicação (não repúdio): Proteção contra a alegação por parte de um dos participantes de uma comunicação que não ocorreu.

Coelho et al. (2014) [19] consideram, ainda, como essenciais os seguintes requisitos:

- Conformidade: Estar em conformidade é estar de acordo seguindo e fazendo com que se cumpram leis e regulamentos internos e externos.
- Controle de acesso: Trata de limitar e controlar o acesso lógico/ físico aos ativos de uma organização por meio dos processos de identificação, autenticação e autorização, visando proteger os recursos contra acessos não autorizados.

2.2 Codificação segura

Segundo o site Definirtec, o conceito de codificação segura é a prática de escrever um código-fonte ou uma base de código compatível com os melhores princípios de segurança para um determinado sistema e interface [20].

A codificação segura é uma área em constante evolução e pesquisa. Em seu trabalho, Almorsy et al. (2016) [21] destacam a importância da codificação segura como uma abordagem para o desenvolvimento de *software* que tem em vista reduzir as vulnerabilidades de segurança por meio da aplicação de boas práticas de programação.

Essas boas práticas incluem a validação de entrada de dados, controle de acesso, uso correto de criptografia, entre outras. A codificação segura pode ajudar a reduzir a exposição a ataques de *hackers* e outras ameaças de segurança.

2.3 Ensino de codificação segura na indústria de tecnologia

O ensino de codificação segura na indústria de tecnologia é importante para garantir que os desenvolvedores de *software* estejam cientes das melhores práticas de segurança e possam aplicá-las em seu trabalho. Muitas organizações de tecnologia oferecem treinamento em codificação segura para seus desenvolvedores, incluindo cursos online e presenciais. O ensino de codificação segura pode ajudar a reduzir as vulnerabilidades de segurança em *software* e aumentar a segurança geral dos sistemas de informação.

Segundo Payne et al. (2017) [22], muitas organizações de tecnologia oferecem treinamento em codificação segura para seus desenvolvedores, incluindo cursos online e presenciais. O ensino de codificação segura pode ajudar a reduzir as vulnerabilidades de segurança em *software* e aumentar a segurança geral dos sistemas de informação.

O ensino de codificação segura na indústria de tecnologia é uma prática importante para garantir que os desenvolvedores estejam preparados para criar *softwares* seguros. Kizza (2015) [15] ressalta que o treinamento em codificação

segura pode ser realizado por meio de cursos, palestras, treinamentos, *workshops* e outras iniciativas que visem aprimorar as habilidades dos desenvolvedores.

2.4 Vulnerabilidades de software

As vulnerabilidades de *software* são uma ameaça constante à segurança da informação. As referências relevantes em segurança da informação, como o OWASP Top 10, fornecem uma lista das vulnerabilidades de *software* mais comuns e como evitá-las. Os desenvolvedores devem estar familiarizados com essas referências e implementar as melhores práticas de codificação segura em seus projetos de *software* [23].

As vulnerabilidades de *software* são falhas de segurança que permitem que um atacante execute código malicioso ou acesse informações sensíveis do sistema. Payne et al. (2017) [22] destacam que as vulnerabilidades de *software* são uma das principais causas de ataques cibernéticos, portanto é importante que os desenvolvedores estejam cientes dessas vulnerabilidades e tomem medidas para eliminá-las em seus *softwares*.

Segundo Khan e Khan (2019) [24], as vulnerabilidades de *software* são falhas no código de um programa que podem ser exploradas por *hackers* para obter acesso não autorizado a um sistema de informação. Essas vulnerabilidades podem ser introduzidas durante o processo de desenvolvimento de *software*, como resultado de *bugs* ou problemas de segurança na codificação.

2.5 Crescimento de ataques a *softwares*

O aumento de ataques a sistemas tem sido uma preocupação crescente nos últimos anos. Thomas e Kessler (2019) [25] afirmam que o número de ataques cibernéticos tem aumentado significativamente, especialmente em setores como finanças, saúde e governo. Isso destaca a importância de medidas de segurança mais robustas e eficazes para garantir a proteção dos sistemas de informação.

Segundo o relatório de 2021 do Data Breach Investigations Report da Verizon Business [26], o número de violações de dados aumentou significativamente em

2020, com um aumento de 11% em comparação a 2019. Os *hackers* podem usar uma variedade de técnicas para explorar vulnerabilidades de segurança em sistemas de informação, como destacado por Thomas e Kessler (2019) [25], incluindo ataques de força bruta, ataques de injeção de SQL, *phishing*, entre outros.

2.6 Habilidades e experiência dos desenvolvedores

As habilidades e a experiência dos desenvolvedores são fatores críticos na criação de *softwares* seguros. Payne et al. (2017) [22] afirmam que os desenvolvedores devem possuir conhecimentos em segurança da informação, além de habilidades técnicas em programação e outras áreas relacionadas. Além disso, é importante que os desenvolvedores estejam atualizados em relação às novas ameaças de segurança e técnicas de ataque.

Segundo uma pesquisa da SANS Institute, apenas 26% dos desenvolvedores de *software* acreditam que possuem habilidades suficientes em segurança cibernética [27]. Uma pesquisa da Veracode ainda revelou que 52% dos desenvolvedores acreditam que suas equipes não têm as habilidades necessárias para detectar e corrigir vulnerabilidades de segurança em software [28].

2.7 Ferramentas e metodologias de segurança

As ferramentas e metodologias de segurança são recursos essenciais para garantir a segurança dos *softwares*. Kizza (2015) [15] destaca a importância de ferramentas como análise estática de código, análise dinâmica de código, criptografia, autenticação e controle de acesso.

Além disso, metodologias como o modelo de ciclo de vida de desenvolvimento seguro (SDL) e o Processo de Segurança de Desenvolvimento de Aplicações são fundamentais para garantir que a segurança seja considerada desde o início do processo de desenvolvimento de *software*.

Essas metodologias fornecem orientações e práticas recomendadas para os desenvolvedores implementarem a segurança de maneira proativa, em vez de

reativa. Dessa forma, é possível minimizar a presença de vulnerabilidades e aumentar a eficácia das medidas de segurança implementadas.

2.8 Segurança por design (*security by design*)

O *Security by Design*, ou Segurança por Design em português, é uma abordagem de desenvolvimento de *software* que incorpora a segurança desde o início do processo de desenvolvimento. A ideia central é que a segurança deve ser considerada um elemento fundamental da arquitetura, *design* e implementação do *software*.

Esse conceito pode ser visto como uma extensão do princípio de “Pense em segurança desde o início”, que enfatiza a importância da segurança em todas as fases do processo de desenvolvimento de *software*, em vez de tentar corrigir problemas de segurança após a conclusão do *software*. O custo de corrigir uma vulnerabilidade de segurança em um sistema de *software* é muito maior do que corrigi-la antes do lançamento do produto.

Portanto, é crucial que os desenvolvedores considerem a segurança desde o início do processo de desenvolvimento [29].

A abordagem *Security by Design* oferece vários benefícios, incluindo:

- Maior segurança: Ao incorporar a segurança desde o início do processo de desenvolvimento, os desenvolvedores podem identificar e corrigir vulnerabilidades de segurança mais cedo, o que ajuda a reduzir o risco de ataques cibernéticos.
- Maior qualidade do software: Incorporar a segurança desde o início do processo de desenvolvimento pode garantir que o *software* seja mais confiável e de maior qualidade, ajudando a melhorar a reputação da empresa.
- Redução de custos: Corrigir vulnerabilidades de segurança após a conclusão do *software* pode ser muito mais caro do que corrigi-las durante o processo de desenvolvimento. O *Security by Design* pode ajudar a reduzir os custos de correção de vulnerabilidades de segurança.
- Conformidade regulatória: Muitas regulamentações de segurança exigem que os desenvolvedores incorporem a segurança desde o início do processo de

desenvolvimento de software. Ao seguir a abordagem S*ecurity by Design*, os desenvolvedores podem garantir a conformidade com essas regulamentações. [30]

2.9 Diretrizes de codificação segura

As diretrizes de codificação segura são um conjunto de práticas recomendadas para garantir que o software seja desenvolvido com segurança e proteção contra ameaças cibernéticas. Essas diretrizes visam reduzir o risco de vulnerabilidades de segurança em aplicativos e sistemas, protegendo dados e informações confidenciais.

A adoção dessas diretrizes pode ajudar a garantir a integridade, confidencialidade e disponibilidade dos dados em sistemas de software, tornando-os menos vulneráveis a ataques e invasões. As organizações devem estar cientes dessas diretrizes e implementá-las durante todo o processo de desenvolvimento de software para garantir que seus sistemas sejam seguros e protegidos contra ameaças cibernéticas.

Além disso, a adoção de diretrizes de codificação segura não é apenas benéfica para a segurança do software, mas também pode ser vantajosa do ponto de vista financeiro. Vulnerabilidades de segurança podem levar a violações de dados, roubo de informações confidenciais e perda de credibilidade com os clientes. A correção de falhas de segurança após uma violação pode ser extremamente cara, prejudicando a reputação da organização e resultando em multas e penalidades regulatórias. A implementação de práticas de codificação segura desde o início do processo de desenvolvimento pode ajudar a evitar esses custos desnecessários e minimizar os riscos para a organização.

A OWASP (*Open Web Application Security Project*) é uma organização sem fins lucrativos que se dedica a fornecer recursos e informações sobre segurança de aplicativos da web. Algumas das diretrizes de codificação segura relacionadas pela OWASP incluem:

- Validar todas as entradas: validar todas as entradas do usuário para evitar ataques de injeção de código malicioso, como SQL *Injection* e *Cross-Site Scripting* (XSS).

- Evitar a exposição de informações sensíveis: evitar a exposição de informações sensíveis, como senhas e dados pessoais, ao armazenar e transmitir dados de forma segura.
- Gerenciar a autenticação e autorização corretamente: gerenciar a autenticação e autorização corretamente para garantir que os usuários tenham acesso apenas ao que lhes é permitido.
- Proteger contra ataques de quebra de sessão: proteger contra ataques de quebra de sessão, como a falsificação de solicitações entre sites (CSRF) e a falsificação de solicitações direcionadas (CORS).
- Prevenir ataques de codificação incorreta: prevenir ataques de codificação incorreta, como ataques de *buffer overflow* e de desbordamento de inteiro.
- Implementar medidas de segurança no código: implementar medidas de segurança no código, como controle de acesso, auditoria de log e detecção de intrusão.
- Realizar testes de segurança: realizar testes de segurança regulares para identificar e corrigir vulnerabilidades no *software*.
- Manter a segurança ao atualizar o *software*: garantir que as atualizações de *software* sejam realizadas com segurança, para evitar vulnerabilidades em potencial.

Essas são algumas das diretrizes de codificação segura relacionadas pela OWASP que podem ser implementadas para proteger *softwares* contra ameaças de segurança.

2.10 Trabalhos relacionados

Este subtópico apresenta uma revisão bibliográfica sobre a educação em segurança da informação no desenvolvimento de *software*, baseada em três artigos relevantes sobre o tema.

O primeiro artigo, intitulado "*Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey*" [13], investigou a necessidade de educação em segurança da informação para profissionais de desenvolvimento de *software*.

O segundo artigo, "'*Think secure from the beginning': A Survey with Software Developers*" [14], apresentou uma pesquisa com desenvolvedores de *software* sobre a importância da segurança da informação no processo de desenvolvimento de *software*.

O terceiro artigo, "*The changing face of software security 2021 - Whitepaper*" [31], destaca a importância da segurança da informação no desenvolvimento de *software* em um cenário de aumento de ameaças cibernéticas.

2.10.1 *Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey*

Bruce Schneier, um grande pesquisador de segurança, baseado em um estudo de Patel et al. [33], afirmou que menos de 50% dos desenvolvedores de software podem identificar possíveis vulnerabilidades de segurança em software [34]. Além disso, uma estimativa do Departamento de Segurança dos Estados Unidos, por volta de 90% dos incidentes de segurança relatados resultam de explorações contra defeitos no projeto ou código do *software*. Junto a esses fatos, o *software* está cada vez mais complexo e maior. De fato, um estudo recente da Sourcegraph [35] mostra que mais de 80% dos desenvolvedores estão lidando com 20 vezes mais código do que há anos atrás.

Em um estudo recente, Assal et al. [14] levantaram como os desenvolvedores são influenciados e influenciam os processos de codificação segura. O estudo apresentado em [13] fez um levantamento da importância da codificação segura no contexto da indústria de *software*.

O artigo "*Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey*" é uma investigação realizada por Tiago Gasiba, Maria Pinto Albuquerque e Daniel Méndez Fernández, que teve em vista responder à pergunta se a educação em codificação segura é necessária na indústria.

A pesquisa foi realizada por meio de uma grande escala de questionários, enviados a profissionais da indústria de desenvolvimento de *software*. Os resultados mostraram que a maioria dos entrevistados acredita que a educação em codificação segura é necessária e a falta dela pode ter consequências negativas para a

segurança do *software*. Além disso, os resultados mostraram que os profissionais consideram que a educação em codificação segura deveria ser uma parte integrante dos currículos de ciência da computação e engenharia de *software*.

A segurança do *software* é uma preocupação constante na indústria de desenvolvimento de *software*, especialmente em um cenário cada vez mais conectado e com o aumento constante de ameaças cibernéticas. Nesse sentido, a educação em codificação segura surge como uma necessidade para garantir que os profissionais de desenvolvimento de *software* estejam preparados para lidar com os desafios de segurança.

O estudo traz alguns dados importantes para contextualizarmos.

- Foram enviados questionários para 9.305 profissionais da indústria de desenvolvimento de *software*, e 843 respostas foram recebidas, representando uma taxa de resposta de 9,07%.
- 77,2% dos entrevistados acreditam que a educação em codificação segura é necessária na indústria de desenvolvimento de *software*.
- 82,4% dos entrevistados acreditam que a falta de educação em codificação segura pode ter consequências negativas para a segurança do *software*.
- 85,7% dos entrevistados acreditam que a educação em codificação segura deve ser uma parte integrante dos currículos de ciência da computação e engenharia de *software*.

Os tópicos considerados mais importantes para a educação em codificação segura são: injeção de SQL (67,6%), gerenciamento de autenticação e autorização (59,6%) e gerenciamento de vulnerabilidades (55,7%). As principais razões apontadas para a falta de educação em codificação segura são: falta de tempo (46,4%), falta de recursos financeiros (43,9%) e falta de conscientização sobre a importância da codificação segura (42,2%).

Conforme o estudo, a maioria dos profissionais da indústria de desenvolvimento de *software* acredita que a educação em codificação segura é necessária e a falta dela pode ter consequências negativas para a segurança do *software*. Além disso, os resultados mostraram que os profissionais consideram que

a educação em codificação segura deveria ser uma parte integrante dos currículos de ciência da computação e engenharia de *software*.

Esses resultados apontam para a necessidade de investimentos em educação em codificação segura, tanto por parte das empresas de desenvolvimento de *software* como das instituições de ensino. As empresas devem investir em programas de treinamento e conscientização em codificação segura para seus funcionários, a fim de garantir que eles estejam preparados para lidar com as ameaças de segurança. Além disso, as instituições de ensino devem incluir a educação em codificação segura como uma parte integrante dos currículos de ciência da computação e engenharia de *software*, a fim de preparar os futuros profissionais para lidar com os desafios de segurança.

2.10.2 *Think secure from the beginning': A Survey with Software Developers*

O artigo "*Think Secure from the Beginning: A Survey with Software Developers*" [14] de Hala Assal e Sonia Chiasson é um estudo que busca entender como os desenvolvedores de *software* lidam com a segurança desde o início do processo de desenvolvimento de *software*. O estudo foi realizado por meio de uma pesquisa *on-line* com desenvolvedores de *software* de diferentes organizações e setores.

Os resultados mostraram que a maioria dos desenvolvedores acredita que a segurança da informação é importante no desenvolvimento de *software*, mas muitos deles acham difícil implementar práticas de segurança da informação no processo de desenvolvimento de *software*. Além disso, o estudo destacou a importância de uma abordagem proativa em relação à segurança da informação desde o início do processo de desenvolvimento de *software*.

O artigo apresenta os seguintes dados obtidos a partir da pesquisa com desenvolvedores de *software*:

- 71,1% dos desenvolvedores relataram que suas organizações têm políticas de segurança de *software*, mas apenas 26,7% deles receberam treinamento em segurança de *software* durante a contratação.

- 62,2% dos desenvolvedores disseram que a segurança de *software* é uma responsabilidade compartilhada entre a equipe de desenvolvimento e a equipe de segurança, enquanto 29,3% acreditam que a segurança é uma responsabilidade exclusiva da equipe de segurança.
- 63,9% dos desenvolvedores disseram que a segurança é considerada apenas quando os recursos e prazos permitem, enquanto apenas 18,4% disseram que a segurança é sempre considerada desde o início do processo de desenvolvimento.
- 70,3% dos desenvolvedores relataram usar ferramentas automatizadas de segurança para detectar problemas de segurança em seus *softwares*.
- 56,9% dos desenvolvedores disseram que as práticas de segurança variam significativamente entre as equipes de desenvolvimento em suas organizações.

O estudo revela que muitos desenvolvedores têm uma compreensão limitada sobre segurança cibernética e segurança de *software*, e que a maioria deles se concentra mais em recursos e prazos do que na segurança quando desenvolvem *software*. Isso demonstra a necessidade de uma mudança cultural na indústria de desenvolvimento de *software*, onde a segurança cibernética seja vista como uma prioridade igualmente importante para recursos e prazos.

Além disso, a pesquisa mostra que os desenvolvedores têm pouco treinamento em segurança e muitas vezes dependem de ferramentas automatizadas de segurança para detectar problemas de segurança. Isso destaca a necessidade de mais treinamento em segurança para os desenvolvedores de *software* e uma maior conscientização sobre a importância da segurança cibernética desde o início do processo de desenvolvimento de *software*.

Os autores do estudo enfatizam que a segurança deve ser uma consideração crítica desde o início do processo de desenvolvimento e que deve ser uma responsabilidade compartilhada por toda a equipe de desenvolvimento. Isso significa que a segurança cibernética deve ser incorporada em todas as etapas do processo de desenvolvimento, desde o planejamento até o teste e a implementação.

Além disso, a pesquisa revela que as práticas de segurança variam significativamente entre as organizações e que muitas vezes não há padrões ou políticas de segurança claras. Isso destaca a importância de se ter padrões e políticas de segurança, claros e aplicáveis em todas as organizações de desenvolvimento de *software*.

Em suma, a segurança cibernética deve ser uma consideração crítica desde o início do processo de desenvolvimento. Isso envolve a mudança cultural na indústria de desenvolvimento de *software* para priorizar a segurança cibernética, fornecer treinamento em segurança para os desenvolvedores de *software* e garantir que as práticas de segurança sejam consistentes e padronizadas em todas as organizações de desenvolvimento de *software*. A incorporação da segurança cibernética desde o início do processo de desenvolvimento de *software* é crucial para garantir a proteção dos dados e informações confidenciais dos usuários e das empresas.

