UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO

PRÓ-REITORIA DE GRADUAÇÃO

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

CURSO DE BACHARELADO EM TECNOLOGIA DA INFORMAÇÃO

ROMULO ISMAEL PEREIRA SOBREIRA

AVALIANDO AS RECOMENDAÇÕES DE SEGURANÇA DA OWASP E ISO 25010: UMA VISÃO DOS PARTICIPANTES DE CURSOS DE CURTA DURAÇÃO

PAU DOS FERROS

2021

ROMULO ISMAEL PEREIRA SOBREIRA

AVALIANDO AS RECOMENDAÇÕES DE SEGURANÇA DA OWASP E ISO 25010: UMA VISÃO DOS PARTICIPANTES DE CURSOS DE CURTA DURAÇÃO

PAU DOS FERROS

2021

AVALIANDO AS RECOMENDAÇÕES DE SEGURANÇA DA OWASP E ISO 25010: UMA VISÃO DOS PARTICIPANTES DE CURSOS DE CURTA DURAÇÃO

Trabalho de Conclusão de Curso apresentado à Universidade Federal Rural do Semi-Árido – UFFERSA, *Campus* Pau dos Ferros, como requisito parcial para a obtenção do grau de Bacharel em Tecnologia da Informação.

Orientador: Prof. Dr. Reudismam Rolim de Sousa – UFERSA

PAU DOS FERROS

2021

P677a Pereira Sobreira, Romulo Ismael.
AVALIANDO AS RECOMENDAÇÕES DE SEGURANÇA DA OWASP E ISO 25010: UMA VISÃO DOS PARTICIPANTES DE CURSOS DE CURTA DURAÇÃO / Romulo Ismael Pereira Sobreira. - 2021.
78 f. : il.

Orientador: Reudismam Rolim de Sousa.
Monografia (graduação) - Universidade Federal Rural do Semi-árido, Curso de Tecnologia da Informação, 2021.

1. Aplicação Web. 2. Segurança. 3. Desenvolvimento Seguro. 4. Web. 5. OWASP. I. Rolim de Sousa, Reudismam, orient. II. Título.

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC´s) foi desenvolvido pelo Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) e gentilmente cedido para o Sistema de Bibliotecas da Universidade Federal Rural do Semi-Árido (SISBI-UFERSA), sendo customizado pela Superintendência de Tecnologia da Informação e Comunicação (SUTIC) sob orientação dos bibliotecários da instituição para ser adaptado às necessidades dos alunos dos Cursos de Graduação e Programas de Pós-Graduação da Universidade.

ROMULO ISMAEL PEREIRA SOBREIRA

AVALIANDO AS RECOMENDAÇÕES DE SEGURANÇA DA OWASP E ISO 25010: UMA VISÃO DOS PARTICIPANTES DE CURSOS DE CURTA DURAÇÃO

Monografia apresentada a Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Tecnologia da Informação.

Defendida em: 01/ 06/ 2021.

BANCA EXAMINADORA

REUDISMAM ROLIM DE SOUSA:08392843495 Assinado de forma digital por REUDISMAM ROLIM DE SOUSA:08392843495 Dados: 2021.06.04 11:15:28 -03'00'

Reudismam Rolim de Sousa, Prof. Dr. (UFERSA)
Presidente

KENNEDY REURISON LOPES:05655427451 Assinado de forma digital por KENNEDY REURISON LOPES:05655427451 Dados: 2021.06.04 11:22:31 -03'00'

Kennedy Reurison Lopes, Prof. Dr. (UFERSA)
Membro Examinador

WALBER JOSE ADRIANO SILVA:••••••••••

Walber José Adriano Silva, Prof. Dr. (UFERSA)
Membro Examinador

AGRADECIMENTOS

Agradeço à minha mãe Maria do Desterro Pereira Sobreira, e ao meu pai Francisco de Ismael Sobreira, por serem essenciais e presentes na minha vida. Esta monografia é apenas uma pequena prova de que todo o esforço de vocês, no final, valeu a pena. Agradeço a minha irmã Daniela Pereira Sobreira, a minha querida avó Eraldina Ferreira dos Anjos e aos meus amigos e amigas por me incentivarem em todos os momentos de dificuldade a ser uma pessoa cada vez melhor e a nunca desistir dos meus sonhos.

Agradeço também a minha tia Maria Noêmia Cavalcante da Silva e o seu marido Jurandir Joaquim da Silva, juntamente com meu tio Raimundo Cesário e minha madrinha Maria do Socorro Ismael da Silva, por sempre estarem ao meu lado me aturando quase que diariamente e sempre me ajudando, muito obrigado!

Agradeço também ao meu orientador Reudismam Rolim de Sousa por aceitar esse grande trabalho de me orientar, você me mostrou uma direção a seguir quando julguei que não fosse possível; você acreditou em mim até quando eu duvidei.

Agradeço aos professores Kennedy Reurison Lopes e Walber José Adriano Silva por aceitarem fazer parte da banca examinadora, vocês são professores que admiro muito e quero dizer que foi uma grande honra e prazer ter a oportunidade ter sido um aluno de vocês.

E também gostaria de agradecer a pessoas que não estão presentes neste momento, mas tiveram grande contribuição para este momento, meu padrinho Aquino Rodrigues da Silva, Meu tio Antônio Pereira dos Anjos, meu avô paterno Lourival Sobreira de Sousa e meu avô materno Bibiano Pereira do Anjos.

Agradeço também a nova família que a universidade meu deu, Heluan, Daniel, Alex, Euder, João Victor Queiroz, Ana Paula, João Victor Crescêncio e sua mãe Francisca Ferreira. E a meu primo Lucas Cavalcante sempre dando aquela moral para nos mantermos firmes e mantermos o foco nos nossos objetivos.

“Se o dinheiro for a sua esperança de independência, você jamais a terá. A única segurança verdadeira consiste numa reserva de sabedoria, de experiência e de competência.”

Henry Ford

RESUMO

As empresas que disponibilizam cursos de curta duração, que são realizados no período, tipicamente, de uma semana e o participante é apresentado a uma visão imersiva no tema que está sendo abordado. Os desenvolvedores de sistemas Web não apresentam como foco a utilização de orientações para prover o desenvolvimento seguro de aplicações Web. Nesse sentido, o presente trabalho propõe avaliar se os cursos de curta duração em questão levam a segurança da informação durante o desenvolvimento da aplicação sugerida. Com o objetivo de verificar também se problemas de segurança que podem ocorrer nas aplicações trabalhadas nos cursos de curta duração podem ser levados a projetos reais e também identificar a preocupação dos participantes desses cursos com segurança em suas práticas profissionais, foi realizada um *Survey*, com uma abordagem quantitativa para conhecer de forma correta e objetiva a adoção de práticas e técnicas de segurança relacionadas a OWASP e a ISO 25010. Foram também aplicadas técnicas e métodos de segurança nos projetos desenvolvidos nos cursos de curta duração, com o objetivo de aplicar e avaliar as recomendações propostas pela OWASP. O trabalho buscou observar as relevâncias das recomendações e técnicas de segurança utilizadas e a conscientização das pessoas envolvidas no projeto.

Palavras-chave: aplicação Web; segurança; desenvolvimento seguro; Web; Internet e OWASP.

ABSTRACT

Companies that provide short courses, which are held in a period typically of one week and the participant is presented with an immersive view of the topic being covered. Web system developers do not focus on the use of guidelines to provide secure development of Web applications. In this sense, the present work proposes to evaluate whether the short courses in question lead to information security during the development of the suggested application. With the objective of also verifying if security problems that can occur in the applications worked on in the short courses can be taken to real projects and also to identify the concern of the participants of these courses with security in their professional practices, a Survey was carried out, with a quantitative approach to know in a correct and objective way the adoption of security practices and techniques related to OWASP and ISO 25010. Safety techniques and methods were also applied in the projects developed in the short courses, with the objective of applying and evaluating the recommendations proposed by OWASP. The work sought to observe the relevance of the safety recommendations and techniques used and the awareness of the people involved in the project.

