A educação em desenvolvimento de software seguro é necessária na indústria de software? Respostas de profissionais de um hub de tecnologia no Brasil

José Claudino Santos Neto,
Carla Silva, Jéssyka Vilela
Centro de Informática
Universidade Federal de Pernambuco (UFPE)
Recife, Pernambuco, Brasil
{jcsn2, ctlls, jffv}@cin.ufpe.br

Mariana Peixoto
Universidade de Pernambuco (UPE)
Garanhuns, Pernambuco, Brasil
mariana.peixoto@upe.br

ABSTRACT

Contexto: A educação e a formação de profissionais de segurança da informação são essenciais para garantir a proteção de dados e sistemas, bem como a privacidade e segurança de informações sensíveis. Problema: Este trabalho tem como objetivo explorar o contexto de um hub tecnológico local para responder à seguinte questão de pesquisa: A educação em desenvolvimento de software seguro é necessária na indústria de software? Solução: Para responder a esta pergunta, foi realizado um estudo exploratório para compreender a necessidade de educação em desenvolvimento de software seguro do ponto de vista dos profissionais de software em um centro tecnológico. Método: Um questionário foi elaborado e enviado a profissionais de um polo tecnológico brasileiro. As respostas foram analisadas utilizando métodos de pesquisa qualitativa. Resultados: Obtivemos trinta e oito respostas. 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, a educação em segurança da informação ainda é insuficiente. Contribuições: Conclui-se que as empresas deveriam investir mais em treinamentos adequados e abrangentes sobre o tema, além de incentivar e premiar os profissionais que priorizam a segurança de software em seus projetos. É fundamental disseminar uma cultura de segurança da informação em toda a organização, desde a alta administração até os profissionais de desenvolvimento, para conscientizar todos sobre a importância da segurança da informação e a responsabilidade de cada indivíduo em mantê-la. Por fim, cabe destacar que os desenvolvedores têm um papel crucial na promoção da segurança do software, sendo responsáveis por buscar conhecimento e aprimorar suas habilidades de desenvolver software seguro por meio de treinamento, leitura e prática.

KEYWORDS

Desenvolvimento de Software Seguro; Educação em Segurança da Informação; Codificação Segura; Survey.

1 Introdução

Conforme Nakamura e Geus [1], “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”.

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 [2], “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”.

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 a 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 as use 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.

Para se ter proatividade na implementação de código seguro desde o início do ciclo de vida do software, 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?

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.

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" [3].

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" [4].

Por conta dessas pesquisas terem sido realizadas em um cenário externo, tornou-se importante conhecer o cenário local. Com base no objetivo da pesquisa, foram desenvolvidas as questões de pesquisa (RQs) apresentadas no Quadro 1.

Este estudo é classificado como uma pesquisa quantitativa, com o objetivo de 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.

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.

O restante do artigo estrutura-se em: Seção 2 apresentando a contextualização da área e trazendo breve discussão sobre trabalhos anteriores relacionados ao tema. Na seção 3 é descrito o método de pesquisa adotado. A seção 4 aborda uma visão dos resultados mais importantes da análise dos dados coletados. Finalmente, a seção 5 apresenta conclusões e trabalhos futuros.

2 REVISÃO DE LITERATURA

As vulnerabilidades de software são uma ameaça constante à segurança da informação. As referências relevantes em segurança da informação, como o OWASP Top 10[1], 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 [8].

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. [7] 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.

[1] https://owasp.org/www-project-top-ten/

Segundo Khan e Khan [9], 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.

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 [6].

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.

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 [12]. 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.

O ensino de codificação segura na indústria de tecnologia é importante para garantir que os desenvolvedores 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. [7], muitas organizações de tecnologia oferecem treinamento em codificação segura para seus desenvolvedores, incluindo cursos online e presenciais. 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 [5] 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.

De fato, as habilidades e a experiência dos desenvolvedores são fatores críticos na criação de softwares seguros. Payne et al. [7] 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 [10]. 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 [11].

O objetivo é adotar o Security by Design (SbD), ou Segurança por Design em português, que 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.

2.1 Trabalhos relacionados

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

O primeiro artigo, intitulado "*Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey*" [3], 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*" [4], apresentou uma pesquisa com desenvolvedores de software sobre a importância da segurança da informação no processo de desenvolvimento de software.

Nesta seção apresentamos uma comparação dos trabalhos que foram as inspirações para o survey. O Quadro 1 apresenta 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. [3] 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 [4] 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.