2.10.3 *The changing face of software security 2021 - Whitepaper*

O relatório "*Shifting from reaction to prevention: The changing face of software security 2021*" [31] é um *whitepaper* que aborda as mudanças no cenário da segurança de *software*, especialmente no que diz respeito à mudança do foco reativo para o preventivo.

O relatório discute a importância da segurança de *software* e como ela se tornou um elemento crítico para organizações de todos os tamanhos. Ele examina os desafios enfrentados pelas empresas na tentativa de garantir a segurança de seus sistemas de *software*, incluindo as ameaças cada vez mais sofisticadas de *hackers* e outros cibercriminosos.

O relatório também discute como as empresas estão mudando suas abordagens para a segurança de *software*, adotando cada vez mais abordagens proativas e preventivas em vez de simplesmente reagir a incidentes de segurança. Ele discute o papel das ferramentas de segurança de *software* automatizadas e da integração contínua e entrega contínua (CI/CD) na prevenção de vulnerabilidades de segurança.

Por fim, o relatório destaca a importância da colaboração entre desenvolvedores, operações e equipes de segurança em garantir a segurança de *software* em toda a organização. Ele fornece recomendações práticas para as empresas que buscam adotar uma abordagem preventiva para a segurança de *software* e se preparar para os desafios futuros.

O relatório apresentou alguns resultados interessantes em relação à segurança de *software*. Alguns deles incluem:

- A segurança de *software* é uma preocupação crescente para empresas de todos os tamanhos, com 80% dos entrevistados afirmando que a segurança de *software* é muito importante ou extremamente importante para sua organização.
- As empresas estão mudando sua abordagem para a segurança de *software*, com 56% dos entrevistados relatando que estão adotando uma abordagem mais proativa e preventiva em relação à segurança de *software*, em vez de apenas reagir a incidentes.
- As ferramentas de segurança de *software* automatizadas estão se tornando cada vez mais populares, com 74% dos entrevistados afirmando que estão usando ferramentas de segurança de *software* automatizadas para identificar vulnerabilidades de segurança em seus sistemas.
- A integração contínua e entrega contínua (CI/CD) está se tornando cada vez mais comum, com 80% dos entrevistados afirmando que estão usando CI/CD em seus processos de desenvolvimento de *software*.
- A colaboração entre desenvolvedores, operações e equipes de segurança é crucial para garantir a segurança de *software* em toda a organização, com 68% dos entrevistados afirmando que estão trabalhando em estreita colaboração entre essas equipes.
- As empresas estão investindo cada vez mais em segurança de *software*, com 73% dos entrevistados relatando que planejam aumentar seus investimentos em segurança de *software* nos próximos 12 meses.

O relatório "*Shifting from reaction to prevention: The changing face of software security 2021*" [31] destaca a importância da abordagem proativa e preventiva para a segurança de *software*. Nesse sentido, a integração contínua e entrega contínua

(CI/CD) surge como uma técnica fundamental para garantir que os sistemas de *software* estejam sempre seguros e atualizados.

A CI/CD é uma abordagem de desenvolvimento de *software* que envolve a entrega contínua de *software* em pequenas quantidades, em vez de grandes lançamentos periódicos. Isso permite que as empresas detectem e corrijam rapidamente vulnerabilidades de segurança, além de melhorar a qualidade geral do *software*.

No entanto, para implementar com sucesso a CI/CD, as empresas precisam investir em ferramentas de automação e testes para garantir que as alterações de código sejam seguras e confiáveis. É necessário também que as equipes de desenvolvimento, operações e segurança trabalhem em estreita colaboração, de forma que todas as partes tenham um entendimento claro dos riscos de segurança associados às alterações de código.

Conforme o relatório [31], apenas 24% dos entrevistados afirmaram que suas organizações oferecem treinamento em segurança de *software* para todos os desenvolvedores de *software*. Além disso, somente 26% dos entrevistados afirmaram que suas organizações têm uma equipe dedicada à segurança de *software*.

Esses dados sugerem haver uma necessidade urgente de melhorar o treinamento em segurança de *software* para desenvolvedores de *software*. É essencial que as empresas invistam em treinamento e educação em segurança de *software* para garantir que todos os desenvolvedores estejam cientes dos riscos de segurança associados ao desenvolvimento de *software* e possam desenvolver códigos seguros desde o início do processo de desenvolvimento.

Além disso, o mesmo relatório destaca a importância de dar *feedback* imediato aos desenvolvedores de *software* sobre vulnerabilidades de segurança em seu código. Cerca de 67% dos entrevistados afirmaram que suas organizações dão *feedback* imediato sobre vulnerabilidades de segurança aos desenvolvedores, o que é um passo importante para garantir que os desenvolvedores possam corrigir vulnerabilidades de segurança o mais rapidamente possível. As empresas que investem em treinamento em segurança de *software* e fornecem *feedback* imediato

aos desenvolvedores estão em uma posição melhor para garantir a segurança de seus sistemas de *software* e minimizar o risco de violações de segurança.

2.10.4 Comparativo entre base teórica e pesquisa

Neste item podemos fazer uma comparação mais simples entre os itens da base teórica 2.10.1 e 2.10.2 que foram as inspirações para o survey e os quais compararemos os resultados na parte de resultados deste documento.

Quadro 2 – Quadro comparativo entre esta pesquisa e base teórica.

	Esta pesquisa	**GASIBA et al. (item 2.10.1)**	**ASSAL e CHIASSON (item 2.10.2)**
Tema	Educação em codificação segura na indústria local	Necessidade de educação em codificação segura	Desafios enfrentados pelos desenvolvedores na implementação de práticas de segurança
Metodologia	Pesquisa por meio de survey online	Grande pesquisa por meio de um questionário	Pesquisa com desenvolvedores de software por meio de entrevistas
Amostra	Profissionais da indústria de software local	Profissionais da indústria de software	Desenvolvedores de software
Foco principal	Percepção da necessidade de educação em codificação segura	Percepção da necessidade de educação em codificação segura	Desafios específicos na implementação de práticas de segurança
Resultados principais	Falta de educação em codificação segura, falta de recursos dedicados, falta de conscientização dos desenvolvedores	Falta de recursos dedicados, falta de conscientização dos desenvolvedores, falta de adesão a padrões de segurança	Falta de treinamento em segurança, falta de documentação, falta de tempo para implementar práticas de segurança

Contribuição principal	Identificação das necessidades de educação em codificação segura na indústria local de software	Grande escala de pesquisa que confirma a falta de recursos e conscientização em relação à segurança	Identificação de desafios específicos enfrentados pelos desenvolvedores na implementação de práticas de segurança
Limitações principais	Tamanho da amostra pequeno, limitado a empresas locais	Limitado a profissionais de software, pode não representar a indústria de software como um todo	Limitado a uma amostra específica de desenvolvedores

Neste quadro fica fácil identificar lacunas e oportunidades de pesquisa em relação aos outros estudos. Por exemplo, pode-se observar que o estudo proposto por essa pesquisa é semelhante ao de GASIBA et al. em relação ao foco na percepção de profissionais da indústria de *software*, mas difere em relação ao tamanho da amostra e à metodologia utilizada. Essa diferença pode representar uma oportunidade para aprofundar ainda mais a discussão sobre a necessidade de educação em codificação segura na indústria, com uma amostra diferente e uma abordagem metodológica distinta.

Por outro lado, se pode notar que o estudo de ASSAL e CHIASSON se concentrou em desafios específicos enfrentados pelos desenvolvedores de *software* na implementação de práticas de segurança, o que pode ser uma área interessante para explorar ainda mais em uma futura pesquisa. Este quadro pode, portanto, ajudar a identificar as principais contribuições e limitações de cada um dos estudos e como sua pesquisa pode se beneficiar dessas informações.

Além disso, o estudo de GASIBA et al. (2019) também abordou a importância da educação em codificação segura na indústria de *software*, assim como o Trabalho de Conclusão em questão. No entanto, diferentemente do estudo de ASSAL e CHIASSON (2019), que se concentrou em desenvolvedores de *software* específicos, o estudo de GASIBA et al. (2019) buscou uma amostra mais ampla de profissionais de TI de diferentes países e setores. Em termos de semelhanças, ambos os estudos destacaram a falta de conhecimento em segurança cibernética e

a necessidade de treinamento em codificação segura para os profissionais de TI. Entretanto, enquanto o estudo de GASIBA et al. (2019) se concentrou em explorar as principais barreiras para a implementação de treinamentos em codificação segura, a pesquisa em questão buscou investigar especificamente a percepção dos profissionais de TI em relação à necessidade de educação em codificação segura na indústria local de *software*.

Outra diferença importante é que o estudo de ASSAL e CHIASSON (2019) apresentou um foco específico em como os desenvolvedores de *software* pensam sobre a segurança cibernética e como isso influencia seu trabalho diário. Por outro lado, o trabalho de conclusão em questão buscou investigar mais amplamente a percepção dos profissionais de TI em relação à necessidade de educação em codificação segura, incluindo gerentes de projeto e outros profissionais envolvidos no processo de desenvolvimento de *software*.

Neste próximo quadro seguirá uma visão bem resumida dos resultados coletados que serão discutidos na seção 4 deste documento.

Quadro 3 – Quadro comparativo quanto aos resultados com essa pesquisa e base teórica.

Artigo	Resultados Obtidos
Esta pesquisa	A maioria dos participantes concorda que a educação em codificação segura é necessária na indústria de software. A principal barreira para a implementação de treinamentos em codificação segura é a falta de tempo e recursos financeiros.
GASIBA et al. (2019) (item 2.10.1)	A maioria dos participantes concorda que a educação em codificação segura é necessária na indústria de software. A principal barreira para a implementação de treinamentos em codificação segura é a falta de apoio dos gerentes de projeto.
ASSAL e CHIASSON (item 2.10.2)	A maioria dos desenvolvedores de software concorda que a segurança cibernética é importante. No entanto, muitos não se sentem confiantes em sua habilidade de escrever código

	seguro. Eles também destacaram que a pressão para concluir projetos no prazo pode afetar negativamente a segurança cibernética.

Observa-se que, de acordo com a revisão bibliográfica realizada, a educação em codificação segura é considerada um aspecto crucial para a segurança cibernética. No entanto, diferentes estudos apontam para diferentes barreiras que impedem a implementação de treinamentos efetivos na indústria de *software*. Enquanto o trabalho em questão enfatiza a falta de tempo e recursos financeiros como principal obstáculo, GASIBA et al. (2019) destaca a falta de apoio dos gerentes de projeto como um fator crítico. Já o estudo de ASSAL e CHIASSON (2019) ressalta que a pressão por concluir projetos no prazo pode ter impactos negativos na segurança cibernética.

Outro ponto a ser destacado é a falta de confiança dos desenvolvedores em suas habilidades para escrever código seguro, o que indica a necessidade de abordagens mais específicas para melhorar a educação em segurança cibernética. Enquanto esta pesquisa e o estudo de GASIBA et al. (2019) não trataram diretamente dessa questão, o estudo de ASSAL e CHIASSON (2019) enfatiza essa preocupação.

Apesar das diferenças nos resultados e no escopo da pesquisa, todos os estudos ressaltam a importância da educação em codificação segura e indicam que ainda há desafios significativos a serem superados para a implementação de treinamentos efetivos na indústria de *software*.

3 MÉTODO DE PESQUISA

3.1 Natureza e classificação da pesquisa

De acordo com Andrade (2010, p.126) [36], “pesquisa é o conjunto de procedimentos sistemáticos, baseado no raciocínio lógico, cujo objetivo é encontrar soluções para problemas propostos, mediante a utilização de métodos científicos. Pesquisar é realizar uma série de coleta, interpretação baseada em métodos com o objetivo de sintetizar respostas sobre um determinado material de estudo.”

Assis (2009, p. 17) [37], traz o seguinte conceito sobre natureza de pesquisa básica:

> “Busca o progresso da ciência e tem por objetivo adquirir conhecimentos científicos, sem interessar-se por suas aplicações e consequências práticas. Seu desenvolvimento tende a ser bastante formalizado e tem como objetivo a generalização, visando à construção de teorias e leis;”.

Partindo desta definição, conforme a natureza da pesquisa, ela classifica-se como básica, pois tem como objetivo o avanço do conhecimento em uma determinada área, sem necessariamente buscar uma aplicação prática imediata.

A pesquisa será do tipo exploratória. A pesquisa exploratória permite uma maior compreensão sobre o tema estudado, e a abordagem quantitativa permite a análise dos dados coletados de maneira objetiva e estatística.

De acordo com Gil (2002, p.41) [38], as pesquisas exploratórias tendem a ser mais flexíveis em seu planejamento, pois pretendem observar e compreender os mais variados aspectos relativos ao fenômeno estudado pelo pesquisador. Ainda de acordo com Gil (2002, p.42) [38], ressalta que o estudo descritivo tem como objetivo primordial a descrição das características de determinada população ou fenômeno.

Neuman (2003) define pesquisa quantitativa da seguinte forma: “A pesquisa quantitativa pode ser descrita como uma tentativa de examinar a relação entre variáveis por meio da coleta sistemática e análise de dados quantitativos.” [39]. Devido ao uso de *Survey* de pesquisa com predominância de perguntas fechadas

para uma coleta de dados, essa pesquisa teve como abordagem quantitativa o tratamento dos dados.

Segundo Medeiros (2019) [40], a pesquisa de levantamento é um tipo de pesquisa que se realiza para a obtenção de dados ou informações sobre características, ou opiniões de um grupo de pessoas, selecionado como representante de uma população (em termos estatísticos).

Quadro 4 – Dados de classificação da pesquisa.

Natureza da pesquisa:	Básica
Tipo da Pesquisa:	Exploratória
Abordagem da pesquisa:	Quantitativa
Técnica de coleta de dados:	Pesquisa de levantamento

3.2 Ética

A pesquisa será conduzida conforme os princípios éticos da pesquisa científica, com a garantia da confidencialidade dos dados coletados e a proteção da privacidade dos participantes. Será obtido o consentimento informado dos participantes e a participação na pesquisa será voluntária e sem qualquer tipo de pressão.

Os dados coletados serão utilizados exclusivamente para fins da pesquisa e não serão divulgados ou compartilhados com terceiros. A pesquisa será realizada imparcialmente e sem qualquer tipo de influência externa.

3.3 Forma de abordagem e coleta de dados

Para a coleta de dados, serão realizados convites para participação na pesquisa por meio de redes sociais, grupos de discussão e e-mails direcionados a empresas da área de desenvolvimento de *software*. O convite incluirá um link para o *Survey* online no Google Forms. Os participantes serão informados sobre os objetivos da pesquisa e assegurados sobre a confidencialidade dos dados

coletados. A participação na pesquisa será voluntária e os participantes poderão desistir a qualquer momento.

O instrumento de coleta de dados utilizado será um *Survey* elaborado de forma online no Google Forms. O *Survey* será composto por questões fechadas e abertas, com o objetivo de obter informações sobre a necessidade do ensino de codificação segura na indústria de *software*, bem como identificar a percepção dos profissionais da área em relação a esse tema.

Mattar (1996, p. 48) [41], assim conceitua:

> "Dados primários: são aqueles que não foram antes coletados, estando ainda em posse dos pesquisados, e que são coletados com o propósito de atender às necessidades específicas da pesquisa em andamento. As fontes básicas de dados primários são: pesquisado (sic), pessoas que tenham informações sobre o pesquisado e situações similares".

Para a realização deste trabalho de conclusão e pesquisa foram utilizados dados de fontes primárias, uma vez que temos em posse, através do *Survey* aplicado, dados ainda não estudados.

A população desta pesquisa é composta por profissionais da área de desenvolvimento de *software*. Para a definição da amostra, foi utilizado o método de amostragem não probabilística por conveniência, em que a seleção dos participantes foi feita de forma voluntária e por meio de convite online para participação na pesquisa.

Para a conclusão deste trabalho e pesquisa, as informações foram obtidas de maneira sensata por meio de *Survey* aplicado com 51 questões relacionadas ao assunto do estudo, sendo esse *Survey* aplicado junto a profissionais das empresas de *software* local, tendo sido convidados remotamente a responderem o *Survey*. O *Survey* foi aplicado entre 08 de março de 2023 até 4 de abril de 2023, o convite aos participantes foi feito através de lista de e-mail da UFPE, grupos de *WhatsApp*, grupos de *Facebook* voltados para a área de SI e *Classroom* da disciplina de Auditoria e Segurança.

O *Survey* desenvolvido neste trabalho (Apêndice A) foi inspirado nos questionários aplicados em dois outros artigos, o "*Is Secure Coding Education in the*

Industry Needed? An Investigation Through a Large Scale Survey" [13] e o "*Think secure from the beginning": A Survey with Software Developers* [14] que tratam do mesmo escopo de problema, porém a primeira foi uma pesquisa global aplicada a várias indústrias e a segunda foi realizada com desenvolvedores da América do Norte, então a ideia foi traduzir ambos questionários (Anexo A e Anexo B), levantar junto as perguntas que mais faziam sentido para nossa pesquisa local, validar com a orientadora e reorganizar para aplicação na indústria de *software* local. No primeiro artigo o objetivo dele vai em total concordância com o objetivo deste trabalho que é investigar a conformidade dos desenvolvedores com as diretrizes de codificação segura e levantar a necessidade do ensino de codificação segura na indústria.

Participaram do estudo 38 funcionários de empresas de *software* da indústria local. Do qual 71% atua diretamente no desenvolvimento de *software*. Com relação aos dados demográficos, 34,2% da amostra tem entre 3 e 5 anos de experiência no ramo e 42,1% utilizam a linguagem de programação Java.

De forma geral, o objetivo do *Survey* aplicado neste estudo é realizar uma pesquisa sobre o estado atual do ensino sobre desenvolvimento de *software* seguro do ponto de vista dos profissionais de Engenharia de *Software* no contexto da indústria local de *software.* Com esse estudo será possível traçar orientações sobre como melhorar a educação voltada para a codificação segura nas empresas.

3.4 Ameaças a validade

PERRY et al. (2000) [42] define ameaças à validade de um estudo empírico como sendo as influências que podem limitar nossa capacidade de interpretar ou tirar conclusões a partir de dados do estudo.

De acordo com Wohlin et al. (2012) [43], uma questão fundamental a respeito dos resultados de uma pesquisa é se estes resultados são realmente válidos. A validade dos resultados deve ser levada em consideração já na fase de planejamento do estudo, pois esta questão pode influenciar sobremaneira a validade do resultado.

De acordo com Campbell e Stanley (1963) [44] e Cook e Campbell (1979) [45], existem quatro tipos de ameaças à validade de um experimento:

- Validade de conclusão: possibilidade de tirar conclusões imprecisas das observações;
- Validade Interna: ameaças que podem ter afetado os resultados e não foram devidamente levadas em conta;
- Validade de construção: ameaças sobre a relação entre a teoria e a observação;
- Validade externa: ameaças que afetam a generalização dos resultados.