Keywords: Web application; security; secure development; Web; Internet and OWASP.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
API	Application Programming Interface
CWE	Common Weakness Enumeration
CVE	Commom Vulnerabilities and Exposures
DoS	Denial Of Service
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
OWASP	Open Web Application Security Project
ReDoS	Regular expression Denial of Service
SQL	Standard Query Language

SUMÁRIO

1 INTRODUÇÃO

Diante de uma sociedade moderna cada vez mais dependente de software para realizar suas atividades, as empresas se veem gradualmente mais preocupadas com a segurança da informação. No entanto, devido à necessidade de entregar soluções progressivamente mais complexas e em pouco tempo, as empresas de desenvolvimento de sistemas comumente focam em entregar as funcionalidades do sistema, em oposição a desenvolver um software com qualidade e livre de falhas de segurança (SOMMERVILLE, 2011). Dessa forma, os produtos de software podem ser entregues com vulnerabilidades de segurança, que podem ser exploradas por um atacante de forma a comprometer o sistema ou os negócios da empresa.

Para a produzir software mais seguro e auxiliar os pesquisadores a projetarem melhores ferramentas para tratar problemas de segurança, algumas empresas elencam as principais vulnerabilidades relacionadas a ataques em sistemas de software reais. Dentre essas empresas, a OWASP (*Open Web Application Security Project*) foca no desenvolvimento de aplicações seguras de software para os sistemas Web, ou seja, aqueles sistemas que estão disponíveis na internet por isso, são alvos fáceis de ataques de segurança (OWASP, 2017), demandando o desenvolvimento de um software seguro. A cada três anos, a OWASP lista os *top*-10 problemas de segurança relacionados ao desenvolvimento de sistemas Web. Por exemplo, uma das vulnerabilidades comuns é a SQL *Injection* (OWASP, 2017), que permite que um atacante possa realizar qualquer operação à sua escolha no banco de dados do sistema, que pode variar desde alterar algum dado ou remover completamente toda a base de dados.

Outro ambiente voltado para o desenvolvimento de sistemas seguros de *software* é a CWE (*Common Weakness Enumeration*). A CWE define uma lista formal das fraquezas dos softwares criados, com um intuito de permitir que as organizações tenham uma maior segurança de que os produtos que elas adquirem e desenvolvem estão livres de tipos conhecidos de falhas de segurança. Para isso, a CWE lista algumas categorias de fraquezas como comuns, como, por exemplo, o estouro de *buffer*, problemas de estrutura e validade, erro de canal e caminho, entre outros.

Segundo o *International Organization of Standardization* (ISO), que regulamenta padrões internacionais, oferecem especificações de classe mundial para produtos, serviços e sistemas, a norma específica foco deste trabalho é a ISO/IEC 25010, a qual se define em:

A. Um modelo de qualidade em uso composto de cinco características (algumas das quais são subdivididas em subcaracterísticas) que se relacionam com o resultado da interação quando um produto é usado em um contexto particular. Este modelo de sistema é aplicável ao sistema completo de humano-computador, incluindo tanto sistemas de computador em uso quanto produtos de software em uso.
B. Um modelo de qualidade de produto composto de oito características (que são subdivididas em subcaracterísticas) que se relacionam com propriedades estáticas de software e propriedades dinâmicas do sistema computador. O modelo é aplicável a sistemas de computador e produtos de software.

Ultimamente tornou-se comum a realização de cursos de curta duração. Visto que o período de realização dos cursos é curto, o tempo pode não ser suficiente para focar na resolução de problemas de segurança que porventura os softwares venham a ter. Notadamente, as práticas desenvolvidas ao longo dos cursos podem ser levadas para a atuação profissional dos participantes, o que pode fazer com que os problemas de segurança sejam disseminados para os projetos desenvolvidos pelos participantes.

Neste sentido, o propósito deste trabalho de conclusão de curso é avaliar a aplicação das recomendações de segurança da OWASP e também da ISO 25010 nos projetos desenvolvidos pelos participantes de cursos de curta duração, no intuito de compreender quais são os problemas de segurança mais enfrentados por esses sistemas. Para identificar que problemas de segurança estão presentes nos sistemas desenvolvidos nos cursos, foram utilizadas ferramentas de análise de código que identificam problemas de segurança em sistemas de software. Após a aplicação das ferramentas, os problemas foram analisados e classificados. Também foi realizado uma pesquisa com estudantes que participam destes cursos no sentido de identificar quais os problemas de segurança são alvos deles e se os participantes usam os códigos desenvolvidos nesses cursos em suas práticas profissionais, com ou sem adaptações, o que pode disseminar vulnerabilidades.

1.1 PROBLEMATIZAÇÃO

Ao longo do desenvolvimento de software, desde as fases iniciais de elicitação dos requisitos até a parte da implantação, a segurança, frequentemente, pode não ser um dos principais fatores considerados. De modo a compreender como medir riscos nessas aplicações e como as falhas podem gerar vulnerabilidades, a segurança de aplicações Web deve ser abordada desde o início do desenvolvimento, pois, geralmente, é mais barato construir um sistema seguro, do que corrigir os problemas após a entrega do produto ao cliente como versão final (SOMMERVILLE, 2011).

Como os processos de desenvolvimento de software focam em desenvolver um sistema de software no tempo preestabelecido, os problemas de segurança de software e como contorná-los podem não ser tratados devido à necessidade de desenvolver sistemas de forma rápida. Neste sentido, um software entregue que atenda aos requisitos funcionais do sistema é priorizado em detrimento de se desenvolver um sistema seguro. Dessa forma, os sistemas de software disponíveis na Web podem apresentar problemas de segurança.

1.2 JUSTIFICATIVA

A prática de priorizar o desenvolvimento de sistemas de software funcionais em vez de um produto como segurança podem resultar em problemas para o software e também para a empresa que vai perder possíveis clientes devido à má qualidade dos seus produtos. Em especial no contexto Web, os sistemas estão disponíveis para qualquer pessoa acessar, sendo essa uma das premissas da Web.

No entanto, nem todo sistema pode ser acessado de toda forma, um sistema bancário, por exemplo, terá um conjunto de funcionalidades disponíveis para o cliente, tais como consultar saldo, transferir, etc., mas, vários outros serviços estão disponíveis apenas para usuários de maior privilégio, tal como o gerente do banco. No entanto, um atacante pode invadir o sistema e de alguma forma acessar dados do qual o atacante não possui privilégios. Dessa forma, deve-se desenvolver sistemas de forma segura, principalmente se ele for disponibilizado na Internet.

1.3 OBJETIVOS

Nesta seção são apresentados os objetivos gerais e específicos do trabalho.

1.3.1 Objetivos Gerais

O trabalho objetiva avaliar a aplicação das recomendações de segurança da OWASP e da ISO 25010 nos projetos desenvolvidos pelos participantes de cursos de curta duração, no intuito de assimilar quais são os problemas de proteçaõ mais enfrentados por esses sistemas e se os problemas de segurança destes sistemas são levados para a atuação profissional dos participantes.