Além disso, o estudo de Gasiba et al. [3] também abordou a importância da educação em codificação segura na indústria de software, assim como este presente estudo. No entanto, diferentemente do estudo de Assal e Chiasson [4], que se

concentrou em desenvolvedores de software específicos, o estudo de Gasiba et al. [3] buscou uma amostra mais ampla de profissionais de Tecnologia da Informação (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. [3] 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 [4] apresentou um foco específico em como os desenvolvedores 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 software.

No quadro 2 temos uma visão bem resumida dos resultados coletados que serão discutidos na seção 4 deste documento.

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. [3] destaca a falta de apoio dos gerentes de projeto como um fator crítico. Já o estudo de Assal e Chiasson [4] 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. Essa preocupação é enfatizada por Assal e Chiasson [4].

Quadro 1 – Quadro comparativo entre esta pesquisa e base teórica.

	Esta pesquisa	**Gasiba et al. [3]**	**Assal e Chiasson [4]**
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

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 importantes a serem superados para a implementação de treinamentos efetivos na indústria de software.

3 MÉTODO DE PESQUISA

A pesquisa foi conduzida conforme os princípios éticos da pesquisa científica, com a garantia da confidencialidade dos dados

coletados e a proteção da privacidade dos participantes. Foi obtido o consentimento informado dos participantes e a participação na pesquisa foi voluntária e anônima. Os participantes foram informados sobre os objetivos da pesquisa e eles poderiam desistir a qualquer momento. A análise dos dados foi realizada imparcialmente e sem influência externa.

3.1 Coleta de dados

Para a coleta de dados, foram 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 incluiu um link para o Survey online no Google Forms.

O Survey é 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 [13], 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 desta 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 o convite dos participantes foi feito por meio de convite online para participação na pesquisa.

Quadro 2 – Quadro comparativo quanto aos resultados com essa pesquisa e base teórica.

Estudo	**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. [3]	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 [4]	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.

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 de empresas de software locais, os quais respoderam o questionário remotamente. 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 universidade, grupos de WhatsApp, grupos de Facebook voltados para a área de TI e classroom da disciplina de Segurança.

O Survey desenvolvido neste trabalho está no material suplementar[2] e 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" [3] e o "Think secure from the beginning": A Survey with Software Developers [4] que tratam da mesma problemática, 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 (material suplementar), 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. No material suplementar, há também um quadro de rastreamento identificando quais perguntas são reusadas de algum dos dois artigos.

Participaram do estudo 38 funcionários de empresas de software da indústria local, dos quais 71% atuam diretamente no desenvolvimento de software. Com relação aos dados demográficos, 34,2% da amostra tem entre 3 e 5 anos de experiência 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.

[2]Material: https://zenodo.org/doi/10.5281/zenodo.12996490

3.2 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.

3.3 Ameaças a validade

Perry et al. [14] 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. [15], 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 [16] e Cook e Campbell [17], existem quatro tipos de ameaças à validade de um estudo empírico: (a) Validade de conclusão: possibilidade de tirar conclusões imprecisas das observações; (b) Validade Interna: ameaças que podem ter afetado os resultados e não foram devidamente levadas em conta; (c) Validade de construção: ameaças sobre a relação entre a teoria e a observação; (d)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. Para lidar com isso, o questionário foi enviado antecipadamente a um colega profissional da área de segurança e para a pesquisadora sênior deste estudo, a fim de identificar e corrigir 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, muitas 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.

4 ANÁLISE DOS RESULTADOS

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 obtidos nesta pesquisa.

Na pergunta 3, 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, 12 participantes afirmaram não conhecer nenhum dos padrões mencionados.

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 considerável de 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.

A pergunta 4 buscou avaliar a experiência de trabalho em TI 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.

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 ser explicado por diversos fatores: (i) Falta de Experiência Prática: Alguns profissionais podem ter menos experiência prática com incidentes de segurança, levando a uma percepção menor das consequências reais; (ii) Contexto Específico: Os 7,9% que não reconhecem as consequências podem estar em contextos onde as falhas de segurança não tiveram um impacto visível em seus projetos; (iii) Educação Incompleta: Mesmo reconhecendo a importância do treinamento de segurança (pergunta 50), esses profissionais podem não ter recebido uma educação abrangente que explique detalhadamente as consequências das falhas de segurança. Isso pode levar a produtos e serviços vulneráveis e expostos a ameaças de segurança. No entanto, essas são apenas suposições e confirmar as reais razões que levaram 7,9% dos profissionais a não terem conhecimento sobre as consequências negativas das falhas de segurança requer uma investigação adicional, não contemplada no presente survey.

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 concordem totalmente que conhecem esse ciclo de vida, 11 concordam parcialmente, e 7 ficaram neutros, sugerindo que uma parcela razoável dos participantes pode ter conhecimento 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.