A principal ameaça à Validade de construção em pesquisas por meio de questionários é a possibilidade de os participantes não entenderem corretamente as perguntas, o que poderia impactar nos resultados. Para lidar com isso, o questionário foi enviado antecipadamente a um colega profissional da área de segurança e para orientadora, para identificar possíveis pontos de confusão ou mal-entendidos.

Em relação à validade interna, o número de respostas (38) pode ser identificado como uma ameaça, já que as opiniões daqueles que não participaram podem ter influenciado os resultados. Além disso, se considerarmos que as atividades desenvolvidas nas empresas são bem diferentes entre empresas e projetos, um grande número de respostas de participantes do mesmo projeto ou da mesma empresa podem afetar os resultados. No entanto, consideramos o número de respostas e a diversidade dos participantes uma boa base para uma visão geral do tema abordado por esse trabalho.

Existem ainda outras duas ameaças potenciais à validade desta pesquisa que devem ser consideradas. A primeira é o uso de questionários que já foram aplicados em pesquisas anteriores e validados em pesquisas internacionais. Essa ameaça é conhecida como ameaça de validade externa, pois a validade da pesquisa pode ser afetada pela generalização dos resultados para uma população diferente daquela em que o questionário foi originalmente validado.

A segunda ameaça é o uso de um questionário muito extenso, que pode fazer com que o participante da pesquisa perca o foco ou perca o interesse em responder

às perguntas com precisão. Essa ameaça é conhecida como ameaça de validade interna, pois pode afetar a validade dos resultados da pesquisa devido a possíveis erros nos dados coletados.

3.5 Desenvolvimento do Survey

O desenvolvimento do *survey* para pesquisa acadêmica é uma etapa crucial em qualquer estudo científico. Para criar um *survey* que seja válido, confiável e capaz de coletar informações precisas, é necessário seguir algumas etapas importantes. Primeiramente, foi essencial definir claramente o objetivo da pesquisa e as perguntas que seriam abordadas. Em seguida, foram selecionadas as perguntas e formatos de resposta adequados para obter as informações necessárias, levando em consideração a clareza, especificidade e relevância das perguntas.

Além disso, é fundamental avaliar a extensão do *survey* e garantir que ele não seja excessivamente longo ou tedioso para o participante, por esse motivo foram descartadas no momento da criação deste *survey* diversas perguntas que caberiam no escopo deste estudo. Por fim, foi realizada uma validação junto a professora orientadora e um colega especialista de segurança para garantir que as perguntas fossem compreendidas corretamente e que as respostas fossem facilmente interpretadas. Seguindo essas etapas, pode-se desenvolver um *survey* eficaz para coletar informações precisas e confiáveis.

Como mencionado anteriormente nosso *survey* foi elaborado baseado em dois outros artigos, no apêndice B segue um quadro de rastreamento informando se foi original ou se a pergunta veio de algum dos dois artigos.

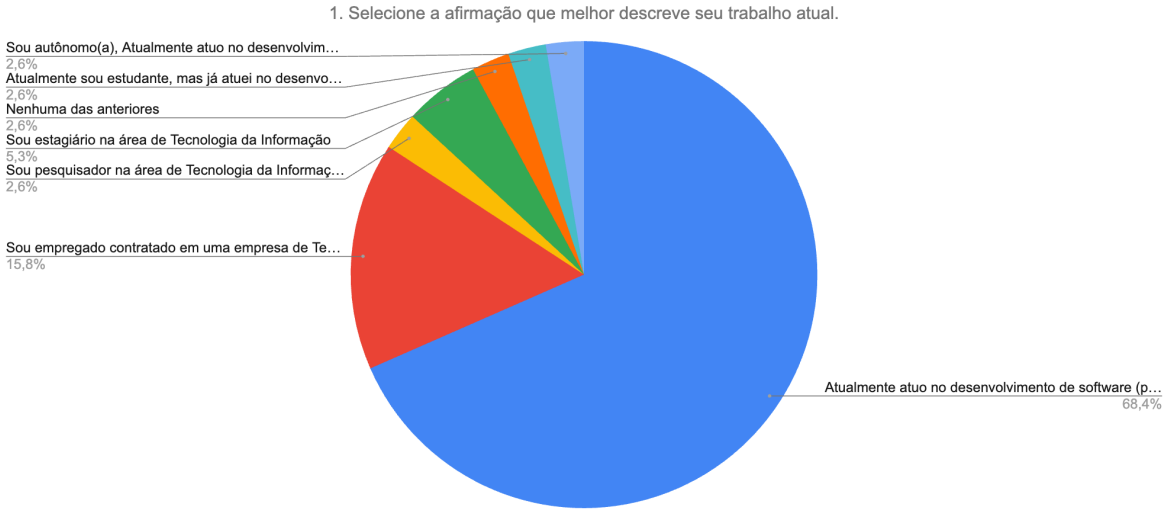
4 RESULTADOS DA PESQUISA E DISCUSSÃO

Nesta seção serão apresentados os resultados obtidos a partir da coleta de dados realizada por meio de um *survey online* respondido por 38 funcionários de empresas de *software* da indústria local. As respostas foram analisadas a fim de verificar o nível de conhecimento e aderência às práticas de codificação segura por parte dos entrevistados e a necessidade do ensino de codificação segura na indústria, o formulário ficou disponível para recebimento de respostas por 27 dias, compreendo o período entre 08 de março de 2023 e 04 de abril de 2023.

A primeira pergunta da pesquisa tinha como objetivo saber qual é o trabalho atual dos participantes. Pelos dados que você coletados, pode-se observar que a grande maioria dos entrevistados (32 dos 38) é empregada contratada em uma empresa de Tecnologia da Informação, sendo que a maioria delas (26 dos 32) atua no desenvolvimento de software, como programadores, desenvolvedores, desenvolvedores web ou engenheiros de software. Dois entrevistados afirmaram ser estagiários na área de Tecnologia da Informação, um trabalha como desenvolvedor de software de forma autônoma e apenas um deles se descreveu como pesquisador na área de TI.

A maioria dos participantes estão envolvidos na área de TI, atuando diretamente com desenvolvimento de código, fortalecendo os dados fornecidos nesta pesquisa.

Gráfico 1 – Resultados coletados da pergunta 1 do Survey



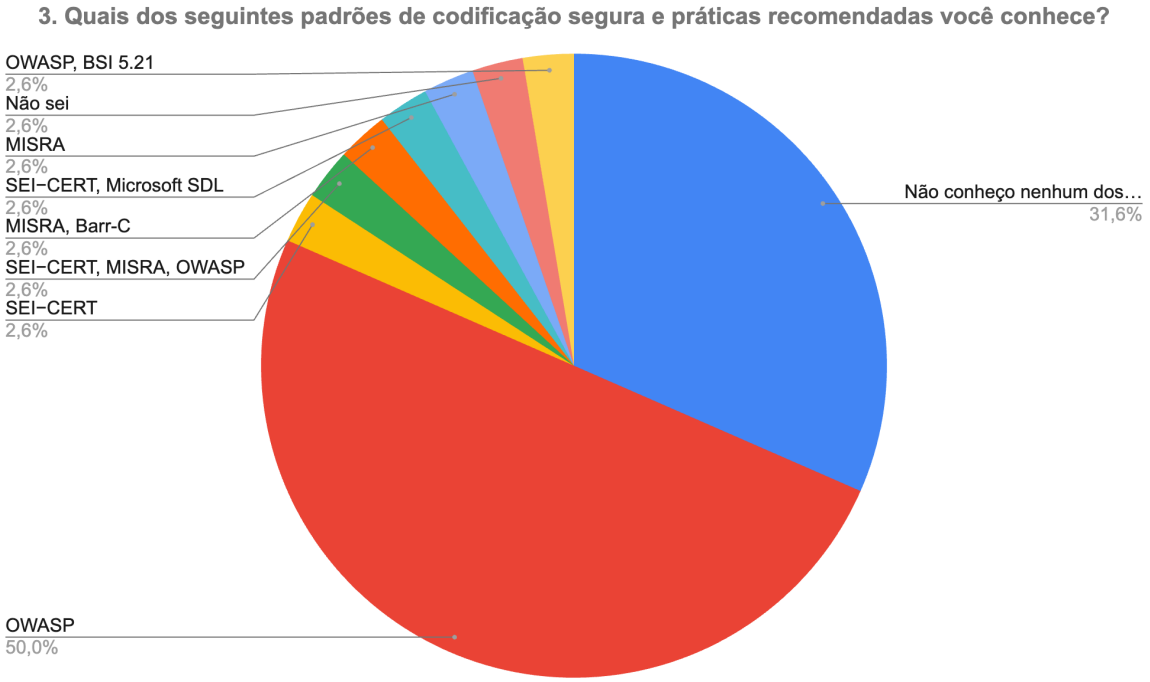
Fonte: O autor (2023).

Na pergunta 3 da pesquisa, buscamos avaliar o conhecimento dos correspondentes em relação aos padrões de codificação segura e práticas recomendadas. Dos padrões mencionados, o OWASP foi o mais conhecido, sendo citado por 22 dos 38 participantes. Por outro lado, um número significativo de participantes afirmou não conhecer nenhum dos padrões mencionados, totalizando 12 participantes.

Dentre os outros padrões mencionados, o SEI-CERT foi citado por duas pessoas, o MISRA foi citado por 3 participantes, enquanto o Barr-C, BSI 5.21 e Microsoft SDL foram citados por apenas um participante cada, além de um participante responder que não conhecia nenhum dos padrões mencionados.

Embora o OWASP seja amplamente conhecido na comunidade de desenvolvedores, é preocupante que uma parcela significativa dos participantes afirme não conhecer nenhum dos padrões de codificação segura mencionados. Esses resultados podem indicar uma falta de conscientização e conhecimento em relação às melhores práticas de segurança.

Gráfico 2 – Resultados coletados da pergunta 3 do Survey



Fonte: O autor (2023).

A pergunta 4 buscou avaliar a experiência de trabalho em tecnologia da informação dos participantes. Dos 38 participantes, a maioria (12) possui entre 3 e 5 anos de experiência, seguido por 12 participantes que possuem mais de 10 anos de experiência, além disso, 8 participantes possuem entre 6 e 10 anos de experiência e apenas 5 participantes possuem menos de 3 anos de experiência em TI.

É importante destacar que, em geral, quanto maior a experiência de um profissional de TI, maior a sua capacidade de identificar e solucionar problemas complexos. Por outro lado, profissionais mais jovens tendem a ter uma visão mais atualizada e dinâmica sobre as tecnologias em uso, o que pode ser útil na implementação de novas soluções de segurança.

Em relação à pesquisa, é possível inferir que a maioria dos participantes possui uma vasta experiência em TI, o que pode ser benéfico para aplicação de melhores práticas de segurança no momento do desenvolvimento do *software*. No entanto, é importante garantir que esses profissionais estejam atualizados em relação às novas tendências e tecnologias, e estejam dispostos a adotar mudanças em suas práticas para garantir a segurança.

Gráfico 3 – Resultados coletados da pergunta 4 do Survey

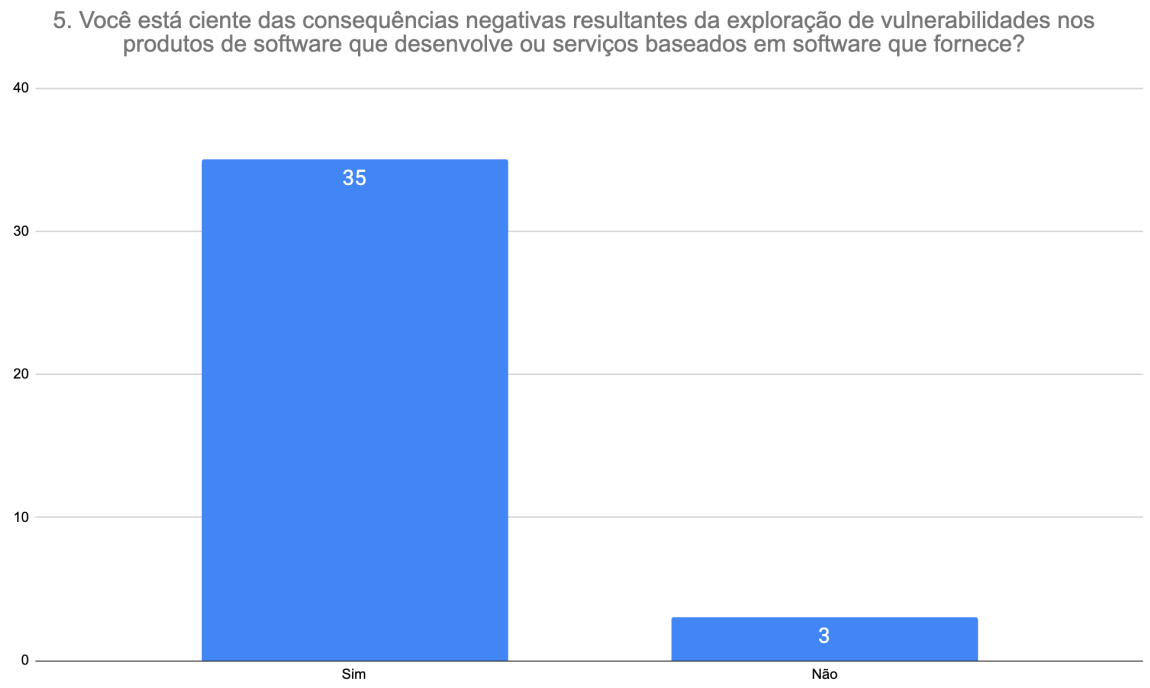
Fonte: O autor (2023).

A pergunta 5 de nossa pesquisa teve em vista avaliar se os participantes estavam cientes das consequências negativas resultantes da exploração de vulnerabilidades nos produtos de *software* que desenvolvem ou serviços baseados em *software* que fornecem. Dos 38 participantes, 35 afirmaram estar cientes dessas consequências, enquanto apenas 3 afirmaram não estar cientes.

Esses resultados indicam que a grande maioria (92,1%) dos profissionais de desenvolvimento estão cientes das consequências negativas da exploração de vulnerabilidades em seus produtos e serviços. Este é um resultado positivo, ao indicar que esses profissionais reconhecem a importância da segurança do *software*.

No entanto, é importante ressaltar que ainda há uma pequena parcela (7,9%) de profissionais que não estão cientes das consequências negativas da exploração de vulnerabilidades. Isso pode refletir falta de conscientização e educação em relação à segurança do *software*, o que pode levar a produtos e serviços vulneráveis e expostos a ameaças de segurança.

Gráfico 4 – Resultados coletados da pergunta 5 do Survey



Fonte: O autor (2023).

As perguntas 7, 8 e 9 foram avaliadas através da escala de Likert, que variava de 1 a 5, sendo 1 “Discordo Totalmente” e 5 “Concordo Totalmente”.

As três perguntas tratam da percepção dos participantes sobre a conformidade e verificação das diretrizes de codificação segura dentro de suas empresas, bem como seu conhecimento sobre o ciclo de desenvolvimento de *software* seguro.

A partir dos dados da pergunta 7, pode-se observar que a maioria dos participantes (22) concordam totalmente que a conformidade com as diretrizes de codificação segura é uma parte importante do desenvolvimento dos produtos da empresa, o que pode indicar um compromisso geral com a segurança do desenvolvimento de *software*.

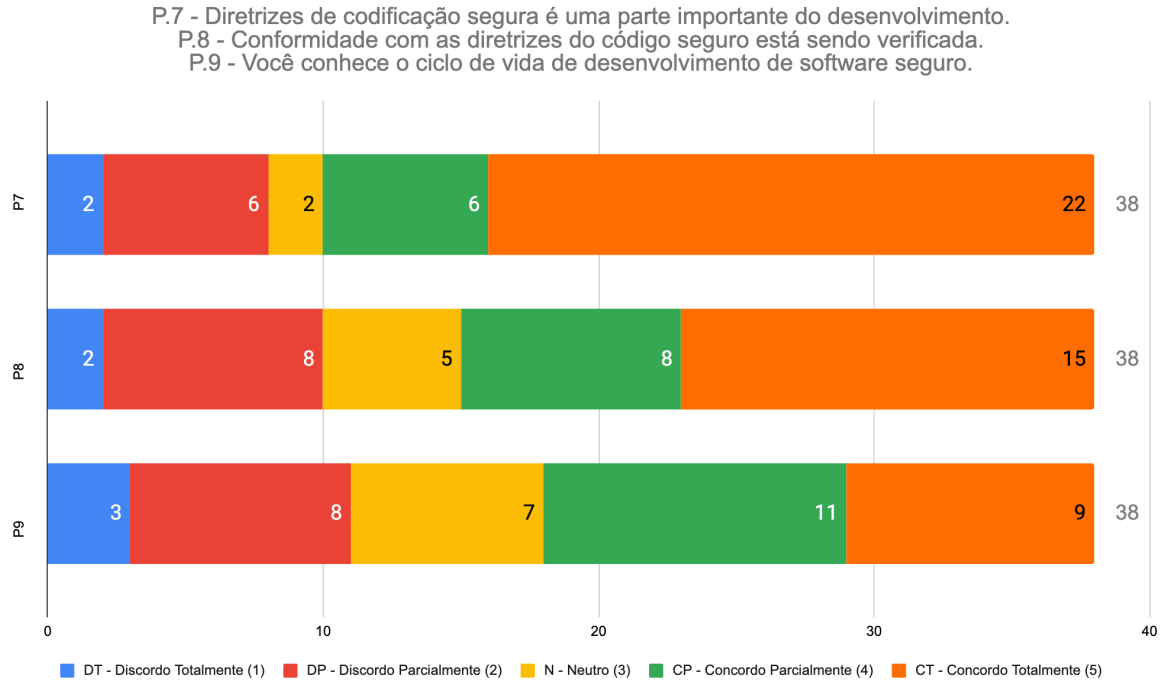
Para a pergunta 8, podemos ver que embora a maioria concorde totalmente (15) ou parcialmente (8) que a conformidade com as diretrizes de código seguro é importante, muitos participantes discordam parcialmente (8) ou totalmente (2) que a conformidade está sendo verificada em seus projetos. Isso indica uma lacuna entre

a importância dada à segurança do código e as práticas implementadas para garantir a conformidade com as diretrizes de código seguro.

No entanto, em relação ao conhecimento do ciclo de vida de desenvolvimento de *software* seguro em suas empresas, os dados da pergunta 9 mostram uma distribuição mais equilibrada. Embora 9 participantes concordam totalmente que conhecem esse ciclo de vida, 11 concordam parcialmente, e 7 ficaram neutros, sugerindo que uma parcela significativa dos participantes pode ter algum conhecimento, mas não necessariamente profundo, sobre esse processo.

Em geral, a análise dos dados sugere que embora muitos participantes estejam cientes da importância da segurança do código e do ciclo e vida de desenvolvimento de *software* seguro, ainda há espaço para melhorias na implementação e na conscientização das práticas de segurança em suas empresas.

Gráfico 5 – Resultados coletados das perguntas 7,8 e 9 do Survey



Fonte: O autor (2023).