1.3.2 Objetivos Específicos

- Será primeiramente realizada uma análise da literatura para identificar quais são os principais aspectos relacionados ao tema proposto;
- Em seguida, serão identificadas ferramentas de código aberto que possam ser utilizadas para testar vulnerabilidades em sistemas de software;
- Logo, em seguida será definido um conjunto de produtos criados em cursos de curta duração para aplicação das técnicas elencadas;
- As ferramentas serão aplicadas aos sites selecionados, produzindo como resultado um conjunto de problemas de segurança;
- Esses erros relacionados a vulnerabilidades serão analisados e classificados conforme os problemas de segurança estabelecidos pela OWASP e ISO 25010;
- Será realizado um *Survey* com estudantes que participam dos cursos de curta duração;
- As respostas dos participantes serão analisadas conforme as recomendações da OWASP e ISO 25010.

O trabalho está subdividido em capítulos: este capítulo de introdução aborda a problematização do tema proposto, a justificativa do porquê do tema proposto e os objetivos do trabalho, subdividindo-se em objetivos gerais e específicos, respectivamente; no Capítulo 2, apresenta-se o referencial teórico, elencando temas, tais como segurança da informação, padrões de problemas de segurança e trabalhos relacionados, respectivamente; por outro lado, no Capítulo 3, aborda-se como a metodologia de elaboração do trabalho; já no Capítulo 4 é abordado os resultados das execuções das atividades do trabalho; por fim, no Capítulo 5 são apresentadas as considerações finais do trabalho.

2 REFERENCIAL TEÓRICO

Neste capítulo, descreve-se a base teórica que fundamenta a elaboração deste trabalho, sendo organizada nas seguintes subseções. Na Seção 2.1 é apresentada uma contextualização sobre segurança; na Seção 2.2 são descritos os conceitos inerentes a informação; na Seção 2.3 são apresentadas as normas presentes no trabalho sobre segurança da informação; na Seção 2.4 são apresentadas as vulnerabilidades mais críticas conforme a OWASP. Na seção 2.5 é apresentada a OWASP; na Seção 2.6 é apresentada a ISO 25010; na Seção 2.7 é apresentada uma descrição sobre os cursos de curta duração; e por fim, na Seção 2.8 são apresentados os trabalhos relacionados.

2.1 SEGURANÇA

Com relação às práticas de segurança utilizadas em torno da proteção da informação, na idade média, pode-se citar as bibliotecas. Nessa época, a principal dificuldade para a compra de livros era o fator econômico, visto que o preço do pergaminho era muito alto (ALEXANDRIA, 2009). A partir do século XIV, devido às novas técnicas de papelaria e à multiplicação das oficinas de papel, o uso do papel, até treze vezes mais barato que o pergaminho, propagou-se pela Europa. Porém, o custo das cópias ainda era muito elevado (CÂNDIDO & OLIVEIRA, 2005). Dessa forma, a biblioteca detinha um valor alto de mercado e representava uma forma de vantagem econômica e intelectual, deixada para os herdeiros (VERGER (1999, apud CÂNDIDO & OLIVEIRA, 2005).

Esta relação entre segurança e restrição à informação retoma-se, na história recente, com os regimes governamentais totalitaristas. No Brasil, durante o período da ditadura militar, de 1964 a 1985, os generais impuseram censura aos meios de comunicação de massa (ALEXANDRIA, 2009). Os atos institucionais, particularmente, em especial o AI-5, promulgado em 13 de dezembro de 1968, foram instrumentos ditatoriais de censura e ataques à liberdade de imprensa (acesso à informação). Durante este período era prática comum das forças de repressão do governo a invasão de redações de jornais e destruição de suas oficinas (SOARES, 1989).

2.2 INFORMAÇÃO

Como qualquer outro ativo importante, a informação é essencial para os

negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT NBR ISO/IEC 17799:200, 2005).

Segundo TOFLER (1990), a sociedade humana se rege em três poderes: força (o poder físico), riqueza (o poder econômico) e o conhecimento (o poder da informação). Contudo, no século contemporâneo, estamos sendo regidos pelo poder da informação. Logo, conforme o autor, após a Segunda Guerra Mundial, com o surgimento da comunicação, dos computadores, etc., começamos a perceber uma mudança na sociedade, em que a informação começou a ser o novo poder. A informação como poder tem algumas qualidades únicas, a citar: (I) ao contrário da riqueza, que originalmente se baseava nas propriedades de terra e ainda se baseia em propriedades de recursos finitos, a informação não está atrelada a recursos finitos, visto que os conhecimentos têm potencial praticamente inesgotável; (II) as informações são valiosas para o comércio, quando você as possui e alguém a deseja, mas se essas informações forem conhecidas por outras pessoas, elas se tornarão praticamente inúteis para você negociar, sendo úteis para outras aplicações; (III) a informação, diferentemente das mercadorias, não custa para se movimentar; (IV) as informações podem ser compartilhadas e usadas repetidamente, sem exaustão; (V) as informações podem ficar sem valor como resultado de algumas novas informações que as substituem ou as invalidem; isso não acontece com dinheiro – exceto nos casos de colapso econômico total.

A informação tem relação próxima com outros dois termos e costuma ser confundida, são eles dados e conhecimento. As diferenças entre eles são elencadas a seguir:

- **Dados**: são elementos fundamentais e brutos, ou seja, a matéria-prima da informação. Se você possui apenas dados brutos, não será possível decidir somente baseada nestes dados.
- **Informação**: é o conjunto de dados organizado de forma ordenada de modo a transmitir um significado dentro de um contexto. A informação nos dá a capacidade de tomar decisões sobre os mesmos dados que, isoladamente, não faziam muito sentido.
- **Conhecimento**: é o maior nível de abstração, quando um conjunto de

informações constitui um saber sobre determinado assunto. A informação passa a ter um valor agregado e pode ser utilizada para um determinado propósito.

2.3 SEGURANÇA DA INFORMAÇÃO

Segundo a norma NBR ISO/IEC 27002 (2005), a segurança da informação é a proteção da informação quanto a várias categorias de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio e maximizar o retorno sobre o investimento e as oportunidades de negócio (NBR ISO/IEC 27002).

Segundo Veronezi (2017) para que a informação possa ser repassada entre diversos atores, é necessário um mecanismo de transmissão; esta transmissão, também denominada comunicação, pode ser em tempo real, como em uma transmissão de vídeo ao vivo, ou então ela pode ser armazenada para ser acessada, como, por exemplo, no armazenamento de dados digitais em um *data center*, ou em um armazenamento físico, como em um livro.

A segurança da informação pode ser definida como a preservação da confidencialidade, da integridade e da disponibilidade da informação (NBR ISO/IEC 27002, 2005; Dantas, 2011), que podem ser definidas da forma seguinte:

- **Integridade**: a integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento (NBR ISO/IEC 27002:2005). Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, e que ela seja legítima e permaneça consistente. Ocorre a quebra da integridade quando a informação é corrompida, falsificada, roubada ou destruída. Garantir a integridade é manter a informação na sua condição original.
- **Disponibilidade**: a disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 27002:2005). Ocorre a quebra da disponibilidade quando a informação não está disponível para ser utilizada, ou seja, ao alcance de seus usuários e destinatários, não podendo ser acessada no momento em que for necessário utilizá-la. Garantir a disponibilidade é assegurar o êxito da leitura, do trânsito e do armazenamento da informação.

- **Confidencialidade**: a confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas (NBR ISO/IEC 27002:2005). Ocorre a quebra da confidencialidade da informação ao se permitir que pessoas não autorizadas tenham acesso ao seu conteúdo. A perda da confidencialidade é a perda do segredo da informação. Garantir a confidencialidade é assegurar o valor da informação e evitar a divulgação indevida.