Para as perguntas 10, 11 e 12, verificamos as informações sobre as diretrizes de codificação segura. Na pergunta 10 buscamos o porquê de os participantes estarem dispostos a usar as diretrizes de codificação segura, onde 14,6% responderam que usam as diretrizes por segurança ser um requisito e a opção 'torna o código resistente a ataques' aparece em 2o lugar com 12,8%, seguida pela opção 'para reduzir os riscos de segurança' com 12,2% das repostas. Apenas 3% dos participantes responderam com a opção 'não se aplica'.

Já a pergunta 11 verifica o porquê de o 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.

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. Por exemplo, há uma grande concentração no produto sem considerar a segurança (10,5%), 9,2% não usam diretrizes de codificação segura alguma e 9,2% também citaram 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 senioridade 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.

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 respostas com pontuações baixas: 5 participantes neutros (3) ou 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 20, 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.

Na pergunta 23, foi perguntado se os participantes 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 o fazer sempre. Duas pessoas responderam que não, enquanto 4 responderam que não sabem o que responder.

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 (Figura 1).

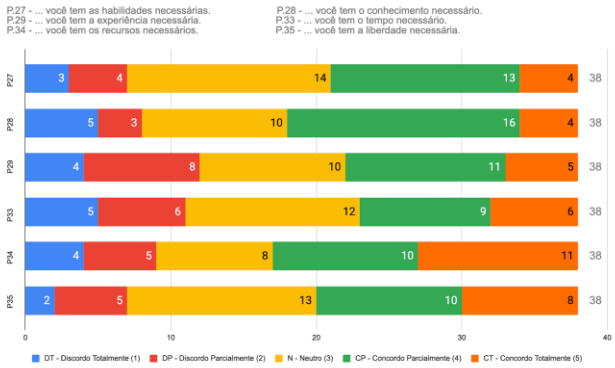

Figura 1. Resultados coletados das perguntas 27, 28, 29, 33, 34 e 35 do Survey

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.

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 software seguro e considera que as diretrizes de codificação segura devem ser seguidas, independentemente da situação. No entanto, ainda há um número considerável 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.

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 sobre desenvolvimento de software seguro.

Analisando as perguntas 39, 40, 47, 48, 49 e 50 (Figura 2), vemos 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 ser uma lacuna de conhecimento que precisa ser preenchida pelas empresas. Essa falta de treinamento pode estar relacionada à pergunta 48, na qual a maioria diz não ter recebido 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 mais bem 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.

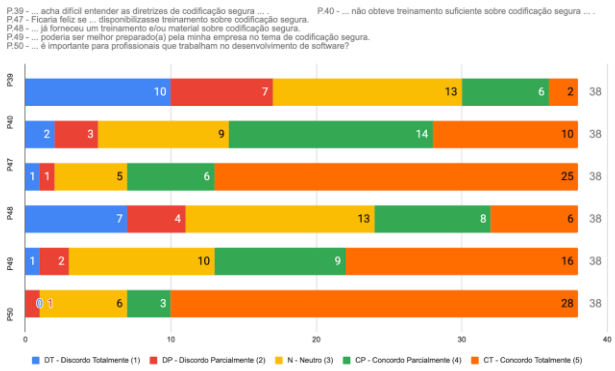

Figura 2. Resultados coletados das perguntas 39, 40, 47, 48, 49 e 50 do Survey

5 CONCLUSÃO

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, apesar de uma conscientização crescente sobre a segurança, ainda existem lacunas significativas na aplicação prática de diretrizes de segurança devido a barreiras como falta de tempo, recursos e apoio gerencial.

Os resultados deste estudo fornecem uma visão mais detalhada das barreiras locais específicas que dificultam a adoção de práticas de codificação segura, algo que não foi abordado em estudos anteriores de âmbito global, europeu ou norte-americano.

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 seguro. 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 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 a perda de clientes e o comprometimento da reputação.

O Quadro 2 apresentou uma análise comparativa na qual identificamos que a principal barreira para a implementação de treinamentos em codificação segura é a falta de tempo e de recursos financeiros da empresa. Esse achado adicionou uma nova dimensão aos resultados de estudos anteriores, que indicavam a falta de apoio de gerentes de projeto como uma barreira significativa [3] e a pressão para concluir os projetos como um obstáculo à implementação de práticas de segurança [4].

Portanto, 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 na etapa implementação. No entanto, embora a análise estática seja importante, ela sozinha não é suficiente. Portanto, recomendamos uma abordagem combinada que inclui: (i) Análise Estática: Para detectar vulnerabilidades no código; (ii) Testes Dinâmicos: Para avaliar a segurança em tempo de execução; (iii) Revisões de Código e Pentests: Para identificar falhas que podem não ser capturadas por ferramentas automatizadas. Tais recomendações estão reportadas no estudo de Bezerra et al. [18].