Para as perguntas 10, 11 e 12 verificamos as informações sobre as diretrizes de codificação segura, na pergunta 10 avaliamos o porquê dos participantes estarem dispostos a usar as diretrizes de codificação segura, 14,6% responderam que usam

as diretrizes por segurança ser um requisito, a opção 'torna o código resistente a ataques' aparece em segundo lugar com 12,8% seguida pela opção 'para reduzir os riscos de segurança' com 12,2% dos dados. 3% dos participantes responderam com a opção 'não se aplica'.

Quadro 5 – Dados coletados da pergunta 10.

10. Você poderia explicar por que usa diretrizes de codificação segura ao escrever código para o produto que desenvolve atualmente?	**Nº de Respostas**
Segurança é um requisito	17
Por causa das verificações de conformidade	4
Torna o código resistente a ataques	15
Imposição de padrões de qualidade no projeto	10
Garante a qualidade do código	9
São as melhores práticas de desenvolvimento de *software*	5
Para reduzir os riscos de segurança	16
O código seguro é confiável	7
Devido à qualidade e proteção de dados	15
Para evitar erros	8
Por causa das verificações de conformidade	7
Não se aplica	3
Sinto-me confortável com segurança	2

Já a pergunta 11 verifica o porquê do participante não usar as diretrizes de codificação segura, a grande maioria respondeu com a opção 'não se aplica'

totalizando 25,3% dos participantes, seguida pela opção 'não é um requisito' com 10,7%.

Além disso, com base nos dados fornecidos, aparece vários motivos pelos quais as diretrizes de codificação segura não são seguidas, como a concentração nos produtos em vez da segurança (5,3%), pressão de tempo (5,3%), conhecimento limitado (6,7%), economia de custos (2,7%) e o uso de base de código antiga (4%). Além disso, alguns participantes afirmaram que a segurança é adicionada posteriormente (2,7%). Também foi mencionado que os clientes não “enxergam” o recurso (2,7%), que consome tempo (5,3%) e que o *software* será implantado em ambiente seguro (2,7%). Um participante também afirmou que está trabalhando em provas de conceito e que estão testando com poucos clientes (1,7%), o que significa que a segurança pode não ser uma prioridade no momento. Por fim, outro participante usa *software* de código aberto (1,3%), o que pode afetar a segurança de seus produtos.

Quadro 6 – Dados coletados da pergunta 11.

11. Você poderia nos dizer por que não usa as diretrizes de codificação segura?	**Nº de Respostas**
Concentro-me nos produtos, não na segurança	6
A segurança é adicionada depois	3
Usamos base de código antiga (por exemplo, >10 anos)	5
Até agora não tivemos problemas	2
Não se aplica	19
Consome tempo	5
Devido a restrições de tempo	8
Os clientes não "enxergam" o recurso	3
Pressão de tempo	4
Não é um requisito	9

Tenho conhecimento limitado	6
Maior parte dos desenvolvimentos é de provas de conceito	1
O *software* será implantado em ambiente seguro	3
Economia de custos	2
Uso *software* de código aberto	1
A gente da *bypass* em muita coisa pq minha *squad* é de experimentação rápida, e estamos testando com poucos clientes	1

Com base nos dados fornecidos para a pergunta 12, podemos verificar que há várias razões pelas quais a conformidade com as diretrizes de código seguro não está sendo verificada ativamente nos projetos dos participantes da pesquisa, algumas razões mais comuns observadas foram:

Concentração no produto e não na segurança (10,5%), 9,2% não usam diretrizes de codificação segura alguma e 9,2% também citou a falta de recursos para não verificação das diretrizes em seus projetos. Alguns itens foram citados, entre eles: falta de consciência, empresa pequena, economia de custo, baixa senoridade dos analistas.

É importante notarmos que a falta de conformidade com as diretrizes de codificação segura pode levar a vulnerabilidade de segurança, o que pode levar a brechas de segurança e exposição de dados confidenciais. É recomendado que sejam tomadas medidas para abordar as razões pelas quais a conformidade com as diretrizes de codificação segura não está sendo verificada. Isso pode incluir a adoção de diretrizes de codificação segura, a alocação de recursos para a segurança, a conscientização dos desenvolvedores e da gestão, e a utilização de ferramentas automáticas para auxiliar nas verificações de conformidade.

Quadro 7 – Dados coletados da pergunta 12.

12. Por que a conformidade com as diretrizes de codificação segura não está sendo verificada ativamente nos projetos em que você trabalha?	**Nº de Respostas**
Não se aplica	19
Não usamos diretrizes de codificação segura	7
Concentramo-nos nos produtos, não na segurança	8
Falta de recursos	7
Não faz parte do nosso processo de desenvolvimento de software	5
Não é exigido pelo cliente	6
A segurança não é crítica para os produtos	2
Falta de tempo	6
A segurança é um complemento	3
Falta de ferramentas automáticas para auxiliar nas verificações de conformidade	4
Baixa Senioridade de Alguns Analistas	1
A segurança não é compreendida pelos desenvolvedores de software	3
O comprometimento da gestão superior é insuficiente	2
Falta de consciência	1
A empresa é pequena	1
Economia de custo	1

A pergunta 19 questiona a percepção do participante quanto membro de uma equipe de desenvolvimento de sistemas sobre a importância da segurança de *software*. Os dados revelam que a maioria dos participantes (30 de 38) acredita que a segurança do *software* é importante, considerando as notas da escala de Likert 4 e 5 (concordo parcialmente e concordo totalmente).

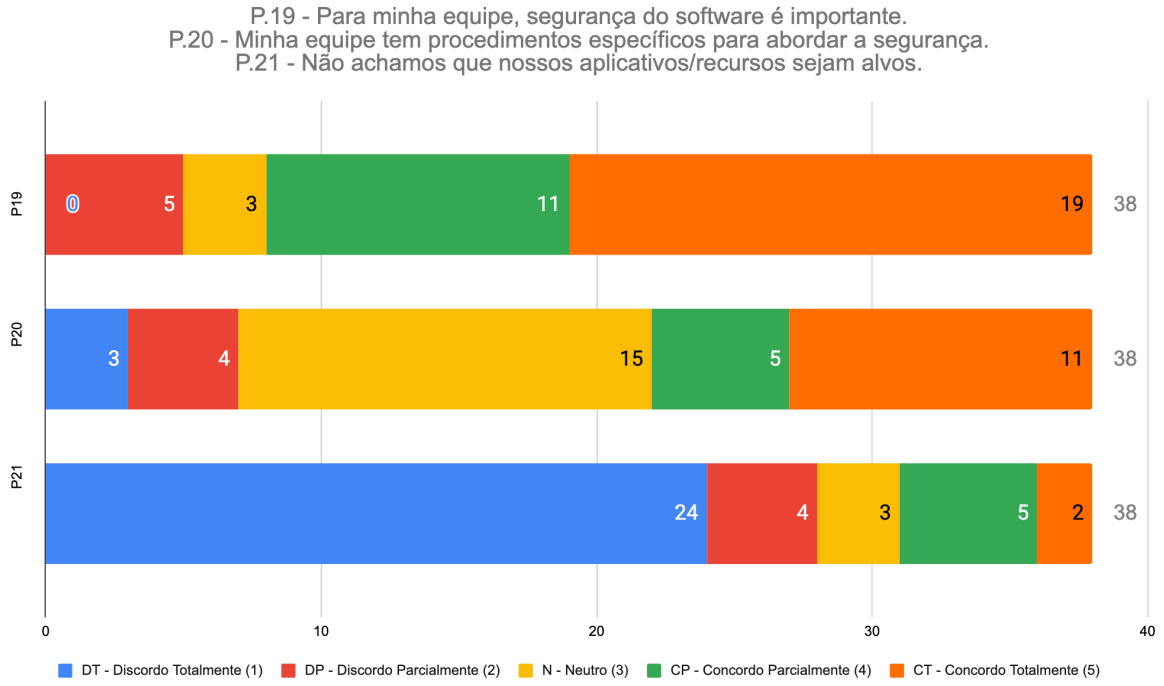
No entanto, é importante notar que houve algumas respostas mais baixas, com duas pontuações, 5 participantes neutros(3) e discordando parcialmente(5). Isso pode indicar que há membros da equipe que não estão tão convencidos da importância da segurança de *software* ou que podem não estar totalmente cientes dos riscos de segurança envolvidos no desenvolvimento de *software*.

Na pergunta seguinte, indica que ele como membro do time não tem um consenso claro sobre a existência de procedimentos específicos para abordar a segurança do *software*. Embora haja algumas respostas positivas (notas 4 e 5), a maioria varia entre 1 e 3, o que sugere que muitos acreditem não haver procedimentos bem definidos para lidar com a segurança do *software*.

Essa falta de procedimentos específicos pode levar a inconsistência na abordagem da segurança de *software* e potencialmente aumentar o risco de vulnerabilidade de segurança.

Já a visão da pergunta 21 é analisar a percepção do participante em relação à segurança dos aplicativos/recursos desenvolvidos pela empresa. A maioria das respostas (28 de 38) indicou que a equipe não acha que os aplicativos/recursos sejam alvos interessantes para invasores, com a nota 1 sendo a mais frequente(24). Isso pode indicar uma falta de consciência dos riscos e ameaças existentes ou uma subestimação dos possíveis danos que uma invasão poderia causar.

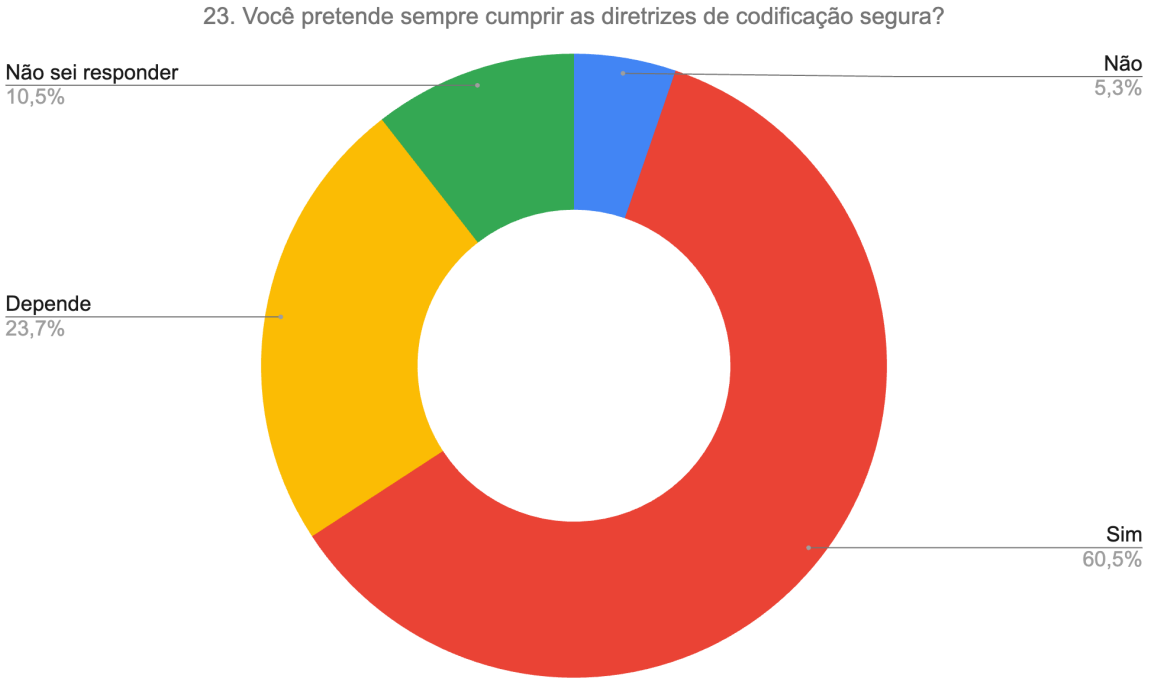
Gráfico 6 – Resultados coletados das perguntas 19,20 e 21 do Survey



Fonte: O autor (2023).

Na pergunta 23, foi perguntado aos participantes se eles pretendem sempre cumprir as diretrizes de codificação segura. Os dados mostram que a maioria dos entrevistados (23 de 38) respondeu que sim, eles pretendem sempre cumprir essas diretrizes. Nove pessoas responderam que depende, o que sugere que eles podem estar dispostos a seguir as diretrizes de codificação segura, mas podem não fazê-lo sempre. Duas pessoas responderam que não, enquanto 4 responderam que não sabem o que responder.

Gráfico 7 – Resultados coletados da pergunta 23 do Survey



Fonte: O autor (2023).

As perguntas 27,28 e 29 tratam do conhecimento, habilidade e experiências dos participantes para escrever código seguro. Já as perguntas 33,34 e 35 tratam do tempo, recursos e liberdade necessários para escrever código seguro.

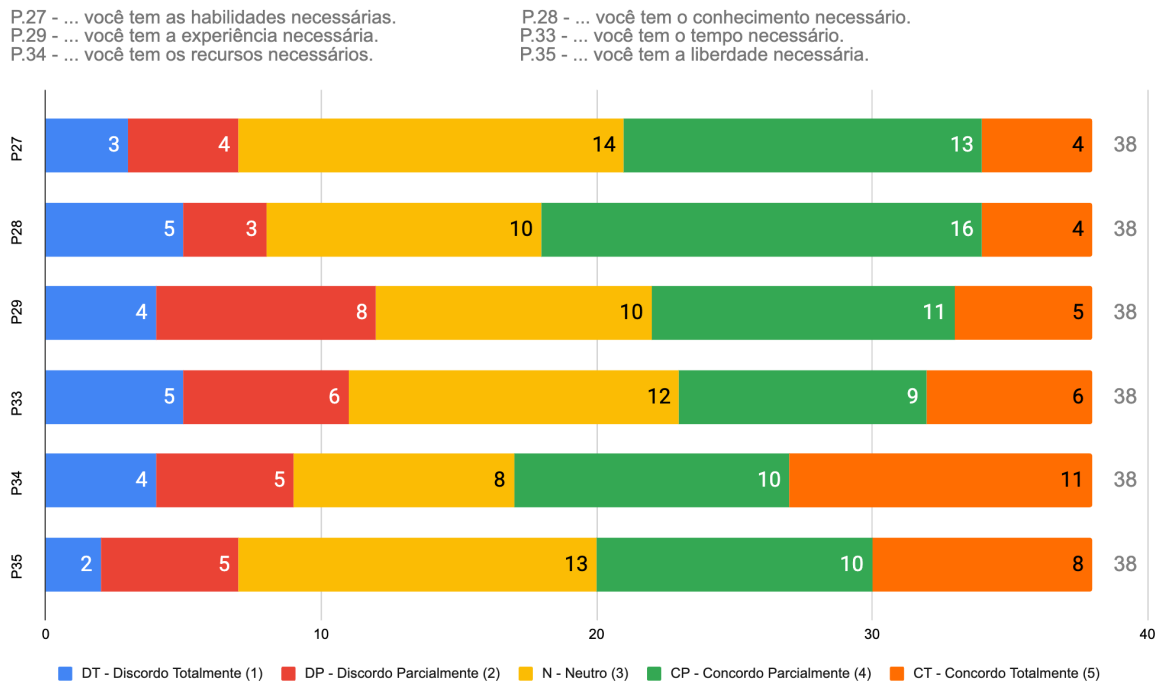
Analisando o conjunto destas seis perguntas, podemos identificar que a maioria dos participantes acredita possuir habilidades, conhecimentos e experiência suficientes para escrever um código seguro. Cerca de 17 dos 38 participantes (marcaram a opção 4 ou 5) dos participantes afirmaram ter as habilidades necessárias, enquanto 20 (marcaram entre 4 e 5) afirmaram ter o conhecimento e a experiência necessários. No entanto, quando questionados sobre o tempo e os recursos necessários, apenas 16 participantes afirmam possuir tempo necessário e 15 recursos necessários.

Isso indica que, embora muitos participantes possuam as habilidades e conhecimentos necessários para escrever um código seguro, eles podem estar lutando com a falta de tempo, recursos e liberdade para fazer isso. É possível que muitos participantes estejam sobrecarregados com outras tarefas e não consigam se dedicar o suficiente à segurança de seus códigos. Além disso, é possível que muitos

participantes não tenham a liberdade necessária para seguir as melhores práticas de segurança devido a restrições impostas por suas empresas ou organizações.

Portanto, é importante que as empresas considerem esses fatores ao tentar promover a segurança de *software*. É importante fornecer aos desenvolvedores tempo e recursos suficientes para garantir a segurança de seus códigos e permitir que eles tenham a liberdade necessária para seguir as melhores práticas de segurança. Além disso, os desenvolvedores também devem se esforçar para melhorar suas habilidades e conhecimentos de segurança para garantir a segurança de seus códigos.

Gráfico 8 – Resultados coletados das perguntas 27, 28, 29, 33, 34 e 35 do Survey



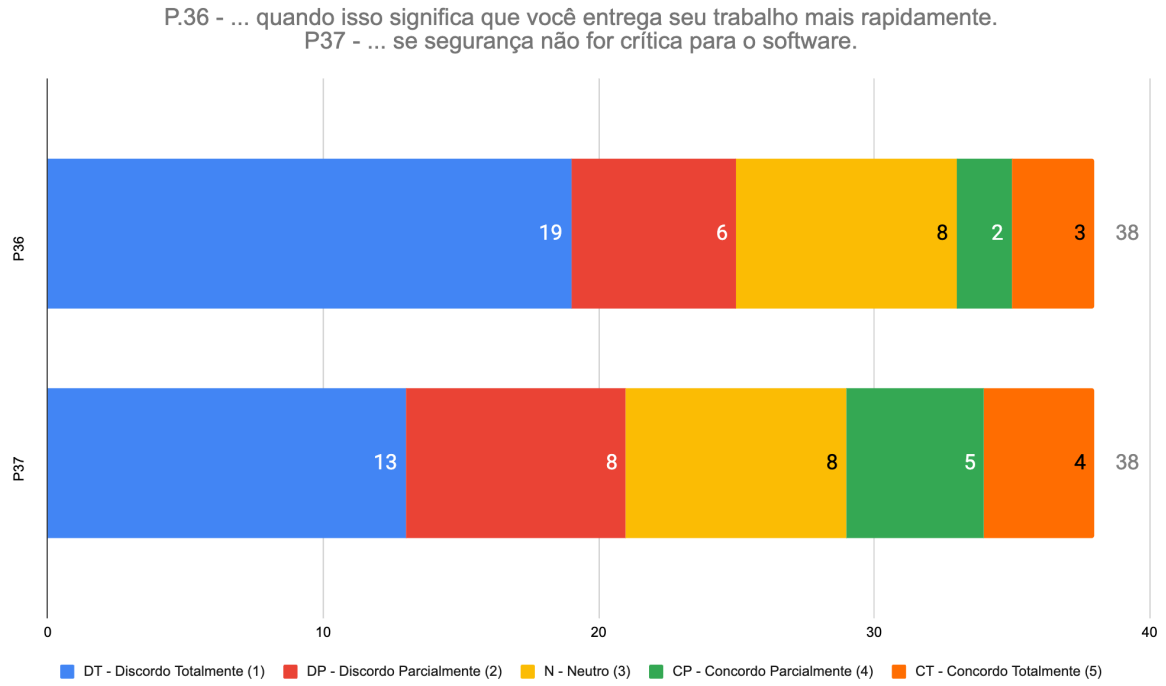
Fonte: O autor (2023).