Com a evolução da área de segurança da informação, observa-se a preocupação com outras propriedades, mais precisamente em relação ao processo de comunicação; a NBR ISO/IEC 17799:2001 estabelecia que a segurança da informação estava caracterizada pela preservação da confidencialidade, da integridade e da disponibilidade da informação. Já a NBR ISO/IEC 27002:2005 mantém esse conceito, acrescentando outras propriedades, tais como: autenticidade, responsabilidade, não repúdio e confiabilidade (DANTAS,2011), definidas como segue:

- **Autenticidade**: a autenticidade é a garantia de que a informação é oriunda da fonte que lhe é atribuída e elaborada por quem tem autoridade para tal.
- **Confiabilidade**: a confiabilidade é a garantia de que a informação é confiável, oriunda de uma fonte autêntica e que expressa uma mensagem verdadeira. A autenticidade e confiabilidade estão interligadas. A primeira diz respeito à idoneidade da fonte, isto é, digna de fé e confiança, e a segunda ao seu conteúdo. A avaliação da fonte para a sua autenticidade pode ser feita com relação à sua idoneidade, como, por exemplo: completamente idônea, regularmente idônea, inidônea e cuja idoneidade não se pode avaliar. E a avaliação da confiabilidade pode ser feita com relação ao seu conteúdo, como, por exemplo: confirmação por outras fontes, por ser verdadeira, duvidosa ou improvável.
- **Não repúdio**: o não repudio é garantia que o emissor ou pessoa que executou determinada transação de forma eletrônica, não poderá, posteriormente negar sua autoria.
- **Responsabilidade**: a responsabilidade é a coparticipação de

responsabilidades por todos os que produzem, manuseiam, transportam e descartam a informação, seus sistemas e redes de trabalho.

2.4 VULNERABILIDADES

Segundo Monteverde (2014) vulnerabilidades são condições que quando exploradas por pessoas mal intencionadas podem resultar em falhas de segurança. Dentre as vulnerabilidades existentes, as que afetam sistemas Web são estudadas e elencadas pela OWASP et al. (2017), sendo organizadas em uma lista com as dez vulnerabilidades mais críticas (OWASP Top10). A classificação da OWASP compreende aos seguintes grupos:

1. **Injeção** (*Injection*): ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta legítima. Os dados hostis do atacante podem enganar o interpretador levando-o a executar comandos não pretendidos ou a aceder a dados sem a devida autorização.
2. **Quebra de autenticação** (*Broken Authentication*): as funções da aplicação que estão relacionadas com a autenticação e gestão de sessões são muitas vezes implementadas incorretamente, permitindo que um atacante possa comprometer senhas, chaves, *tokens* de sessão, ou abusar de outras falhas da implementação que lhe permitam assumir a identidade de outros utilizadores (temporária ou permanentemente).
3. **Exposição de Dados Sensíveis** (*Sensitive Data Exposure*): muitas aplicações Web e APIs não protegem de forma adequada dados sensíveis, tais como dados financeiros, de saúde ou dados de identificação pessoal. Os atacantes podem roubar ou modificar estes dados mal protegidos para realizar fraudes com cartões de crédito, roubo de identidade, ou outros crimes. Os dados sensíveis necessitam de proteções de segurança extra como encriptação quando armazenados ou em trânsito, tal como precauções especiais quando trocadas com o navegador Web.
4. **Entidades Externas de XML** (XXE) (XML *External Entities*): muitos processadores de XML mais antigos ou mal configurados avaliam referências a entidades externas nos documentos XML. Estas entidades externas podem ser usadas para revelar arquivos internos, usando o processador de URI de documentos, realizar partilhas internas dos arquivos,

pesquisar portas de comunicação internas, realizar execução de código remoto e ataques de negação de serviço, tal como o ataque *Billion Laughs*.

5. **Quebra de Controle de Acessos** (*Broken Access Control*): as restrições sobre o que os utilizadores autenticados estão autorizados a fazer nem sempre são corretamente verificadas. Os atacantes podem abusar destas falhas para controlar funcionalidades ou dados para os quais não têm autorização, tais como dados de outras contas de utilizador, visualizar arquivos sensíveis, modificar os dados de outros utilizadores, alterar as permissões de acesso, entre outros.
6. **Configurações de Segurança Incorretas** (*Security Misconfiguration*): as más configurações de segurança são o aspecto mais observado nos dados recolhidos. Normalmente isto é consequência de configurações padrão inseguras, incompletas ou *ad hoc*, armazenamento na nuvem sem qualquer restrição de acesso, cabeçalhos HTTP mal configurados ou mensagens de erro com informações sensíveis. Não somente todos os sistemas operativos, *frameworks*, bibliotecas de código e aplicações devem ser configurados de forma segura, como também devem ser atualizados e alvo de correções de segurança antecipadamente.
7. ***Cross-Site Scripting*** (XXS): as falhas de XXS ocorrem sempre que uma aplicação inclui dados não-confiáveis numa nova página Web sem a validação ou filtragem apropriadas, ou quando atualiza uma página Web existente com dados enviados por um utilizador através de uma API do browser que possa criar JavaScript. O XXS permite que atacantes possam executar *scripts* no navegador da vítima, os quais podem raptar sessões do utilizador, descaracterizar sites Web ou redirecionar o utilizador para sites maliciosos.
8. **Desserialização Insegura** (*Insecure Deserialization*): desserialização insegura normalmente leva à execução remota de código. Mesmo que isto não aconteça, pode ser usada para realizar ataques, incluindo ataques por repetição, injeção e elevação de privilégios.
9. **Utilização de Componentes Vulneráveis** (*Using Components with Known Vulnerabilities*): componentes tais como, bibliotecas, *frameworks* e outros módulos de software, são executados com os mesmos privilégios que a aplicação. O abuso de um componente vulnerável pode conduzir a uma

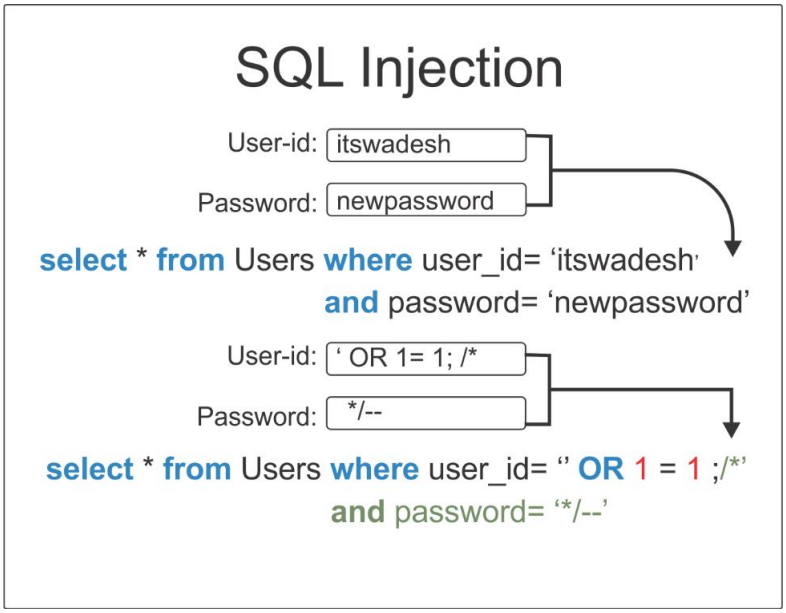
perda seria de dados ou controle completo de um servidor. Aplicações e APIs que usem componentes com vulnerabilidades conhecidas podem enfraquecer as defesas da aplicação, possibilitando ataques e impactos diversos.

10. **Registro e Monitorização Insuficiente** (*Insufficient Logging & Monitoring*): o registo e monitorização insuficientes, em conjunto com uma resposta a incidentes inexistentes ou insuficiente permite que os atacantes possam abusar do sistema de forma persistente, que o possam usar como entrada para atacar outros sistemas, e que possam alterar, extrair ou destruir dados.