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. A recomendação de incentivos para o desenvolvimento de software seguro visa criar uma cultura onde a segurança é uma prioridade desde o início (Secure by Design). Reconhecemos que a aplicação prática desses incentivos pode variar, mas algumas estratégias incluíram, por exemplo: (i) Recompensas por Bug Bounties: Incentivar desenvolvedores a encontrar e corrigir vulnerabilidades; (ii) Avaliações de Desempenho: Integrar métricas de segurança dos produtos e serviços baseados em software desenvolvidos na empresa nos critérios de avaliação de desempenho dos desenvolvedores. No entanto, ainda é preciso realizar estudos empíricos que demonstrem a efetividade da adoção dessas e de outras estratégias para incentivar a estabelecer a cultura de segurança da empresa.

Esta pesquisa apresenta algumas limitações que precisam ser consideradas ao interpretar os resultados. A pesquisa foi realizada apenas em empresas de software locais e com uma amostra de desenvolvedores de software pequena, o que pode limitar a generalização dos resultados para outros países e localidades.

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.

Este estudo abre caminho para algumas pesquisas futuras na área de educação em codificação segura. Uma das possibilidades é investigar as razões pelas quais as empresas não estão investindo em treinamentos de codificação segura ou de outras atividades que promovem o desenvolvimento de software seguro.

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 investigar a efetividade de estratégias adotadas para incentivar desenvolvedores a criar software seguro, visando melhorar a qualidade dos produtos e serviços baseados em software, e estabelecer a cultura de segurança em uma empresa.

AGRADECIMENTOS

Agradecemos aos participantes desta pesquisa.

REFERÊNCIAS

[1] Nakamura, E. Geus, P. 2002. Segurança de redes em ambientes corporativos. São Paulo: Berkeley Brasil.

[2] Peixoto, M. C. P. 2006. Engenharia social e segurança da informação na gestão corporativa. Rio de Janeiro: Brasport.

[3] Gasiba, T., Albuquerque, M. P., Fernández, D. M. 2021. Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey. CyberSecurity Challenges, [S. l.], p. 1-13. DOI 10.1109/ICSE-SEET52601.2021.00034.

[4] Assal, H., Chiasson, S. 2019. 'Think secure from the beginning': A Survey with Software Developers. Security and privacy, [S. l.], p. 1-13. DOI: 10.1145/3290605.3300519.

[5] Kizza, J. M. 2015. Guide to computer network security. Springer.

[6] DEFINIRTEC. Codificação segura. Disponível em: https://definirtec.com/codificacao-segura/. (último acesso 10/04/23).

[7] Payne, B. D., Kirsch, J., Farrell, R., Carver, J. 2017. Secure software development: A comparison of the MS SDL and CLASP methodologies. Computers & Security, v. 66, p. 68-81.

[8] SECURITY TODAY. Using References to Prevent Software Vulnerabilities", 2022. Disponível em: https://securitytoday.com/articles/2022/02/01/using-references-to-prevent-software-vulnerabilities.aspx. (último acesso 16/04/23).

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

[10] SANS INSTITUTE. 2020. Developer Security Awareness Report. [S.l.]: SANS Institute.

[11] MacDonald, N. and Head, I. 2016. DevSecOps: How to seamlessly integrate security into DevOps, Gartner, Tech. Rep..

[12] 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. (último acesso 16/04/23).

[13] Mattar, F. N. 1996. Pesquisa de marketing: edição compacta. São Paulo: Atlas.

[14] Perry, D. E., Porter, A. A. and Votta, L. G. 2000. Empirical studies of software engineering: a roadmap. Proceedings of the conference on The future of Software engineering. ACM

[15] Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wesslén, A. 2012. Experimentation in software engineering. Berlin, Springer-Verlag Berlin Heidelberg

[16] Campbell, D. T., Stanley, J. C. 1963. Experimental and Quasi-experimental Designs for Research. Boston, Houghton Mifflin Company.

[17] Cook, T. D., Campbell, D. T. 1979. Quasi-experimentation – Design and Analysis Issues for Field Settings. Boston, Houghton Mifflin Company.

[18] Bezerra, C.M.M., Sampaio, S.C.B., Marinho, M.L.M. 2020. Secure Agile Software Development: Policies and Practices for Agile Teams. In: Quality of Information and Communications Technology. QUATIC 2020. Communications in Computer and Information Science, vol 1266. Springer, Cham. DOI: 10.1007/978-3-030-58793-2_28