As perguntas 36 e 37 abordam a questão de desconsiderar as diretrizes de codificação segura em diferentes situações. Enquanto a pergunta 36 questiona se não há problema em desconsiderar essas diretrizes para entregar o trabalho mais rapidamente, a pergunta 37 questiona se não há problema em desconsiderar as diretrizes se a segurança não for crítica para o *software*.

Analisando os dados das duas perguntas, é possível observar que a maioria dos participantes discorda totalmente ou discorda parcialmente da afirmação de que não há problema em desconsiderar as diretrizes de codificação segura, independentemente da situação. Na pergunta 36, 65,8% dos participantes discordam totalmente ou discordam parcialmente da afirmação, enquanto na pergunta 37, 55,3% dos participantes discordam totalmente ou discordam parcialmente.

Isso sugere que a maioria dos participantes valoriza a segurança no *software* e considera que as diretrizes de codificação segura devem ser seguidas, independentemente da situação. No entanto, ainda há um número significativo de participantes que concordam parcialmente ou concordam totalmente com a afirmação, sugerindo que a pressão por entregas mais rápidas ou a percepção de que a segurança não é crítica podem influenciar a decisão de desconsiderar as diretrizes de codificação segura em alguns casos.

Gráfico 9 – Resultados coletados das perguntas 36 e 37 do Survey



Fonte: O autor (2023).

O tema de codificação segura tem sido cada vez mais importante no desenvolvimento de *software*, principalmente em um contexto em que a tecnologia está cada vez mais presente em nossas vidas. Com isso, torna-se necessário que as empresas forneçam treinamentos e materiais adequados para seus profissionais, para que estes possam desenvolver *software* de forma segura e eficiente.

Analisando as perguntas 39, 40, 47, 48, 49 e 50, percebemos que os profissionais estão em busca de uma educação em codificação segura mais efetiva e abrangente. A pergunta 39 revela que muitos profissionais acham difícil entender as diretrizes de codificação segura de suas empresas, o que sugere que essas diretrizes podem não estar claras o suficiente ou que o treinamento oferecido pode não ser adequado para as necessidades dos profissionais.

Além disso, a pergunta 40 mostra que muitos profissionais sentem que não receberam treinamento suficiente sobre codificação segura durante sua formação profissional, o que pode gerar uma lacuna de conhecimento que precisa ser preenchida pelas empresas. Essa falta de treinamento pode estar relacionada à pergunta 48, na qual a maioria dos profissionais não receberam treinamento ou materiais sobre codificação segura de suas empresas.

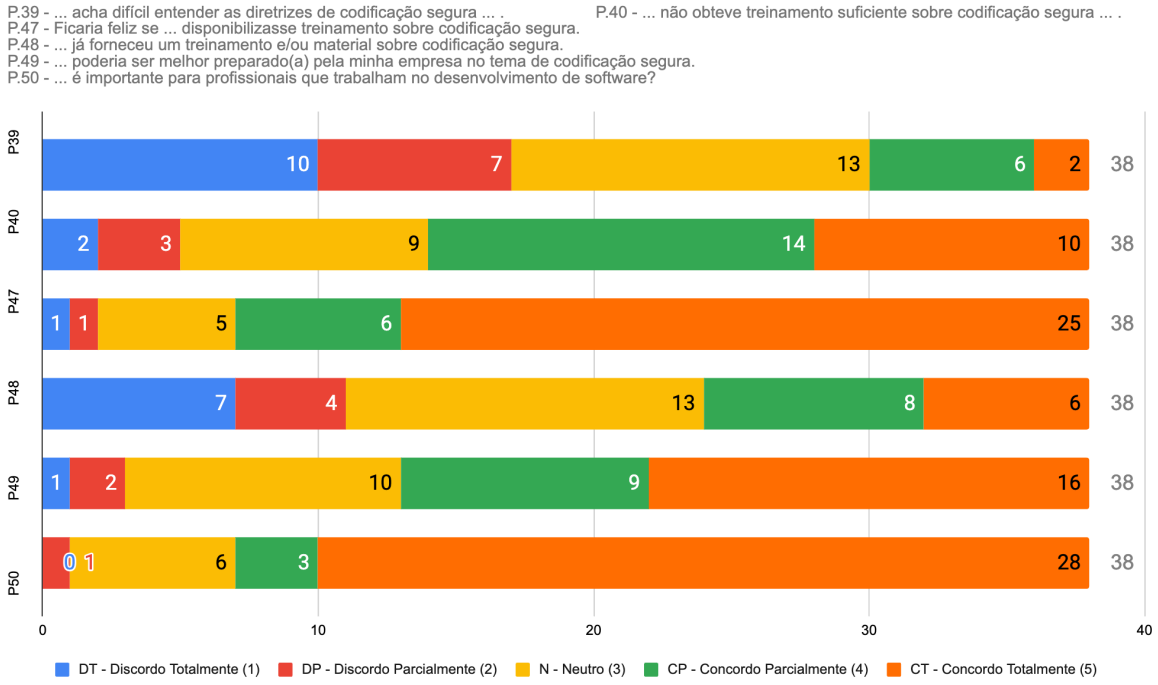
Por outro lado, a pergunta 47 mostra que a grande maioria dos profissionais ficaria feliz se suas empresas fornecessem treinamento sobre codificação segura, indicando uma demanda clara por esse tipo de educação. Já a pergunta 49 revela que a maioria dos profissionais sente que poderia ser melhor preparada pelas empresas no tema de codificação segura, reforçando a necessidade de investimento nessa área.

Por fim, a pergunta 50 traz uma perspectiva mais geral sobre a importância da educação em codificação segura. A grande maioria dos profissionais concorda que essa educação é importante para os profissionais que trabalham no desenvolvimento de *software*, o que indica que existe uma consciência sobre a relevância do tema.

Com base nessas análises, podemos concluir que há uma necessidade clara de as empresas investirem em treinamentos e materiais adequados para a educação em codificação segura de seus profissionais. Essa demanda é

evidenciada pela pergunta 47 e reforçada pelas perguntas 39, 40, 48 e 49. Além disso, a pergunta 50 mostra haver uma consciência geral sobre a importância da educação em codificação segura, indicando uma oportunidade para que as empresas se destaquem no mercado ao oferecer esse tipo de treinamento.

Gráfico 10 – Resultados coletados das perguntas 39, 40, 47, 48, 49 e 50 do Survey



Fonte: O autor (2023).

4.1 Comparação com alguns dados do artigo: *Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey*

Nesta seção do trabalho, serão apresentadas as comparações entre a pesquisa realizada e o artigo da base teórica de GASIBA et al.. Uma das comparações mais significativas é apresentada nas Figuras 1, 2 e 3, que têm como correspondência as perguntas 10, 11 e 12 da presente pesquisa. Essas perguntas visam identificar as razões pelas quais as diretrizes de segurança são seguidas (P10), por que elas não são seguidas (P11) e por que as conformidades não são ativamente verificadas no projeto do participante da pesquisa (P12).

Figura 1 - Você poderia explicar por que você usa diretrizes de codificação segura ao escrever código para o produto que você desenvolve atualmente?

CBg4	
Why use secure coding guidelines?	No.
Security is a requirement	11
Because of compliance checks	5
Makes code resistant to attaks	4
Code is safe and reliable	3
Due to quality and data protection	3
Imposed by project quality gates	2
Ensure code quality	2
It's software development best practices	1
Comfortable with security	1
To avoid bugs	1
To reduce security risks	1

Fonte: GASIBA et al. (2021).

Na comparação entre a Figura 1 do artigo da base teórica e o Quadro 5 da presente pesquisa, observou-se que a resposta mais citada para os desenvolvedores seguirem as diretrizes de codificação segura em ambos os estudos foi o fator da segurança ser um requisito. Esse resultado indica uma concordância entre as duas pesquisas em relação à importância da segurança como fator motivador para a conformidade com as diretrizes de codificação segura.

Figura 2 - Você poderia nos dizer por que você não usa diretrizes de codificação segura?

CBg5	
Why not use secure coding guidelines?	No.
Not a requirement	12
Focus on products, not security	9
Limited knowledge	4
Takes too much time	2
Rely on SAST tools	2
Due to real-time constraints	2
Software deployed in secure environment	2
Customers do not "see" the feature	2
Security is added afterwards	2
Due to usage of proprietary software tools	1
Old code-base (e.g. >10 years)	1
Use open-source software	1
Cost saving reasons	1
Until now we had no issues	1
Time pressure	1

Fonte: GASIBA et al. (2021).

Na comparação entre a Figura 2 do artigo original utilizado na base teórica e o Quadro 6 desta pesquisa, pode-se observar que a resposta mais citada para o não seguimento das diretrizes de codificação segura no primeiro estudo foi a segurança não ser um requisito, seguida pela priorização do foco no produto em detrimento da segurança. No entanto, os dados coletados nesta pesquisa indicam que a resposta mais citada foi "Não se Aplica", seguida por "não é um requisito" e "devido a restrições de tempo".

Figura 3 - Por que a conformidade com as diretrizes de codificação segura não está sendo verificada ativamente nos projetos em que você trabalha?

CBg6	
Why is compliance to SCG not being checked?	No.
Not using secure coding guidelines	4
Focus on products, not security	4
Not required by customer	3
Lack of resources	2
Products are not safety-critical	2
Lack of automatic tools to assist in compliance checks	1
Not enough higher management commitment	1
Nobody in the projects thinks about security	1
Lack of time	1
Small company	1
Security is an add-on	1
Cost saving	1
Not in our software development process	1
Lack of awareness	1
Security is not understood by software developers	1

Fonte: GASIBA et al. (2021).

Ao analisar a conformidade verificada no projeto, é possível observar na Figura 3 do artigo base teórica que as três respostas mais citadas pelos desenvolvedores para não seguir as diretrizes de codificação segura são: não utilizar as diretrizes, focar no produto e não na segurança, e não ser exigido pelo cliente. Já na pesquisa atual, apresentada no Quadro 7, as três respostas mais citadas foram: não se aplica, foco no produto e não na segurança, e falta de recursos. Esses resultados estão em linha com a pesquisa da base teórica.

4.2 Comparação com alguns dados do artigo: *Think secure from the beginning': A Survey with Software Developers*

Nesta seção do trabalho, são apresentadas as comparações realizadas entre os dados obtidos na pesquisa realizada e aqueles descritos na base teórica. Os resultados obtidos visam oferecer uma análise comparativa com a finalidade de obter diferentes perspectivas.

Com relação à experiência profissional, tamanho da empresa e método de desenvolvimento utilizado na empresa, os dados da base teórica revelaram os seguintes resultados:

Figura 4 - Resumo dos dados demográficos dos participantes.

Professional Experience		
Time spent in company		μ = 8 years (Md = 5)
Time spent in team		μ = 4.6 years (Md = 2.5)
Overall development experience		μ = 16.4 years (Md = 15)
Organization Information		
Company Age		μ = 41.3 years (Md = 20)
Size	1-249	34 (28%)
	250-999	29 (24%)
	1,000 or more	60 (49%)
Team Information		
Size		μ = 13.3 members (Md = 8)
TDD	Yes	32 (26%)
	No	82 (67%)
	Don't know	9 (7%)
*Dev Method	Waterfall development	27 (22%)
	Iterative (not truly agile)	26 (21%)
	Rational Unified Process	1 (1%)
	Agile development	58 (47%)
	Other	10 (8%)

Fonte: Hala Assal and Sonia Chiasson (2019).

Nesta pesquisa, os dados foram coletados e conforme apresentado na tabela 1, constatou-se que a maioria dos participantes possuíam entre 3 e 5 anos de experiência, o que representa um tempo consideravelmente menor em comparação com os dados coletados sobre anos de experiência na base teórica do estudo.

Tabela 1 – Anos de experiência de trabalho em Tecnologia da Informação.

Anos de experiência	Qtd. de respostas
Menos de 3 anos	5 (13,2%)
De 3 a 5 anos	13 (34,2%)
De 6 a 10 anos	8 (21,1%)
> 10 anos	12 (31,6%)

Fonte: O autor (2023).

Com relação ao tamanho das empresas, a base teórica do estudo apresenta resultados semelhantes aos dados coletados nesta pesquisa, onde é possível observar que a maioria das empresas possui mil ou mais funcionários.

Tabela 2 – Número de funcionários da empresa.

Número de Funcionários	Qtd. de respostas
1 a 49	3 (7,9%)
50 a 249	7 (18,4%)
250 a 499	1 (2,6%)
500 a 999	5 (13,2%)
>= 1.000	22 (57,9%)

Fonte: O autor (2023).

Com relação ao método de desenvolvimento adotado pelas equipes dos participantes, a base teórica do estudo apresenta o ágil como o processo mais utilizado. Na presente pesquisa, foi possível identificar um padrão semelhante, onde o ágil foi o método mais citado pelos participantes, seguido pelo desenvolvimento iterativo. No entanto, vale ressaltar que, ao contrário do artigo original, que apresenta o desenvolvimento em cascata como o segundo método mais citado, nesta pesquisa foi encontrado o desenvolvimento iterativo como o segundo processo de desenvolvimento mais utilizado.

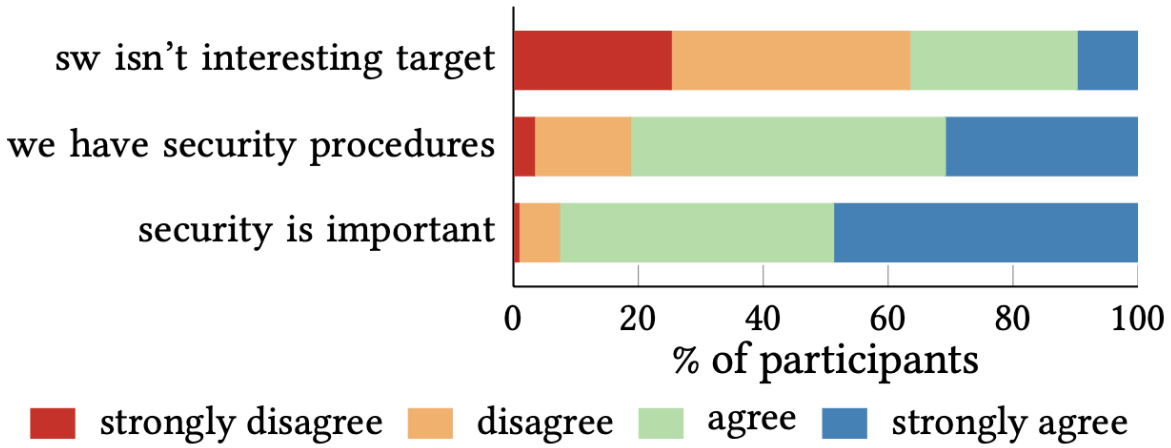
Tabela 3 – Método de desenvolvimento.

Processo de desenvolvimento	Qtd. de respostas
Análise de dados	1 (2,4%)
Desenvolvimento em cascata	8 (19,5%)
Iterativo	12 (29,3%)
Desenvolvimento ágil	20 (48,8%)

Fonte: O autor (2023).

Com relação à percepção dos participantes sobre suas equipes, a Figura 2 do artigo original apresenta uma visão geral dos resultados. Na presente pesquisa, foi possível realizar uma comparação entre as perguntas presentes na Figura 2 e as perguntas 19 a 21 do questionário aplicado, que visavam validar a importância da segurança para as equipes (P19), a existência de procedimentos específicos de segurança (P20) e a possibilidade de o software da equipe ser um alvo interessante para ataques (P21).

Figura 5 - Opinião dos participantes sobre suas equipes.



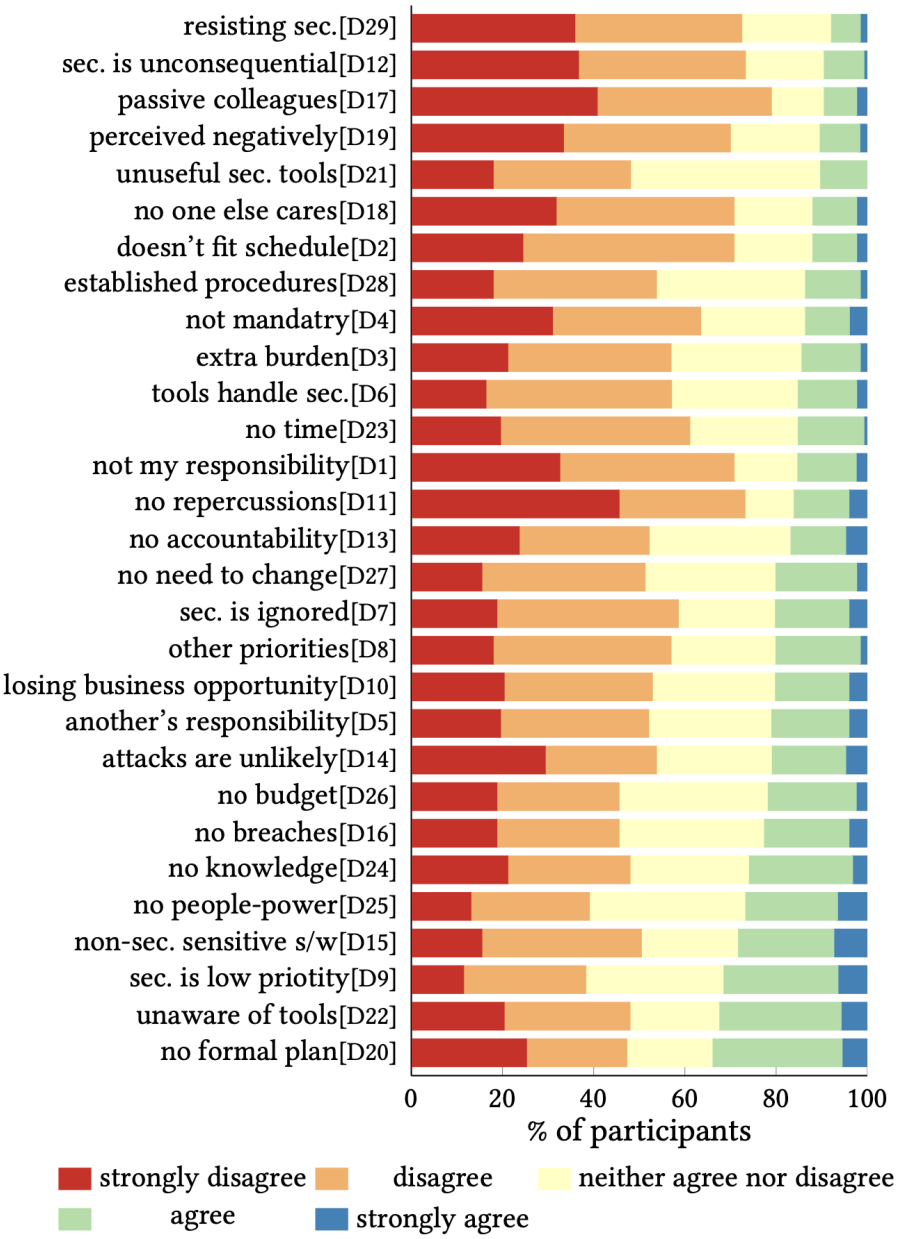
Fonte: Hala Assal and Sonia Chiasson (2019).