2.4.1 EXEMPLOS DE VULNERABILIDADES

Para exemplificar as vulnerabilidades que um sistema Web pode conter, apresenta-se a vulnerabilidade *SQL-Injection*, que pode ser vista na Figura 1.

Figura 1 – Imagem ilustrando a exploração de uma vulnerabilidade



Fonte: Adaptado de (Gabriella Fonseca Ribeiro, 2011).

Na figura é mostrada a injeção do SQL nos campos de login de uma aplicação. No contexto esperado, um usuário fornece o seu login usual, no exemplo "*itswadesh*" e a sua senha, no exemplo "*newpassword*" e a aplicação avaliará se existe um usuário com aquelas credenciais válidas na aplicação.

No entanto, um usuário malicioso ao invés de inserir um nome de usuário válido pode incluir no campo de login um texto que faz parte da sintaxe SQL e dessa forma pode ser interpretado como um comando quando a aplicação realizar a consulta. No exemplo, o usuário digitou o texto 'OR 1=1; /* que interpretado pela aplicação gera a consulta SQL *select * from Users where* id='' *OR* 1 = 1; /* '*and password* ='*/. Dessa

forma o comando 1 = 1 é sempre avaliado como verdadeiro e é conectado por um conector lógico OR, que retorna verdadeira se pelo menos um dos lados da expressão for verdadeiro, o que resulta em uma expressão de valor Booleano verdadeiro, independentemente do valor de login. O restante da consulta SQL, inicia com o /*, que comenta o restante da consulta, dessa forma não avaliando a senha do usuário, que faz com que toda a tabela do usuário seja retornada. Dessa forma, o atacante possui controle total sobre a aplicação e pode executar qualquer consulta de seu interesse, desde acessar dados até mesmo deletar toda a base de dados.

Já na Figura 2 temos a ilustração do ataque XXE o *Billion Laughs,* conhecido como o ataque de um bilhão de risos ou também conhecido como XML *Bomb*. Segundo Soapui (2020), uma bomba XML é uma mensagem composta e enviada com a intenção de sobrecarregar um analisador XML (normalmente servidor HTTP). A entidade continua sendo resolvida para si mesma recursivamente, tornando as solicitações mais lentas e causando um ataque do DoS no aplicativo. Um ataque de *Billion Laughs* pode estar desabilitando o DOCTYPE como no trecho de código abaixo ou definindo um limite máximo na avaliação de entidades. O impacto do XXE e do *Billion Laughs*:

1. XXE pode causar vazamento de informações, ele pode vazar arquivos de sistema que possuem dados críticos.
2. Os dados obtidos do XXE podem ser usados para direcionar sites para vulnerabilidades adicionais.
3. Um *Billion Laughs* pode causar interrupção do serviço ou um ataque de negação de serviço.