Ao analisar os dados coletados na Figura 1, é possível observar que a maioria dos participantes concorda fortemente com a importância da segurança, uma parcela menor, porém ainda considerável, afirma ter procedimentos específicos

de segurança em suas equipes, enquanto uma parcela significativa rejeita a ideia de que seu software não seja interessante para um possível ataque. Esses resultados foram comparados com o Gráfico 6, que apresenta os dados coletados pela presente pesquisa, e mostram uma concordância nas percepções dos participantes em ambos os estudos em relação às suas equipes.

Já a Figura 3 apresenta dados relacionados às motivações que levam os desenvolvedores a não seguirem as diretrizes de codificação segura.

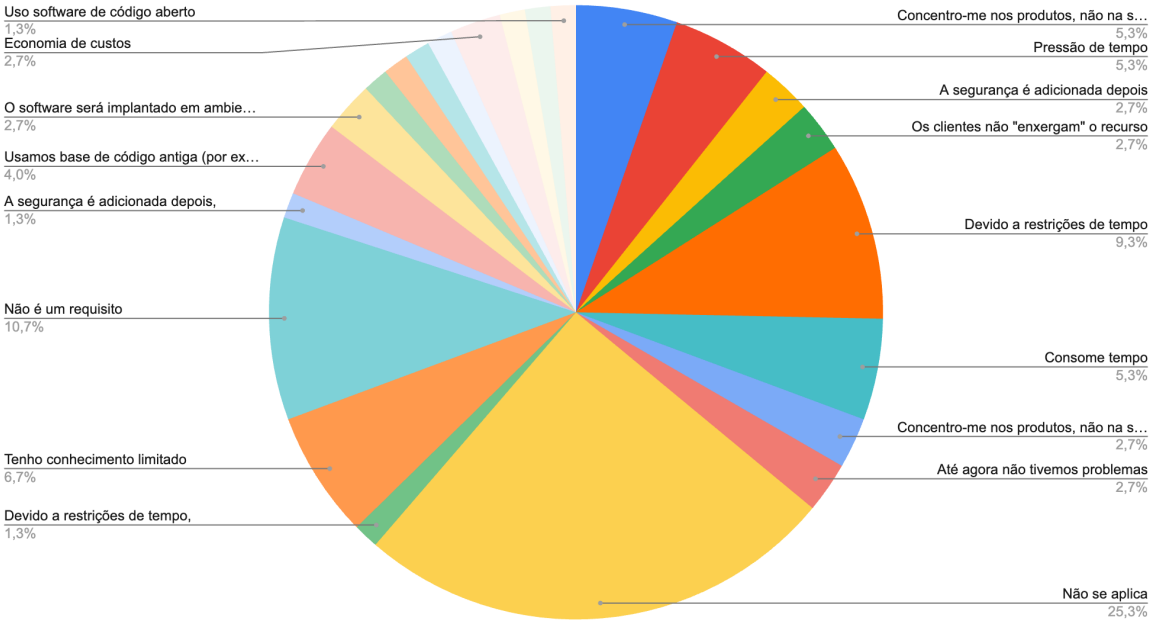
Figura 6 - Motivações para segurança de software.



Fonte: Hala Assal and Sonia Chiasson (2019).

É possível estabelecer um paralelo entre os dados apresentados na Figura 3 do artigo original, que traz informações sobre as motivações que levam os desenvolvedores a não seguir as diretrizes de codificação segura, e a pergunta 11 da presente pesquisa, que visava verificar quais são as motivações para os desenvolvedores não seguirem as diretrizes de codificação segura. Os resultados dessa pergunta foram apresentados em um gráfico na presente pesquisa.

Gráfico 11 – Resultados coletados da pergunta 11 do Survey



Fonte: O autor (2023).

5 CONCLUSÃO

5.1 Contribuições

Este estudo traz algumas contribuições importantes para a área de segurança de *software* e educação em codificação segura. Uma das principais contribuições encontradas é que a maioria dos profissionais de TI reconhece a relevância do assunto e a necessidade de seguir diretrizes de codificação segura para evitar vulnerabilidades de segurança. No entanto, há ainda uma lacuna significativa de conhecimento e treinamento na área, o que pode comprometer a segurança dos *softwares* desenvolvidos.

Outra contribuição deste estudo é mostrar o papel fundamental das empresas na promoção deste ensino de codificação segura e garantir que seus profissionais estejam adequadamente capacitados para desenvolver *software* de forma segura e eficiente. Para isso, é importante investir em treinamentos e materiais adequados, bem como em processos e políticas de segurança que orientem e incentivem a adoção de boas práticas de codificação.

Além disso, é fundamental que as empresas adotem uma abordagem proativa em relação à segurança, identificando e corrigindo possíveis vulnerabilidades antes que elas possam ser exploradas por atacantes. Isso envolve a adoção de práticas de codificação segura desde as fases iniciais do processo de desenvolvimento, bem como a realização de testes de segurança regulares para garantir que o *software* esteja protegido contra possíveis ameaças.

Diante disso, podemos concluir que a codificação segura é um tema crítico para a segurança da informação e para o sucesso das empresas no mercado de tecnologia. As empresas que investem em treinamentos e políticas de segurança adequadas têm mais chances de desenvolver *software* seguro e confiável, evitando prejuízos financeiros e de reputação. Por outro lado, as empresas que negligenciam a segurança arriscam sofrer graves consequências, incluindo a perda de clientes e o comprometimento da reputação.

Assim, é fundamental que as empresas reconheçam a importância do ensino de codificação segura e adotem medidas para garantir que seus profissionais

estejam devidamente capacitados nessa área. Somente assim será possível garantir a segurança dos *softwares* desenvolvidos e manter a confiança dos clientes e usuários.

As empresas podem adotar diversas ações práticas para melhorar a educação em codificação segura de seus profissionais. Primeiramente, é importante que as empresas forneçam treinamentos adequados e abrangentes sobre o tema, com conteúdo atualizado e exemplos práticos de vulnerabilidades comuns e como evitá-las. Além disso, as empresas podem investir em ferramentas de segurança para seus desenvolvedores, como *softwares* de análise estática de código, que podem identificar vulnerabilidades de segurança antes mesmo da implementação do código.

Ademais, é fundamental que a cultura de segurança da informação seja disseminada por toda a organização, desde a alta gestão até os profissionais de desenvolvimento, de forma a conscientizar a todos sobre a importância da segurança da informação e sua responsabilidade em mantê-la.

Além disso, as empresas devem incentivar e recompensar os profissionais que priorizam a segurança do *software* em seus projetos, seja por meio de bônus, promoções ou outros tipos de incentivos. Isso pode ajudar a criar uma cultura de segurança na empresa, onde todos os profissionais se sintam responsáveis pela segurança do *software* que estão desenvolvendo. As empresas têm a responsabilidade de garantir que seus profissionais consigam desenvolver *software* de forma segura e eficiente, evitando vulnerabilidades de segurança que coloquem em risco seus usuários.

5.2 Limitações

Esta pesquisa apresenta algumas limitações importantes que precisam ser consideradas ao interpretar os resultados. Uma das principais limitações é que a pesquisa foi realizada apenas em empresas de software local, o que pode limitar a generalização dos resultados para outros países e localidades. Além disso, a amostra de desenvolvedores de *software* que participaram da pesquisa pode não ser representativa de todos os desenvolvedores de *software* na indústria.

Outra limitação é que a pesquisa se concentrou apenas nas habilidades de codificação segura dos desenvolvedores de *software* e ensino das diretrizes de codificação segura e não levou em conta outras áreas importantes de segurança de *software*, como testes de segurança ou análise de vulnerabilidades. Portanto, estudos futuros podem explorar essas áreas em mais detalhes.

5.3 Trabalhos futuros

Esta pesquisa abre caminho para algumas possíveis pesquisas futuras na área de segurança de *software* e educação em codificação segura. Uma das possibilidades é a investigação das razões pelas quais as empresas podem não está investindo em treinamentos de codificação segura e como essas barreiras podem ser superadas, para fornecer um melhor suporte aos desenvolvedores

Além disso, estudos futuros podem explorar a eficácia de diferentes abordagens de treinamento em codificação segura para desenvolvedores de *software*. Por exemplo, pode-se avaliar a eficácia de treinamentos online, presenciais ou de gamificação.

Por fim, é importante destacar a necessidade de investir em pesquisas sobre segurança de *software*, já que as ameaças e vulnerabilidades estão em constante evolução. Portanto, estudos futuros podem investigar novas vulnerabilidades de segurança que ainda não foram exploradas, bem como novas técnicas e metodologias para preveni-las.

REFERÊNCIAS

[1] DRUCKER, Peter F. **O advento da nova organização**. In: HAVARD Business Review. Rio de Janeiro: Campus, 2000. p. 09-26.

[2] STAIR, Ralph; REYNOLDS, George. **Princípios de sistemas de informação: uma abordagem gerencial**. Rio de Janeiro: LTC, 2002.

[3] NAKAMURA, Emílio; GEUS, Paulo. **Segurança de redes em ambientes corporativos**. São Paulo: Berkeley Brasil, 2002.

[4] PEIXOTO, Mário C. P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006.

[5] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 fev. 2023.

[6] ALEXANDRIA, João C. S. **Gestão de Segurança da Informação: uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica**. São Paulo, 2009. 193f. Tese (Doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009.

[7] MITNICK, Kevin D.; SIMON, Willian L. Mitnick. **A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação**. São Paulo: Makron Books, 2003.

[8] DELISI, Meghan Rimol; HOWLEY, Catherine. **Gartner forecasts worldwide IT spending to grow 2.4% in 2023**. 2023. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2023-01-18-gartner-forecasts-worldwide-it-spending-to-grow-2-percent-in-2023. Acesso em: 02 mar. 2023.

[9] MEHRA, Aashish. **Cyber Security Market worth $266.2 billion by 2027**. Disponível em: https://www.marketsandmarkets.com/PressReleases/cyber-security.asp. Acesso em: 02 mar. 2023.

[10] PETROSYAN, Ani. **Annual number of malware attacks worldwide from 2015 to first half 2022**. 2022. Release date: June 2022. Disponível em: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/#:~:text=During%20the%20first%20half%20of%202022%2C%20the%20number,10.5%20billion%20such%20attacks%20reported%20across%20the%20globe. Acesso em: 02 mar. 2023.

[11] PETROSYAN, Ani. **Annual number of ransomware attacks worldwide from 2016 to first half 2022**. 2022. Release date: June 2022. Disponível em: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/. Acesso em: 02 mar. 2023.

[12] PETROSYAN, Ani. **Average cost of a data breach worldwide from 2014 to 2022**. 2022. Release date: July 2022. Disponível em: https://www.statista.com/statistics/987474/global-average-cost-data-breach/. Acesso em: 02 mar. 2023.

[13] GASIBA, Tiago; ALBUQUERQUE, Maria Pinto; FERNÁNDEZ, Daniel Méndez. **Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey**. CyberSecurity Challenges, [S. l.], p. 1-13, 25 maio 2021. DOI 10.1109/ICSE-SEET52601.2021.00034. Disponível em: https://www.researchgate.net/publication/351420748_Is_Secure_Coding_Education_in_the_Industry_Needed_An_Investigation_Through_a_Large_Scale_Survey. Acesso em: 22 fev. 2023.

[14] ASSAL, Hala; CHIASSON, Sonia. '**Think secure from the beginning': A Survey with Software Developers. Security and privacy**, [S. l.], p. 1-13, 2 maio 2019. Disponível em: https://dl.acm.org/doi/abs/10.1145/3290605.3300519. Acesso em: 20 abr. 2023.

[15] Kizza, J. M. (2015). **Guide to computer network security**. Springer.

[16] SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. 2 ed. Rio de Janeiro: Elsevier, 2014.

[17] Brasil. Tribunal de Contas da União. **Boas práticas em segurança da informação** / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. 103 p.

[18] BEAL, A. **Gestão estratégica da informação: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações**. São Paulo: Atlas, 2012.

[19] COELHO, F.E.S; ARAUJO, L.G.S; BEZERRA, E.K. **Gestão da segurança da informação**. 2. ed. Rede Nacional de Ensino e Pesquisa, 2014. 198 p.

[20] DEFINIRTEC. **Codificação segura**. Disponível em: https://definirtec.com/codificacao-segura/. Acesso em: 10 abr. 2023.

[21] ALMORSY, Mohamed; GRUNDY, John; MÜLLER, Ingo. **An analysis of the cloud computing security problem**. IEEE Security & Privacy, v. 14, n. 5, p. 44-51, 2016.

[22] PAYNE, B. D.; KIRSCH, J.; FARRELL, R.; CARVER, J. **Secure software development: A comparison of the MS SDL and CLASP methodologies**. Computers & Security, v. 66, p. 68-81, 2017.

[23] "**Using References to Prevent Software Vulnerabilities**". Security Today, 1 fev. 2022. Disponível em: https://securitytoday.com/articles/2022/02/01/using-references-to-prevent-software-vulnerabilities.aspx. Acesso em: 16 abr. 2023.

[24] KHAN, R. A.; KHAN, S. U. **Software vulnerabilities, their exploitation and prevention strategies: a survey**. Journal of Network and Computer Applications, v. 137, p. 1-22, 2019.

[25] THOMAS, J.; KESSLER, G. **Cybersecurity risks and mitigation strategies: a survey of organizations in the United States**. Journal of Cybersecurity, v. 5, n. 1, 2019, p. 1-13.

[26] VERIZON BUSINESS. 2021 **Data Breach Investigations Report. [S.l.]**: Verizon Business, 2021. Disponível em: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf. Acesso em: 16 abr. 2023.

[27] SANS INSTITUTE. **Developer Security Awareness Report**. [S.l.]: SANS Institute, 2020.

[28] VERACODE. (2019). **DevSecOps: How to Seamlessly Integrate Security into DevOps**. Veracode.

[29] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems**. NIST Special Publication 800-160. Gaithersburg, MD: National Institute of Standards and Technology, 2017.

[30] OWASP. **Security by Design Principles**. Disponível em: https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A4-Security_by_Design.html. Acesso em: 16 abr. 2023.

[31] SECURE CODE WARRIOR. **Shifting from Reaction to Prevention: The Changing Face of Software Security 2021 - Whitepaper**. Disponível em: https://www.securecodewarrior.com/article/shifting-from-reaction-to-prevention-the-changing-face-of-software-security-2021-whitepaper. Acesso em: 3 abr. 2023.

[33] PATEL, S. "**2019 Global Developer Report: DevSecOps finds security roadblocks divide teams**". Jul. 2020. Disponível em: https://tinyurl.com/y6oypsh3. Acesso em: 6 jan. 2023.

[34] SCHNEIER, B. **Software developers and security**. Online, Jul. 2019. Disponível em:

https://www.schneier.com/blog/archives/2019/07/software_develo.html. Acesso em: 6 abr. 2023.

[35] SOURCEGRAPH. **The Emergence of Big Code – A 2020 Survey of Software Professionals**. [S.l.], Oct. 2020. Disponível em: https://about.sourcegraph.com/blog/the-emergence-of-big-code-a-2020-survey-of-software-professionals/. Acesso em: 15 abr. 2023.

[36] ANDRADE, Maria Margarida de. **Introdução à metodologia do trabalho científico: elaboração de trabalhos na graduação**. 10. ed. São Paulo: Atlas, 2010. 176 p.

[37] ASSIS, Maria Cristina de. Metodologia do Trabalho Científico. In: FARIA, Evangelina Maria B.; ALDRIGUE, Ana Cristina S. (Org.). **Linguagens: usos e reflexões**. 3. ed. João Pessoa: Editora Universitária UFPB, 2009. p. 25-39. Disponível em: https://www.yumpu.com/pt/document/view/13342451/unidade-i-ufpb-virtual-universidade-federal-da-paraiba. Acesso em: 26 mar. 2023.

[38] GIL, A. C. (2002) **Como elaborar projetos de pesquisa**. 4ª. ed. São Paulo: Atlas S/A.

[39] Neuman, W. L. (2003). **Social Research Methods: Qualitative and Quantitative Approaches**. 5th edition. Pearson Education.

[40] MEDEIROS, João Bosco. **Redação Científica: prática de fichamentos, resumos, resenhas**. 13. ed. São Paulo: Atlas, 2019.

[41] MATTAR, Fauze Najib. **Pesquisa de marketing: edição compacta**. São Paulo: Atlas. Acesso em: 23 mar. 2023. , 1996

[42] PERRY, DEWAYNE E., ADAM A. PORTER, and LAWRENCE G. VOTTA (2000). **Empirical studies of software engineering: a roadmap. Proceedings of the conference on The future of Software engineering**. ACM

[43] WOHLIN, C., RUNESON, P., HÖST, M., OHLSSON, M. C., REGNELL, B., and WESSLÉN, A. (2012). **Experimentation in software engineering**. Berlin, Springer-Verlag Berlin Heidelberg

[44] CAMPBELL, D.T., STANLEY, J.C. (1963). **Experimental and Quasi-experimental Designs for Research**. Boston, Houghton Mifflin Company.

[45] COOK, T.D., CAMPBELL, D.T. (1979). Quasi-experimentation – Design and Analysis Issues for Field Settings. Boston, Houghton Mifflin Company.

ANEXO A – SURVEY USADO NO ARTIGO: Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey

Theory	Ref.	Construct	Survey Question
CBG	---	CBg1	In your company compliance to secure code guidelines is being checked in projects you work in
		CBg2	You know the secure software development lifecycle in your company
		CBg3	To which extent do you work with the secure coding standard?
		CBg4	Could you explain why you use secure coding guidelines when writing code for the product you currently develop?
		CBg5	Could you tell us why you do not use secure coding guidelines?
		CBg6	Why is compliance to secure coding guidelines not actively being checked in the projects you work in?
		CBg7	How is the compliance to

			secure coding guidelines checked in your current project?
		CBg8	In your company you use a well established secure software development life-cycle
BGK	---	BgK1	Compliance to secure coding guidelines is an important part of the development of company's products
		BgK2	Which of the following secure coding standards and best practices do you know?
		BgK3	You are aware of negative consequences resulting from exploiting vulnerabilities in the products you work for
		BgK4	What other weaknesses do you pay attention to in developing software for the product you currently work for?
		BgK5*	You know about this weakness
	B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy	ISPA	You know that your company has a policy that mandates the usage of secure

PC	Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS quarterly, vol. 34, no. 3, pp. 523–548, 2010.		coding guidelines in software development
		ITC	You intend to always comply with secure coding guidelines
		GISA	You are aware of the existing security threats to the products of your company
		SE-C1	In your opinion, to write secure code, you have the necessary skills
		SE-C2	In your opinion, to write secure code, you have the necessary knowledge
		SE-C3	In your opinion, to write secure code, you have the necessary competency
	G. D. Moody, M. Siponen, and S. Pahnila, "Toward a Unified Model of Information Security Policy Compliance," MIS quarterly, vol. 42, no. 1, pp. 1–50, 2018.	FacCond5	Support is available if you experience difficulties in complying with secure coding guidelines
		RespCost4	Secure coding guidelines make the task of writing software more difficult
	---	PC-Conf	Complying to SCG makes you feel more confident about the security of the code that

			you write
		PC-NT	In your opinion, to write secure code, you have the necessary time
		PC-NR	In your opinion, to write secure code, you have the necessary resources
		PC-NF	In your opinion, to write secure code, you have the necessary freedom
	M. Siponen and A. Vance, “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations,” MIS quarterly, vol. 34, no. 3, pp. 487–502, 2010.	N-DON3	It is OK to disregard secure coding guidelines when this means that you deliver your work-packages faster
		N-ATHL1	It is OK to disregard secure coding guidelines when you would otherwise not get your job done
		N-DOI1	It is OK to disregard secure coding guidelines when this would result in no harm to the customer
		N-DOI2	It is OK to disregard secure coding guidelines if no damage is done to the company you work for
		N-DOR3	It is OK to disregard secure coding guidelines if

NT			you do not understand them
		N-COC1	It is not as wrong to ignore secure coding guidelines that are not reasonable
		N-COC2	It is not as wrong to ignore secure coding guidelines that require too much time to comply with
		N-MOTL1	You feel that your general adherence to secure coding guidelines compensates for occasionally ignoring them
	---	NT-MArc	It is OK to disregard secure coding practices when this would lead to major architectural changes
		NT-CH	It is OK to disregard secure coding guidelines when this means that it makes your company's customers happy
		NT-SC	It is OK to disregard secure coding guidelines if the software is not safety critical
	J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding Employee	CX2	You find that new employees often know more about secure coding than you do

SRS	Responses to Stressful Information Security Requirements: A Coping Perspective," Journal of management information systems, vol. 31, no. 2, pp. 285–318, 2014.	CX4	You often find it difficult to understand your organization's security coding guidelines
		OL1	Complying to secure coding guidelines forces you to do more work than you can handle
		OL4	You are forced to change your work habits to adapt to your organization's secure coding guidelines
		UC1	There are constant changes in secure coding guidelines your organization
		UC4	There are constant changes in security-related technologies in your organization
AW	N. Haensch and Z. Benenson, "Specifying IT security awareness," in 25th International Workshop on Database and Expert Systems Appli- cations, Munich, Germany. Munich, Germany: IEEE, Sep 2014, pp. 326–330.	Per1*	You can recognize code that contains this weakness
		Be1*	You know how to write code that does not contain this weakness
		Prot1*	You understand the possible consequences that can result from exploiting this weakness

RQ.: Research Question, CBG: Company Background, BGK: Participant Background Knowledge, PC: Policy Compliance Theory, NT: Neutralization Theory, SRS: Security-Related-Stress Theory, AW: Awareness, Note: constructs marked with * are specific for different programming languages

ANEXO B – SURVEY USADO NO ARTIGO: Think secure from the beginning‘: A Survey with Software Developers

“Think secure from the beginning”: A Survey with Software Developers

FULL SURVEY

Q1 Where are you currently employed?
- Africa
- Asia
- Canada
- Europe
- Latin America and the Carribean
- Oceania (Australia, New Zealand, Melanesia, Micronesia, Polynesia)
- USA

Q2 Please select the statement that best describes your current work.
- I am currently on leave
- I am self-employed
- I am currently employed in design (e.g., UI designer, interaction designer)
- I am currently employed in developing software (e.g., programmer, developer, web developer, software engineer, etc.)
- I am currently employed in testing software (e.g., tester, quality analyst, automation engineer, etc.)
- None of the above

Q3 Please select your gender.
- Male
- Female
- Other or not specified

Q4 How long have you been working:
- in your current company?
- in your current team
- in general as a professional developer?

Q5 What is your job title?

Q6 Where did you *mainly* learn to program and develop software?
- Self-taught
- High school courses
- College courses
- University courses
- Online courses
- Industry or on-the-job training
- Other. Please specify.

Q7 Please select the primary development process used by your team.
- Waterfall development (aka Traditional) oIterative (but not truly agile), such as Spiral
- Rational Unified Process (RUP)
- Agile development (including: Scrum, Dynamic Systems Development Model (DSDM), Crystal Methods, Extreme programming (XP), Rapid Application Development (RAD), Feature Driven Development (FDD))
- Other. Please specify

Q8 Does your project team perform Test-Driven Development (TDD)?
- Yes
- No
- I don’t know

Q9 Please describe the types of software you develop and work on.

Q10 Select the most appropriate category that best describes the software you work on.
- Games
- Information display and transaction entry, including websites
- Tools for artistic creativity
- Other consumer-oriented software, including productivity software
- Transaction processing systems for business
- Other Business-oriented software, including management information
- Scientific software, including analysis and visualization
- Computational intensive software such as audio and video processing, machine learning
- Design and engineering software, including CAD-CAM
- Networking and communications software, including telecom and wireless
- Operating systems and their support utilities
- Software for vehicles, aerospace and robots
- Other real-time control and embedded or systems software for devices
- Middleware, system components, libraries and frameworks
- Other tools for software developers, such as IDEs and compilers
- Other. Please specify.

Q11 How old is your organization?

Q12 What is the total number of employees in your organization?
- 1 to 9
- 10 to 249
- 250 to 499
- 500 to 999
- 1,000 or more

Q13 How many members are there in your team? Please enter

numbers only.

Q14 On a scale from 5 (corresponds exactly) to 1 (does not correspond at all), please indicate to what extent each of the following items corresponds to the reasons why you are presently involved in your work. **Why do you do what you do?**
- Because this is the type of work I chose to do to attain a certain lifestyle.
- For the income it provides me.
- I ask myself this question, I don't seem to be able to manage the important tasks related to this work.
- Because I derive much pleasure from learning new things.
- Because it has become a fundamental part of who I am.
- Because I want to succeed at this job, if not I would be very ashamed of myself.
- Because I chose this type of work to attain my career goals.
- For the satisfaction I experience from taking on interesting challenges.
- Because it allows me to earn money.
- Because it is part of the way in which I have chosen to live my life.
- Because I want to be very good at this work, otherwise I would be very disappointed.
- I don't know why, we are provided with unrealistic working conditions.
- Because I want to be a "winner" in life.
- Because it is the type of work I have chosen to attain certain important objectives.
- For the satisfaction I experience when I am successful at doing difficult tasks.
- Because this type of work provides me with security.
- I don't know, too much is expected of us.
- Because this job is a part of my life.

Q15 What does it mean to include security into the development process?

Q16 For the rest of the survey, when we mention "security", we refer to software security as described below. Please note that we are **not** asking about other aspects of security, such as infrastructure and IT security (*e.g.*, ensuring all users in the organization always have software patches installed, and use secure passwords on their accounts)

Software security
- Software security is the idea of building an application that is resistant to: malicious attacks, being used by unauthorized people, or causing harm by inappropriate possibly-accidental use.
- Software security aims to minimize vulnerabilities that could be exploited by attackers (e.g., eliminating buffer overflow vulnerabilities)
- The use of static analysis tools to find potential vulnerabilities in the software being built is an example of software security.

Security functions
- Security functions are the application's security features to protect resources, *e.g.*, authentication to protect user data.
- They can be implemented as functionality within an application (*e.g.*, user authentication).
- Verifying usernames and passwords is an example of security functions.

Which of the following aims to reduce malicious attacks that exploit vulnerabilities? Please select the most accurate choice based on the description above.
- ○ User authentication
- ○ Software security
- ○ Security functions
- ○ All of the above

Q17 Please select the statement that best describes your team. [*4-point Likert scale: strongly agree-strongly disagree.*]
- My team believes that software security is important
- We have specific procedures in place to address software security
- We do not think our applications/features are interesting targets for attackers
- We haven't really considered the security of our software/applications/features

Q18 ***(RQ1)*** As a percentage, how much of your team's overall effort in the development lifecycle relates specifically to security tasks?

Q19 ***(RQ1)*** How are your project team's total software security efforts divided among the following stages? [*Text boxes, total must equal 100*]
- The design stage
- While implementing the code
- During testing by developers
- During code analysis (e.g., using static analysis tools)
- During code review
- During testing that is done by someone other than the code owner

Q20 Rate your agreement with the following. [*5-point Likert scale: strongly agree-strongly disagree.*]
- In my team, when we're choosing a framework/API, we consider whether it gives us security advantages
- I am satisfied with how my team is handling software security

Q21 How likely do you think it is that features developed by your team contain security issues? [*5-point Likert scale: extremely likely-extremely unlikely.*]

Q22 Has your company ever experienced a security issue with software it has developed (e.g., discovering a security vulnerability, or experiencing a security breach)?
- ☐ Yes, we experienced a security breach
- ☐ Yes, a vulnerability in shipped code was discovered
- ☐ Yes, a vulnerability in un-shipped code was discovered
- ☐ No
- ☐ I don't know or prefer not to answer

Q23 How did experiencing a security issue change the attitude towards security over the long term for each of the following? [*single choice: It led to more awareness and*

concern for security, It didn't lead to any change, It lead to less care and awareness for security, I don't know/I prefer not to answer]

- You
- Other developers
- Team leaders
- Higher management
- Users/Customers

Q24 (***RQ2***) Rate your agreement with the following statements. I care about security because... [*5-point Likert scale: strongly agree-strongly disagree, and 'not applicable' choice*]

[M1] My company is audited for software security by an external entity
[M2] My company would lose customers in case of a software security breach
[M3] My company could fail (cease to operate) in case of a software security breach
[M4] My efforts towards software security are recognized
[M5] My efforts towards software security help me grow in the company
[M6] My efforts towards software security are financially rewarding (*e.g.*, through bonuses or a raise)
[M7] My company mandates security practices and I have to follow them
[M8] I see the benefit in security practices mandated by my company
[M9] I understand that my code can have security implications
[M10] My colleagues care about software security
[M11] I care about my company's reputation
[M12] I care about my users' security and privacy
[M13] Software security is in my company's culture
[M14] Software security is a shared responsibility by all those involved in the development lifecycle
[M15] I see software security as my responsibility
[M16] I feel good when I learn about software security
[M17] I feel good when I address potential security issues in my code
[M18] I like to challenge myself to write secure code
[M19] Similar software to that on which I work suffered a security breach and management now cares about securing our applications
[M20] Similar software to that on which I work suffered a security breach and it was an eye-opener for me
[M21] I realized securing my code is important after reading about security breaches in the news

Q25 (***RQ2***) Rate your agreement with each of the following statements. [*5-point Likert scale: strongly agree-strongly disagree*]

[D1] Software security is not my responsibility because it's not in my job description
[D2] Software security does not fit in my schedule
[D3] Software security is a burden on top of my main responsibilities
[D4] Software security is not mandated by my employer
[D5] Software security is handled by someone else in the product lifecycle
[D6] We don't have to worry much about security because frameworks (including APIs)/programming language in-house tools we use handle software security for us
[D7] My team doesn't spend any specific efforts towards software security
[D8] We defer software security due to competing priorities
[D9] In my team, it is more important to deliver features on time than to address software security
[D10] If we focus more on software security, we might lose our business opportunities
[D11] There are no repercussions to ignoring software security
[D12] We do not have competition, so we won't lose customers in case of a software security issue
[D13] I won't be blamed if a security issue is found in my code
[D14] It's unlikely that attackers will attack us
[D15] The software I develop is not prone to security attacks
[D16] Things are fine as they are, we haven't experienced any security breaches
[D17] No one else cares about software security, I won't either
[D18] I understand the importance of addressing security, but I won't waste my time on it since no one else does
[D19] I used to push for software security, but I was perceived negatively by my colleagues
[D20] We do not have a formal process for software security
[D21] Available security code analysis tools are not useful
[D22] I am not aware of tools that would allow security analysis of my code
[D23] I do not have time to address software security
[D24] I do not have necessary knowledge to address software security
[D25] There aren't enough people in my team to address software security
[D26] My team does not have the budget to address software security
[D27] We're doing fine, I don't think we should change in terms of software security
[D28] We have been following the same procedures for years and I don't want to change them
[D29] I tend to resist when I get assigned a security task

Q26 (***RQ1***) Rate your agreement with each of the following statements. [*5-point Likert scale: strongly agree-strongly disagree, and 'not applicable' choice*]

[S1] We rely on libraries and frameworks (including APIs) to help guarantee software security
[S2] Our company/team has baseline security standards with which 3rd party code should comply
[S3] We built our own in-house frameworks to help guarantee software security
[S4] I can get deadline extensions to handle software security
[S5] When a deadline approaches, I try to reduce my

workload to focus on securing my software

[S6] I have my own mental checklist of software security issues that I need to consider in my code

[S7] I have come up with my own software security best practices

[S8] If I didn't have time to address software security, I'd ship the product after adding a work around that allows me to remotely disable the software feature suffering a security breach

[S9] When working on a software security issue, I can get help from others who worked on similar issues

[S10] I prefer to ask for software security advice informally (*e.g.*, by casually asking a colleague, or through discussions over lunch)

[S11] I can rely on the more experienced members of my company/team for help and security advice

[S12] Software security best practices are incorporated in automated checks we run

[S13] Software security best practices are incorporated in tools we use

[S14] We have a document/checklist of items that we need to consider for our application to be secure

[S15] I receive specific instructions on how to solve security issues found in my code

[S16] In code reviews, reviewers explain security issues and fixes to me rather than referring me to resources/books

APÊNDICE A – SURVEY USADO NA COLETA DE DADOS NA PESQUISA

* Tipos de perguntas: SC: Single Choice; MC: Multiple Choice; FT: Free Text; LS: Likert Scale)

Categoria/Propósito	Tipo de Pergunta	Número	Pergunta	Resposta
Parte A - Coleta de dados demográficos				
Pessoa (Para relacionar as respostas ao estado de trabalho atual. Por exemplo, os Desenvolvedores cuidam de codificação segura. Designers não.)	SC	Q1.1	Selecione a afirmação que melhor descreve seu trabalho atual.	Atualmente estou de licença
				Sou autônomo
				Atualmente estou empregado em design (por exemplo: designer de interface do usuário, designer de interação)
				Atualmente estou empregado no desenvolvimento de software (por exemplo: programador, desenvolvedor, desenvolvedor web, engenheiro de software, etc.)
				Atualmente estou empregado em teste de software (por exemplo: testador, analista de qualidade, engenheiro de automação, etc.)

				Nenhuma das anteriores
				Outros _____
Pessoa (Para relacionar as respostas ao tipo de processo de desenvolvimento. Por exemplo, pessoas que trabalham com Desenvolvimento ágil, focam menos em codificação segura.)	SC	Q1.2	Por favor, selecione o processo de desenvolvimento primário usado por sua equipe.	Desenvolvimento em cascata (também conhecido como Tradicional)
				Rational Unified Process (RUP)
				Desenvolvimento ágil (incluindo: Scrum, Modelo de Desenvolvimento de Sistemas Dinâmicos (DSDM), Crystal Methods, Extreme Programming (XP), Rapid Application Development (RAD), Feature Driven Development (FDD))
				Iterativo (mas não verdadeiramente ágil)
				Outros _____
Pessoa (Para verificar quais dos padrões mais conhecidos de codificação	MC	Q1.3	Quais dos seguintes padrões de codificação segura	SEI−CERT

segura o participante conhece.)			e práticas de segurança recomendadas você conhece?	
				MISRA
				C11 Annex J
				OWASP
				BSI 5.21
				Outros _____
Pessoa (Para relacionar as respostas ao tempo de experiência do respondedor.)	SC	Q1.4	Quantos anos de experiência de trabalho você tem?	Menos de 3 anos
				De 3 a 5 anos
				De 6 a 10 anos
				Mais do que 10 anos
Pessoa (Relacionar as respostas à consciência dos riscos das vulnerabilidades no produto da empresa.)	SC	Q1.5	Você está ciente das consequências negativas resultantes da exploração de vulnerabilidades nos produtos de software que desenvolve ou serviços baseados em software que fornece?	Sim
				Não
Pessoa (Relacionar a linguagem utilizada com possíveis vulnerabilidades conhecidas e padrões de segurança)	MC	Q1.6	Qual linguagem é utilizada por você na sua empresa	C
				C++
				Java

				Python
				JavaScript
				PHP
				Ruby
				Outros _____
Parte B - Conhecendo sua empresa				
Diretrizes de Programação Segura (Empresa) (Relacionar a resposta com o sentimento da conformidade sobre a codificação segura)	LS	Q2.1	A conformidade com as diretrizes de codificação segura é uma parte importante do desenvolvimento dos produtos da empresa	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Conformidade com Programação Segura (Empresa) (Relacionar as respostas com o sentimento do participante em relação a sua empresa seguir as diretrizes corretas)	LS	Q2.2	Em sua empresa, a conformidade com as diretrizes do código seguro está sendo verificada nos projetos em que você trabalha	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Ciclo de Desenvolvimento (Pessoa) (Relacionar o nível de conhecimento do participante do ciclo de vida do desenvolvimento seguro)	LS	Q2.3	Você conhece o ciclo de vida de desenvolvimento de software seguro em sua empresa	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Diretrizes de Programação Segura (Pessoa)(Relacionar a resposta ao que o participante considera como ponto chave para escrever código seguro)	MC	Q2.4	Você poderia explicar por que usa diretrizes de codificação segura ao escrever código para o produto que desenvolve	Segurança é um requisito
				Por causa das verificações de conformidade
				Torna o código

			atualmente?	resistente a ataques
				O código é seguro e confiável
				Devido à qualidade e proteção de dados
				Imposto por padrões de qualidade do projeto
				Garante a qualidade do código
				São as melhores práticas de desenvolvimento de software
				Confortável com segurança
				Para evitar erros
				Para reduzir os riscos de segurança
				Não se aplica
				Outros _____
Diretrizes de Segurança (Pessoa) (Relacionar a resposta à opção pessoal do participante em não seguir as diretrizes de segurança)	MC	Q2.5	Você poderia nos dizer por que não usa as diretrizes de codificação segura?	Não é um requisito
				Concentre-se nos produtos, não na segurança
				conhecimento limitado

				Leva muito tempo
				Confio nas ferramentas SAST
				Devido a restrições de tempo real
				Software implantado em ambiente seguro
				Os clientes não "vêem" o recurso
				A segurança é adicionada depois
				Devido ao uso de ferramentas de software proprietárias
				Base de código antiga (por exemplo, >10 anos)
				Uso software de código aberto
				Razões de economia de custos
				Até agora não tivemos problemas
				Pressão de tempo
				Não se aplica
				Outros _____