Figura 2 – Ilustração de um ataque *Billion Laughs*

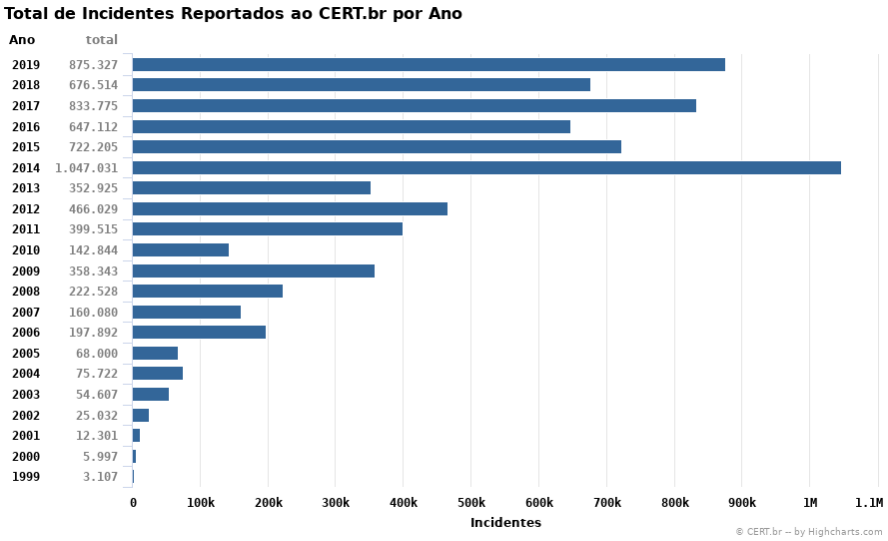
```
<?xml version="1.0"?>
<!DOCTYPE lolz [
   <!ENTITY lol "lol">
   <!ENTITY lol2 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
   <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
   <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
   <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
   <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
   <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
   <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
   <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

Fonte: Soapui (2020)

Diante disso, o CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), que é o órgão responsável por receber as

denúncias de falhas de segurança no Brasil, mostra estatísticas dos ataques que ocorrem de maneira corriqueira no país; as estatísticas são organizadas em gráficos, como pode ser visto nos Gráficos 1, 2 e 3.

Gráfico 1 - Quantidade de ataques registrados no Brasil desde o ano de 1999 até o ano de 2019.



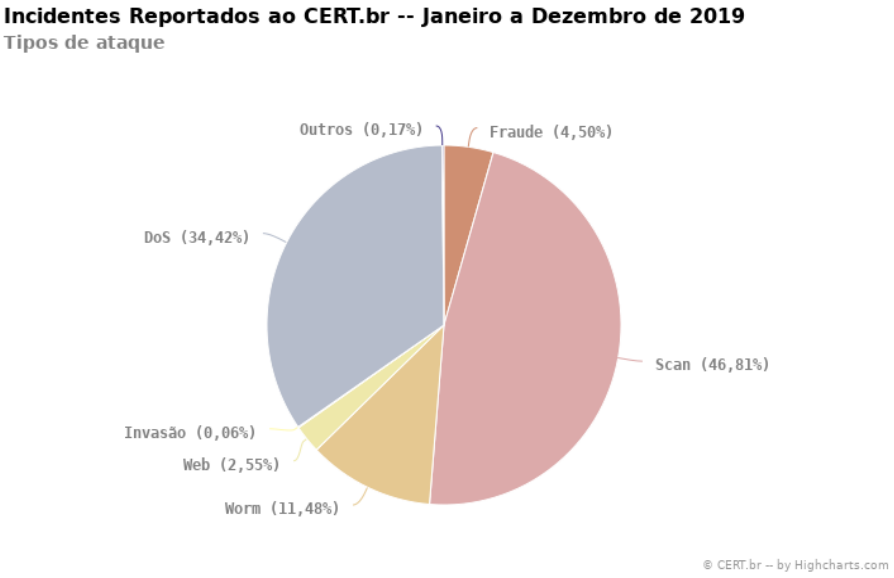
Fonte: CERT.br (2020)

O Gráfico 2 representa as categorias de ataques que foram feitos e registrados durante o ano de 2019. Para fins de melhorar a compreensão, a CERT.br disponibiliza a seguinte legenda:

- ***Worm***: notificações de atividades maliciosas relacionadas com o processo de automatização de propagação de código malicioso na rede.
- **Dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **Invasão**: um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede.
- **Web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- ***Scan***: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

- **Fraude**: segundo o dicionário Houaiss é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

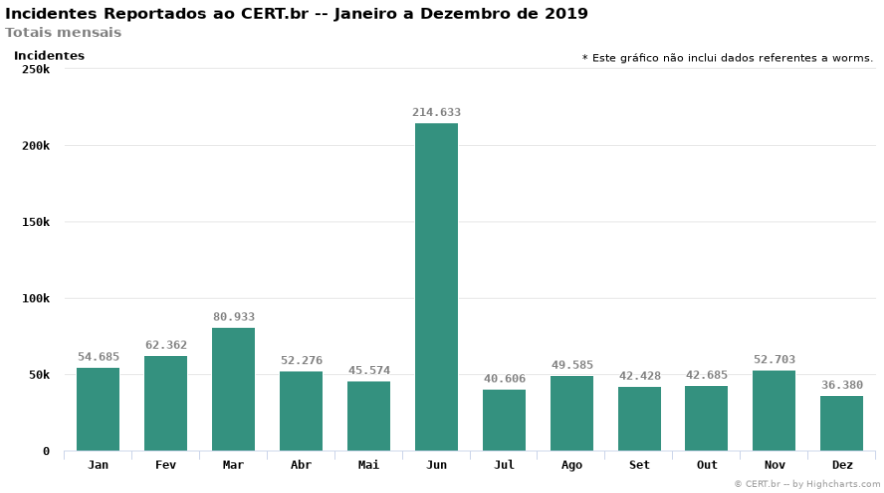
Gráfico 2 – Tipos de incidentes relatados ao CERT.br



Fonte: CERT.br (2020)

O Gráfico 3 mostra a quantidade de ataques por mês no ano de 2019. Um total de 101,477 mil ataques ocorreram no decorrer do ano. Vale a pena ressaltar que os ataques de *worms* não foram relatados nesse gráfico.

Gráfico 3 – Ataques por mês no ano de 2019



Fonte: CERT.br (2020)

2.5 OWASP

A OWASP é uma comunidade de livre acesso cujo enfoque é melhorar a segurança de aplicações Web. Sua missão é divulgar aspectos de segurança para esta categoria de aplicação, de forma que pessoas e organizações possam se manter informadas e com isso tomar as melhores decisões diante de riscos de segurança. Nesta comunidade é possível encontrar informações sobre as vulnerabilidades; explicações sobre como funcionam os ataques a essas; exemplos de teste caixa preta para identificar a vulnerabilidade; entre outros assuntos relacionados (OWASP).

Já na esfera das empresas de grande impacto no mercado, também existe a adoção de projetos do OWASP para mitigar ou prevenir possíveis riscos, ou vulnerabilidades na Web. A Microsoft, por exemplo, faz a utilização do projeto OWASP Top 10 para encontrar possíveis problemas de segurança no ciclo de vida de desenvolvimento de seus softwares (Sullivan 2008).

2.6 ISO 25010

A norma ISO/IEC 25010 é uma norma para Avaliação da Qualidade de Produtos de Software. Tal norma é uma atualização da norma ISO/IEC 9126. Tanto a ISO/IEC 9126 quanto a ISO/IEC 25010 consideram que a qualidade de um produto de software é obtida por um conjunto de atributos. Tais atributos representam características desejáveis em um software.

O modelo de qualidade é a base de um sistema de avaliação da qualidade do produto. O modelo de qualidade determina quais características de qualidade serão consideradas ao avaliar as propriedades de um produto de software. A qualidade de um sistema é o grau em que o sistema satisfaz as necessidades declaradas e implícitas de suas várias partes interessadas e, portanto, fornece valor. As necessidades dessas partes interessadas (funcionalidade, desempenho, segurança, manutenibilidade, etc.) são exatamente o que está representado no modelo de qualidade, que categoriza a qualidade do produto em características e subcaracterísticas. O modelo de qualidade do produto definido na ISO/IEC 25010 compreende oito características de qualidade, são elas:

1. **Adequação Funcional**: esta característica representa o grau em que um produto ou sistema fornece funções que atendem às necessidades declaradas

e implícitas quando usado sob condições especificadas.

2. **Eficiência de desempenho:** essa característica representa o desempenho em relação à quantidade de recursos usados nas condições estabelecidas.
3. **Compatibilidade**: O grau em que um produto, sistema ou componente pode trocar informações com outros produtos, sistemas ou componentes e/ou executar suas funções necessárias enquanto compartilha o mesmo ambiente de hardware ou software.
4. **Usabilidade**: o grau em que um produto ou sistema pode ser usado por usuários específicos para atingir objetivos específicos com eficácia, eficiência e satisfação em um contexto de uso especificado.
5. **Confiabilidade**: o grau em que um sistema, produto ou componente executa funções especificadas sob condições especificadas por um período especificado.
6. **Segurança**: o grau em que um produto ou sistema protege informações e dados para que pessoas ou outros produtos ou sistemas tenham o grau de acesso aos dados apropriado para seus tipos e níveis de autorização.
7. **Manutenibilidade**: esta característica representa o grau de eficácia e eficiência com que um produto ou sistema pode ser modificado para melhorá-lo, corrigi-lo ou adaptá-lo às mudanças do ambiente e dos requisitos.
8. **Portabilidade**: grau de eficácia e eficiência com que um sistema, produto ou componente pode ser transferido de um hardware, software ou outro ambiente operacional, ou de uso para outro.

2.7 CURSOS DE CURTA DURAÇÃO

Os cursos de duração são realizados no período, tipicamente, de uma semana e o participante é apresentado a uma visão imersiva no tema que está sendo abordado. Estes cursos tipicamente focam em atividades práticas direcionadas ao mercado de trabalho, possibilitando ao participante rapidamente aplicar os conceitos abordados no curso em suas práticas profissionais.

No contexto da tecnologia da informação, existem diversos cursos desta categoria que visam mostrar aos participantes temas como: linguagens de programação; tecnologia em alta no mercado, tais como React.js, Node.js, React native e Flutter. A participação nos cursos é, muitas vezes, motivada pelo interesse em adquirir colocação no mercado de trabalho ou de aperfeiçoar os conhecimentos

em um tema específico, para pôr em prática em seus projetos.

Porém, muitas vezes, como o tempo para desenvolver as atividades é bem curto, os cursos podem não abordar questões de segurança ou até mesmo ignorar quaisquer boas práticas neste sentido. Nesse contexto, o participante, que aprendeu uma forma específica de resolução de problemas, pode levar as práticas exercitadas no curso para o seu cotidiano e assim deixar seu sistema vulnerável a ataques.

2.8 TRABALHOS RELACIONADOS

Há na literatura alguns trabalhos relacionados a esta pesquisa, como o de ALEXANDRIA (2007), onde, o autor diagnosticou, avaliou a existência de lacunas na administração da segurança da informação da instituição avaliada (IPEN).

De modo similar, DE CARVALHO (2016), realizaram uma análise de vulnerabilidades existentes em aplicativos do sistema operacional Android, por exemplo, smartphones e tablets e posteriormente adaptada para diversos outros sistemas como relógios com o Android Wear,TV com Android TV, carros autônomos com o Android Auto. Para isso foram feitas algumas análises, por exemplo, Análise preliminar, engenharia reversa e ataques de rede, conforme os padrões OWASP e o auxílio de ferramentas de *pentesting*.

Por outro lado, COSTA et al. (2017), analisaram vulnerabilidades em portais de governos eletrônicos, buscando associar os recursos dos estados com seu nível de segurança apresentado em seus portais. Para isso, o autor do trabalho levantou uma hipótese de que existe uma relação entre segurança dos portais e o nível econômico de cada estado aos quais eles pertençam, em que estados mais ricos tendem a ter sites de governo eletrônico mais seguros do que estados mais pobres. E buscou-se provar essa hipótese durante o desenvolvimento do trabalho. A análise foi feita utilizando *scanners* (Uniscan, Skipfish, W3AF e Vega) e usou o NMAP para escanear portas UDP/TCP. Os sites escolhidos como alvos foram os dos governos estaduais de cada estado do Brasil, e também o site do Governo Federal, totalizando 28 portais. Logo após a coleta dos resultados foi utilizado a classificação do top-10 da OWASP onde A1 é a falha mais recorrente e A10 é décima falha mais recorrente, e colocadas em um gráfico tipo pizza, destacando-se entre A1, A2, …, A10.

De outra forma, MONTANHEIRO et.al. (2018) ressaltaram a necessidade de se pensar no quesito de segurança da informação desde o início do projeto de desenvolvimento do software, desde o levantamento de requisitos e a partir desse

momento, deve-se ter em mente que sistemas mal desenvolvidos podem ser invadidos a todo momento.

3 METODOLOGIA

Para atingir o objetivo geral do presente trabalho foi adotada uma metodologia do tipo *Survey,* na qual objetiva elencar informações de um público específico em busca de investigar um problema. E para buscar responder os objetivos específicos foram usadas algumas ferramentas.

3.1 FERRAMENTAS PARA DETECÇÃO DE PROBLEMAS DE SEGURANÇA SEGUNDO A OWASP E A ISO 25010

Uma das primeiras atividades do trabalho foi verificar a ocorrência de problemas de segurança nos sistemas desenvolvidos em cursos de curta duração. Para realizar essa atividade foram elencadas ferramentas que podem realizar essa análise de forma automática.

A OWASP lista um conjunto de ferramentas automatizadas para detecção de vulnerabilidades, que possuem diferentes categorias: pagas, gratuitas, que podem ser utilizadas em um período especifico ou livre para uso em sistemas de código aberto. Essas ferramentas são classificadas em diferentes categorias:

- **SAST**: Teste de segurança de aplicações estáticas (do inglês *Static Application Security Testing*).
- **DAST**: Teste de Segurança de Aplicações dinâmicas (do inglês *Dynamic Application Security Testing*);
- **OSS**: Ferramentas de segurança de software de código aberto (do inglês Open Source Software (OSS) Security);
- **Ferramentas de segurança incorporadas a ambientes DevOps/CI** (*Security Tools Built into DevOps/CI Environments*).

Para a condução do trabalho foram selecionadas ferramentas que englobam cada categoria. As ferramentas foram escolhidas por diferentes critérios, dentre eles a facilidade de uso; estarem incluídas na categoria de ferramentas *open source* ou serem de uso gratuito para projetos *open source*; e possuírem relatórios claros.

3.1.1 Ferramentas SAST

As ferramentas SAST analisam o código-fonte do sistema; dentre as ferramentas de código aberto e livres de uso, listadas pela OWASP[1], elencam-se as

[1] Disponível em: < https://owasp.org/www-community/Source_Code_Analysis_Tools >.

seguintes: LGTM.com, Coverity Scan Static Analysis, reshift, Xanitizer, HCL AppScan CodeSweep. Para o trabalho foram selecionadas as ferramentas LGTM e reshift do tipo SAST.

3.1.2 Ferramentas DAST

As ferramentas DAST [2]analisam aplicações web em execução, sem a análise do código-fonte do programa, em busca de vulnerabilidades, como *Cross-site scripting*, *SQL Injection*, *Command Injection*, *Path Traversal* e configurações inadequadas do servidor. Várias ferramentas comerciais e de código aberto dessa categoria estão disponíveis, cada qual com seus pontos fortes e fracos. Dentre as ferramentas nesta categoria estão: OWASP ZAP, Arachni, VWT Digital's sec-helpers, OWASP purpleteam. Neste nicho de ferramentas foi selecionada a ferramenta OWASP ZAP.

3.1.3 Diferença entre SAST e DAST?

As duas abordagens encontram tipos diferentes de vulnerabilidades, e são mais eficientes ou não conforme o momento em que são empregadas no ciclo de desenvolvimento. O SAST deve ser performado mais no começo e de preferência nos arquivos que contenham o código fonte. Contudo, visto que essa abordagem é feita sobre código estático, ela não identifica vulnerabilidades que surgem com a aplicação em produção.

O DAST, no que lhe concerne, deve ser aplicado no código em execução, em ambiente similar ao de produção. Contudo, o DAST é um teste mais complexo de se realizar, e as vulnerabilidades encontradas (que poderiam ter sido encontradas previamente com um SAST) tendem a ser empurradas para correção apenas no próximo início do ciclo de desenvolvimento.

3.1.4 Ferramentas OSS

As ferramentas OSS[3] analisam as bibliotecas ou componentes de código aberto que os desenvolvedores de aplicações utilizam para desenvolver rapidamente novas aplicações ou adicionar recursos às aplicações existentes. Dentre as ferramentas nesta categoria, incluem-se as seguintes: Snyk, SourceClear,

[2] Disponível em: < https://owasp.org/www-community/Vulnerability_Scanning_Tools >.
[3] Disponível em: < https://owasp.org/www-community/Free_for_Open_Source_Application_Security_Tools>.

WhiteSource, OWASP Dependency Check. Nesta categoria de ferramentas foi escolhida a ferramenta Snyk.

3.1.5 Justificando para escolha das ferramentas

As ferramentas descritas anteriormente detectam diferentes categorias de problemas, dentre os elencados pela OWASP, dado que elas afetam ou têm finalidades distintas; por exemplo, as ferramentas do tipo OSS não possuem como foco a detecção de problemas em consultas SQL, visto que elas visam encontrar vulnerabilidades em extensões do código como, por exemplo, bibliotecas, *frameworks*, etc.

Para permitir uma visão abrangente sobre a identificação de problemas de segurança, pelo menos uma ferramenta de cada categoria citada acima foi aplicada nos softwares analisados. Nesta direção, foram selecionadas duas ferramentas do tipo SAST, uma ferramenta do tipo DAST e uma da categoria OSS. Além dessas ferramentas, foi utilizado também o controle de qualidade de código do GtiLab *security & compliance*, que busca identificar problemas que permeiam todas as categorias citadas anteriormente. Nos testes das ferramentas do tipo SAST, foram utilizadas duas ferramentas, já que testes desse tipo podem retornar falsos positivos, um termo usado para indicar um arquivo ou entidade que foi marcado como malicioso de maneira incorreta, ou seja, trata-se de um trecho seguro.

Os problemas identificados pelas ferramentas são frequentemente categorizados de acordo com lista de CVEs (sigla inglesa para Vulnerabilidades e Exposições Comuns - *Common Vulnerabilities and Exposures*). O CVE é administrado pela MITRE Corporation e financiado pela da Agência de Segurança Cibernética e de Infraestrutura, que integra o Departamento de Segurança Interna dos EUA.

Além da lista de CVEs, as ferramentas podem incluir referências para fraquezas listadas na lista de CWE (do inglês *Common Weakness Enumeration* – enumeração de fraquezas comuns) – que contém a descrição dos defeitos, exemplos, possíveis ataques e remediações. Por exemplo, a ferramenta LGMT retorna a fraqueza de código CWE-089; a descrição e detalhes sobre essa CWE podem ser encontrados no site da mitre.

3.1.6 Diferença entre CVE e CWE

O termo CWE denota uma vulnerabilidade - não a instância dentro de um

produto ou sistema; no que lhe concerne, uma CVE denota a instância específica dentro de um produto ou sistema - não com a falha subjacente.

3.1.7 Tabela comparativa entre as ferramentas