Diretrizes de Segurança (Empresa) (Relacionar a resposta com o porque o participante imagina que a conformidade não está sendo seguida)	MC	Q2.6	Por que a conformidade com as diretrizes de codificação segura não está sendo verificada ativamente nos projetos em que você trabalha?	Não usar diretrizes de codificação segura
				Concentre-se nos produtos, não na segurança
				Não exigido pelo cliente
				Falta de recursos
				Os produtos não são críticos para a segurança
				Falta de ferramentas automáticas para auxiliar nas verificações de conformidade
				Compromisso de gerenciamento superior insuficiente
				Ninguém nos projetos pensa em segurança
				Falta de tempo
				A organização é pequena
				A segurança é um complemento
				Economia de custo
				Não em nosso

				processo de desenvolvimento de software
				Falta de consciência
				A segurança não é compreendida pelos desenvolvedores de software
				Não se aplica
				Outros _____
Diretrizes de Segurança (Empresa) (Checa o tipo de verificação que ocorre no projeto)	SC	Q2.7	Como a conformidade com as diretrizes de codificação segura é verificada em seu projeto atual?	Ferramentas Automatizadas
				Manualmente
				Revisão de código
				Não se aplica
				Outros _____
Ciclo de Desenvolvimento (Empresa) (Relaciona se a empresa segue um ciclo de código seguro em todos os projetos)	SC	Q2.8	Em sua empresa, você usa um ciclo de vida de desenvolvimento de software seguro bem estabelecido	Sim
				Não
				Sim, mas não em todos os projetos
Ciclo de Desenvolvimento (Empresa)(Relacionar com o conhecimento do participante em saber se sua empresa tem uma política bem estabelecida de codificação segura)	SC	Q2.9	Sua empresa tem uma política que exige o uso de diretrizes de codificação segura no desenvolvimento de software?	Sim
				Não
				Não sei responder
Conhecimento da	SC	Q2.10	Qual é o número	1 a 9

Empresa (Relacionar a resposta ao tamanho da empresa)			total de funcionários em sua organização?	10 a 249
				250 a 499
				500 a 999
				1.000 ou mais
Histórico de Vulnerabilidade (Empresa) (Verifica se a empresa do participante já passou por um problema de vulnerabilidade de código)	SC	Q2.11	Sua empresa já teve um problema de segurança com software que desenvolveu (por exemplo, descobrir uma vulnerabilidade ou passar por uma violação de segurança)?	Sim, tivemos uma violação de segurança
				Sim, uma vulnerabilidade no código em produção foi descoberta
				Sim, foi descoberta uma vulnerabilidade no código que ainda não estava em produção
				Não
				Não sei
Parte C - Conhecendo sua equipe				
Demografia (Time) (Relacionar a pesquisa a categoria do projeto do participante)	SC	Q3.1	Selecione a categoria mais apropriada que melhor descreve o software em que você trabalha.	Jogos
				Exibição de informações e entrada de transações, incluindo sites
				Ferramentas para criatividade artística
				Outros softwares voltados ao consumidor, incluindo software

				de produtividade
				Sistemas de processamento de transações para empresas
				Outros softwares de negócios, incluindo informações de gerenciamento
				Software científico, incluindo análise e visualização
				Software intensivo de computação, como processamento de áudio e vídeo, aprendizado de máquina
				Software de design e engenharia, incluindo CAD-CAM
				Software de rede e comunicação, incluindo telecomunicações e sem fio
				Sistemas operacionais e seus utilitários de suporte
				Software para veículos,

				aeroespacial e robôs
				Outras ferramentas para desenvolvedores de software, como IDEs e compiladores
				Prefiro não responder pois identificaria a empresa
				Outros _____
Parte D - Conhecendo sua equipe em relação a codificação segura				
Importância da Codificação Segura (Time) (Relacionar a noção de importância da segurança dentro do time)	LS	Q3.2	Minha equipe acredita que a segurança do software é importante.	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Importância da Codificação Segura (Time) (Verificação do time e de procedimentos de segurança)	LS	Q3.3	Minha equipe tem procedimentos específicos para abordar a segurança de software.	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Fatores Determinantes para Não Seguir as Diretrizes de Codificação Segura(Time) (Verificação dos fatores para o time não seguir suas diretrizes de segurança)	LS	Q3.4	Não achamos que nossos aplicativos/recursos sejam alvos interessantes para invasores.	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Fatores Determinantes para Não Seguir as	LS	Q3.5	Não consideramos realmente a	Discordo totalmente

Diretrizes de Codificação Segura(Time) (Verificação dos fatores para o time não seguir suas diretrizes de segurança)			segurança de nosso software/aplicativos/ recursos.	(1/2/3/4/5) Concordo totalmente
Parte E - Diretrizes de codificação segura				
Fatores Determinantes para Seguir ou Não As Diretrizes de Segurança (Pessoa) (Relacionar as respostas com fatores que determinam ou não para o participante no desejo de cumprir as diretrizes de segurança)	SC	Q.3.6	Você pretende sempre cumprir as diretrizes de codificação segura?	Sim Não Não sei responder
Fatores Determinantes para Seguir ou Não As Diretrizes de Segurança (Pessoa) (Relacionar as respostas com fatores que determinam ou não para o participante no desejo de cumprir as diretrizes de segurança)	SC	Q.3.7	Você está ciente das ameaças de segurança existentes aos produtos de sua empresa?	Sim Não Não sei responder Não temos ameaças a nenhum produto atualmente
Fatores Determinantes para Seguir ou Não As Diretrizes de Segurança (Pessoa) (Verificar diretamente para o participante o que ele acha que é incluir segurança no desenvolvimento de software)	FT	Q.3.8	Na sua opinião, o que significa incluir segurança no processo de desenvolvimento?	
Diretrizes de Segurança (Empresa) (Valida a resposta do participante	SC	Q.3.9	O enfrentamento de um problema de segurança mudou a	Levou a mais consciência e preocupação com

em saber como mudou na empresa dele, após um caso de problema de segurança)			atitude em relação à segurança a longo prazo na sua empresa?	a segurança
				Não levou a nenhuma mudança prática
				Levou a menos cuidado e conscientização com a segurança
				Não sei/prefiro não responder
Conhecimento das Diretrizes de Segurança (Pessoa) (Levantamento da opinião do participante em relação às diretrizes de segurança)	LS	Q.3.10	Na sua opinião, para escrever um código seguro, você tem as habilidades necessárias	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Conhecimento das Diretrizes de Segurança (Pessoa) (Levantamento da opinião do participante em relação às diretrizes de segurança)	LS	Q.3.11	Na sua opinião, para escrever um código seguro, você tem o conhecimento necessário	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Conhecimento das Diretrizes de Segurança (Pessoa) (Levantamento da opinião do participante em relação às diretrizes de segurança)	LS	Q.3.12	Na sua opinião, para escrever um código seguro, você tem a experiência necessária	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Suporte a Codificação Segura (Pessoa) (Verifica se na visão do participante a empresa dá o suporte necessário para ele seguir as diretrizes de segurança)	SC	Q.3.13	Existe um suporte disponível se você tiver dificuldades em cumprir as diretrizes de codificação segura	Sim
				Não
				Não sei responder

Diretrizes de Codificação Segura - Percepção (Levantamento da opinião do participante em relação às diretrizes de segurança)	LS	Q.3.14	Diretrizes de codificação segura tornam a tarefa de escrever software mais difícil	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Diretrizes de Codificação Segura - Percepção(Levantamento da opinião do participante em relação às diretrizes de segurança)	LS	Q.3.15	A conformidade com as diretrizes de codificação segura (SCG) faz com que você se sinta mais confiante sobre a segurança do código que escreve	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Diretrizes de Codificação Segura - Percepção (Levantamento da opinião do participante em relação às diretrizes de segurança)	LS	Q.3.16	Na sua opinião, para escrever um código seguro, você tem o tempo necessário	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Diretrizes de Codificação Segura - Percepção (Levantamento da opinião do participante em relação às diretrizes de segurança)	LS	Q.3.17	Na sua opinião, para escrever um código seguro, você tem os recursos necessários	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Diretrizes de Codificação Segura - Percepção (Levantamento da opinião do participante em relação às diretrizes de segurança)	LS	Q.3.18	Na sua opinião, para escrever um código seguro, você tem a liberdade necessária	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Diretrizes de Codificação Segura -	LS	Q.3.19	Não há problema em desconsiderar	Discordo totalmente

Percepção (Levantamento da opinião do participante em relação às diretrizes de segurança)			as diretrizes de codificação segura quando isso significa que você entrega seus pacotes de trabalho mais rapidamente	(1/2/3/4/5) Concordo totalmente
Diretrizes de Codificação Segura - Percepção (Levantamento da opinião do participante em relação às diretrizes de segurança)	LS	Q.3.20	Não há problema em desconsiderar as diretrizes de codificação segura se o software não for crítico para a segurança	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Diretrizes de Codificação Segura - Percepção (Percepção sobre codificação segura)	LS	Q.3.21	Você descobre que os novos funcionários geralmente sabem mais sobre codificação segura do que você	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Diretrizes de Codificação Segura - Percepção (Percepção sobre codificação segura)	LS	Q.3.22	Muitas vezes você acha difícil entender as diretrizes de codificação de segurança da sua organização	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Diretrizes de Codificação Segura - Percepção (Percepção sobre codificação segura)	LS	Q.3.23	Muitas vezes você acha que não obteve treinamento suficiente sobre codificação segura na sua formação profissional	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Parte F - Necessidade de ensino de codificação segura				
Disposição para seguir ou não as diretrizes de segurança (Valida se para o projeto o tema	LS	Q.4.1	Posso obter extensões de prazo para lidar com a segurança do	Discordo totalmente (1/2/3/4/5) Concordo

segurança é mais importante que realizar uma entrega insegura)			software	totalmente
Disposição para seguir ou não as diretrizes de segurança (Valida fatores que podem determinar o seguimento de diretrizes por parte do participante.)	LS	Q.4.2	Tenho minha própria lista de verificação mental de problemas de segurança de software que preciso considerar em meu código	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Disposição para seguir ou não as diretrizes de segurança (Relaciona a resposta com o participante ter alguém com maturidade em segurança para apoiar com o tema)	LS	Q.4.3	Posso contar com os membros mais experientes da minha empresa/equipe para obter ajuda e conselhos de segurança	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Disposição para seguir ou não as diretrizes de segurança (Relaciona a resposta ao uso das melhores práticas de segurança nas verificações automatizadas)	LS	Q.4.4	As melhores práticas de segurança de software são incorporadas nas verificações automatizadas que executamos	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Disposição para seguir ou não as diretrizes de segurança (Relaciona a resposta ao uso das melhores práticas de segurança nas ferramentas de desenvolvimento)	LS	Q.4.5	As melhores práticas de segurança de software são incorporadas nas ferramentas que usamos para desenvolvimento	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Disposição para seguir ou não as diretrizes de segurança (Relaciona a resposta ao sentimento do	LS	Q.4.6	Temos um documento/lista de verificação de itens que precisamos	Discordo totalmente (1/2/3/4/5) Concordo

apoio dado pela empresa para melhorar a segurança de software)			considerar para que nosso aplicativo seja seguro	totalmente
Desejo de obter mais conhecimento no tema de segurança de software (Relaciona a resposta ao sentimento do apoio dado pela empresa para melhorar a segurança de software)	LS	Q.4.7	Ficaria feliz se minha empresa disponibilizasse treinamento sobre codificação segura	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Desejo de obter mais conhecimento no tema de segurança de software (Relaciona a resposta ao sentimento do apoio dado pela empresa para melhorar a segurança de software)	LS	Q.4.8	Minha empresa já forneceu um treinamento e/ou material sobre codificação segura	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Desejo de obter mais conhecimento no tema de segurança de software (Relaciona a resposta ao sentimento do apoio dado pela empresa para melhorar a segurança de software)	LS	Q.4.9	Sinto que poderia ser melhor preparado pela minha empresa no tema de codificação segura	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Desejo de obter mais conhecimento no tema de segurança de software (Relaciona a resposta ao sentimento do apoio dado pela empresa para melhorar a segurança de software)	LS	Q.4.10	Você acredita que a educação em codificação segura é importante para profissionais que trabalham no desenvolvimento de software	Discordo totalmente (1/2/3/4/5) Concordo totalmente
Valida se o participante da pesquisa tem interesse de participar de uma possível pesquisa futura voltada a	FT	Q.4.11	Se você tem interesse em participar de uma pesquisa com foco	Discordo totalmente (1/2/3/4/5) Concordo

linguagens específicas de programação e segurança.			em vulnerabilidades em linguagens de programação específicas, por favor, informe o seu e-mail abaixo.	totalmente

APÊNDICE B – MAPEAMENTO DAS PERGUNTAS DO SURVEY DESTA PESQUISA, RELACIONANDO COM OS ARTIGOS DOS TRABALHOS RELACIONADOS

Número da pergunta no survey	Número da pergunta no survey de origem	Referência do artigo idealizador da pergunta	Pergunta
1	Q.2	[14]	Selecione a afirmação que melhor descreve seu trabalho atual.
2	Q.7	[14]	Por favor, selecione o processo de desenvolvimento principal usado por sua equipe.
3	Q.10	[13]	Quais dos seguintes padrões de codificação segura e práticas recomendadas você conhece?
4	-	Autoral desta pesquisa	Quantos anos de experiência de trabalho em Tecnologia da Informação você

			tem?
5	Q.11	[13]	Você está ciente das consequências negativas resultantes da exploração de vulnerabilidades nos produtos de software que desenvolve ou serviços baseados em software que fornece?
6	-	Autoral desta pesquisa	Qual linguagem é utilizada por você na sua empresa?
7	Q.9	[13]	A conformidade com as diretrizes de codificação segura é uma parte importante do desenvolvimento dos produtos da empresa
8	-	Autoral desta pesquisa	Em sua empresa, a conformidade com as diretrizes do código seguro está sendo verificada nos projetos em que você trabalha
9	Q.2	[13]	Você conhece o ciclo de vida de desenvolvimento de software seguro em sua empresa
10	Q.4	[13]	Você poderia explicar por que usa diretrizes de codificação segura ao escrever código para o produto que

			desenvolve atualmente?
11	Q.5	[13]	Você poderia nos dizer por que não usa as diretrizes de codificação segura?
12	Q.6	[13]	Por que a conformidade com as diretrizes de codificação segura não está sendo verificada ativamente nos projetos em que você trabalha?
13	Q.7	[13]	Como a conformidade com as diretrizes de codificação segura é verificada em seu projeto atual?
14	Q.8	[13]	Em sua empresa, você usa um ciclo de vida de desenvolvimento de software seguro bem estabelecido?
15	Q.14	[13]	Sua empresa tem uma política que exige o uso de diretrizes de codificação segura no desenvolvimento de software?
16	Q.12	[14]	Qual é o número total de funcionários em sua organização?
17	Q.22	[14]	Sua empresa já teve um problema de segurança com algum software

			que desenvolveu (por exemplo, descobrir uma vulnerabilidade ou passar por uma violação de segurança)?
18	Q.10	[14]	Selecione a categoria mais apropriada que melhor descreve o software em que você trabalha.
19	Q.17	[14]	Minha equipe acredita que a segurança do software é importante.
20	Q.17	[14]	Minha equipe tem procedimentos específicos para abordar a segurança de software.
21	Q.17	[14]	Não achamos que nossos aplicativos/recursos sejam alvos interessantes para invasores.
22	Q.17	[14]	Não consideramos realmente a segurança de nosso software/aplicativo/recurso.
23	Q.15	[13]	Você pretende sempre cumprir as diretrizes de codificação segura?
24	Q.16	[13]	Você está ciente das ameaças de segurança

			existentes aos produtos de sua empresa?
25	Q.15	[14]	Na sua opinião, o que significa incluir segurança no processo de desenvolvimento?
26	Q.23	[14]	O enfrentamento de um problema de segurança mudou a atitude em relação à segurança a longo prazo na sua empresa?
27	Q.17	[13]	Na sua opinião, para escrever um código seguro, você tem as habilidades necessárias
28	Q.18	[13]	Na sua opinião, para escrever um código seguro, você tem o conhecimento necessário
29	-	Autoral desta pesquisa	Na sua opinião, para escrever um código seguro, você tem a experiência necessária
30	Q.20	[13]	Existe um suporte disponível se você tiver dificuldades em cumprir as diretrizes de codificação segura
31	Q.21	[13]	Diretrizes de codificação segura tornam a tarefa de escrever software

			mais difícil
32	Q.22	[13]	A conformidade com as diretrizes de codificação segura faz com que você se sinta mais confiante sobre a segurança do código que escreve
33	Q.23	[13]	Na sua opinião, para escrever um código seguro, você tem o tempo necessário
34	Q.24	[13]	Na sua opinião, para escrever um código seguro, você tem os recursos necessários
35	Q.25	[13]	Na sua opinião, para escrever um código seguro, você tem a liberdade necessária
36	Q.26	[13]	Não há problema em desconsiderar as diretrizes de codificação segura quando isso significa que você entrega seu trabalho mais rapidamente
37	Q.36	[13]	Não há problema em desconsiderar as diretrizes de codificação segura se segurança não for crítica para o software

38	Q.37	[13]	Você descobre que os novos funcionários geralmente sabem mais sobre codificação segura do que você
39	Q.38	[13]	Muitas vezes você acha difícil entender as diretrizes de codificação segura da sua organização
40	-	Autoral desta pesquisa	Muitas vezes você acha que não obteve treinamento suficente sobre codificação segura da sua formação profissional
41	S4	[14]	Posso obter extensões de prazo para lidar com a segurança do software
42	S6	[14]	Tenho minha própria lista de verificação mental de problemas de segurança de software que preciso considerar em meu código
43	S11	[14]	Posso contar com os membros mais experientes da minha empresa/equipe para obter ajuda e conselhos de segurança
44	S12	[14]	As melhores práticas de

			segurança de software são incorporadas nas verificações automatizadas que executamos
45	S13	[14]	As melhores práticas de segurança de software são incorporadas nas ferramentas que usamos para desenvolvimento
46	S14	[14]	Temos um documento/lista de verificação de itens que precisamos considerar para que nosso aplicativo seja seguro
47	-	Autoral desta pesquisa	Ficaria feliz se minha empresa disponibilizasse treinamento sobre codificação segura
48	-	Autoral desta pesquisa	Minha empresa já forneceu um treinamento e/ou material sobre codificação segura
49	-	Autoral desta pesquisa	Sinto que poderia ser melhor preparado(a) pela minha empresa no tema de codificação segura
50	-	Autoral desta pesquisa	Você acredita que a educação em codificação segura é importante para profissionais que trabalham no

			desenvolvimento de software?
51	-	Autoral desta pesquisa	Se você tem interesse de participar de uma pesquisa com foco em vulnerabilidades em linguagens de programação específicas, por favor, informe o seu e-mail abaixo.