O principal critério utilizado para a seleção das ferramentas foi a disponibilidade. Neste sentido, foram selecionadas ferramentas gratuitas ou gratuitas para uso em projetos *open sources*, com atualizações recentes e de fácil acesso. Para o trabalho, foram selecionadas seis ferramentas: duas do tipo SAST, uma da categoria DAST, uma do gênero OSS e o GitLab.

As ferramentas foram analisadas de acordo com suas funcionalidades, seguindo os seguintes critérios:

- **Relatório**: o relatório deve detalhar cada vulnerabilidade, além de indicar o ponto em que ela aconteceu. Devem existir opções de persistência para o dado relatório;
- **Usabilidade**: o quão fácil é utilizar a ferramenta;
- **Eficácia**: a quantidade de vulnerabilidades detectadas pela ferramenta, considerando a classificação da OWASP (OWASP et al., 2017).

A partir desses pontos foi feita avaliação das ferramentas e com base nos resultados foi elaborada a Tabela 1 que classifica as ferramentas considerando uma nota de 1 a 3 para cada critério, em que a nota 1 denota que a ferramenta não atendeu minimamente aos requisitos; o valor 2 indica que a ferramenta atendeu aos requisitos; o valor 3 denota que a ela supriu os requisitos acima do necessário.

Tabela 1 - Avaliação das ferramentas

Nome	Relatório	Usabilidade	Eficácia
LGMT	2	3	3
Reshift	2	3	3
OWASP ZAP	3	1	3
Synk	3	3	3
GitLab	2	3	3

Fonte: Autores

Referente à eficácia, todas as ferramentas cumprem, e até superam, este requisito. No entanto, no aspecto usabilidade, o cenário se torna um pouco diferente. As ferramentas LGMT, Reshift e Synk possuem uma interface intuitiva. Por outro lado, a ferramenta OWASP ZAP possui uma interface gráfica minimalista, mas não tão intuitiva; caso o usuário não saiba bem o que procura, terá dificuldades em usar a

ferramenta corretamente.

Por sua vez, o GitLab possui um relatório bem completo, permitindo ser exportado facilmente para outras ferramentas. Porém, os usuários podem ter dificuldades ao usar o arquivo exportado. As informações podem ficar confusas ao abrir o arquivo em softwares externos. Apesar de possuir relatório elaborado, tanto a LGMT quanto Reshift receberam notas baixas. A segunda por não permitir exportar as saídas para outros formatos, fazendo com que o usuário fique preso ao ambiente, e a primeira por possuir um erro na exportação do relatório, não permitindo a abertura do arquivo exportado em outros softwares, limitando o usuário ao ambiente da ferramenta.

3.2 PESQUISA COM ALUNOS DA GRADUAÇÃO E PROFISSIONAIS DA ÁREA DE DESENVOLVIMENTO DE SOFTWARE

A segunda etapa do estudo foi a realização de um *Survey* com participantes de cursos de curta duração para identificar a percepção deles sobre a adoção de práticas de segurança nos cursos de curta duração e em suas práticas profissionais. Estudos do tipo *Survey* são realizados com a finalidade de produzir estatísticas, isto é, descrições quantitativas ou numéricas de alguns aspectos da população de estudo. Esta categoria de pesquisa pode ser realizada através de questionários de coleta de dados, entrevistas estruturadas ou técnicas de registro de logs.

O *Survey* foi realizado com graduandos através de um questionário *on-line* para coleta de dados. Na Seção 3.2.1 é abordada a execução do *Survey* e na Seção 3.2.2 são elencados os procedimentos de análise deste estudo.

3.2.1 Execução

O questionário do *Survey* ficou aberto à recepção de respostas no período de 12 de abril até 21 de abril de 2021 pouco discentes se propuseram para responder à pesquisa apesar do curto espaço de tempo o questionário foi enviado duas vezes para todos os alunos da graduação em tecnologia da informação. O questionário foi enviado aos discentes, por e-mail, através da coordenação do curso Interdisciplinar em Tecnologia da Informação do Campus Pau dos Ferros da Universidade Federal Rural do Semi-Árido (UFERSA). A pesquisa também foi enviada para grupos de alunos que incluem discentes dos cursos de Engenharia de Software ou Engenharia de Computação da UFERSA/Pau dos Ferros. No total foram obtidas 15 respostas dos

discentes. Pode ter ocorrido de os alunos não terem checado os seus e-mails que estão cadastrados no sistema da UFERSA que pode ter acarretado no pouco número de respostas, todas as respostas foram coletadas e consideradas como validas, visto que no questionário a maioria das perguntas eram objetivas, que não dava margem para o participante inserir dados de maneira equivocada.

O questionário foi organizado em seções da seguinte forma: 1) dados gerais dos discentes; 2) participação dos discentes em cursos de curta duração; 3) a adoção de métricas de segurança em cursos de curta duração; 4) adoção de métricas de segurança na atuação profissional. Para preservar a identidade dos discentes, as informações dos relatórios foram anonimadas. As questões elencadas no *Survey* podem ser vistas na Tabela 2.

3.2.2 Procedimentos de Análise

Para a análise dos dados obtidos por meio do questionário foi aplicada uma análise quantitativa para as respostas objetivas.

A análise dos dados foi conduzida em caráter quantitativo. A análise quantitativa foi baseada nas respostas fornecidas por meio da Escala Likert, com itens de 1 a 5 (1 = Discordo Totalmente, 2 = Discordo, 3 = Neutro, 4 = Concordo, 5 = Concordo Totalmente).

Na Tabela 2 podem ser vistas as perguntas que foram realizadas no questionário.

Tabela 2 - Perguntas investigadas no *Survey*

	Perguntas objetivas
Parte I	1. Curso
Parte II	2. Você já participou de cursos de curta duração? Como, por exemplo: AluraFlix, JS Expert, MaratonaDev, NextLevel, etc. 3. Caso a resposta anterior tenha sido "Sim", qual das opções abaixo você participou? Com as opções de múltiplas escolhas: AluraFlix, JS Expert, MaratonaDev, NextLevel e outros. 4. Você costuma utilizar parte dos projetos desenvolvidos em suas atuações profissionais? 5. Caso tenha participado de alguma(s) formação(ões), elas tratavam problemas de segurança durante o desenvolvimento? 6. Você costuma levar questões de segurança em consideração quando desenvolve suas práticas profissionais? 7. Há quanto tempo você trabalha em projetos reais?
Parte III	8. O(s) curso(s) de curta duração que você fez abordam ou abordaram algumas das questões a seguir: 9. Os cursos de formação de curta duração abordaram as métricas de confiabilidade a seguir: 10. Os cursos de formação de curta duração abordaram as métricas de Integridade a seguir: 11. Os cursos de formação de curta duração abordaram as métricas de rastreabilidade a seguir: 12. Os cursos de formação de curta duração abordaram as métricas de Autenticidade a seguir:
Parte IV	13. Em suas práticas profissionais você aborda ou abordou algumas das questões a seguir: 14. Em suas práticas profissionais você aborda ou abordou as métricas de confiabilidade a seguir: 15. Em suas práticas profissionais você aborda ou abordou as métricas de Integridade a seguir: 16. Em suas práticas profissionais você aborda ou abordou as métricas de Disponibilidade a seguir: 17. Em suas práticas profissionais você aborda ou abordou as métricas de Autenticidade a seguir:

Fonte: Autores

Por sua vez, na Tabela 3 podem ser vistos as opções das questões referente à métrica confidencialidade.

Tabela 3 - Métricas de confidencialidade

Id	Nome da métrica
1	Controle de acesso
2	Proteção de informações de registro (Log)
3	Controle contra código malicioso
4	Gerenciamento de mídia removível
5	Sessão expirada
6	Força do algoritmo de criptografia
7	Correlação de criptografia de dados
8	Gerenciamento de chave de criptografia

Fonte: Adaptado de SAPTARINI et al

Já na Tabela 4 podem ser vistos as opções das questões referente à métrica integridade.

Tabela 4 - Métricas de integridade

Id	Nome da métrica
1	Conformidade de dados
2	Prevenção de corromper dados internos
3	Inventário de ativos
4	Backup de informações
5	Procedimentos operacionais documentados

Fonte: Adaptado de SAPTARINI et al

De outra forma, na Tabela 3 podem ser vistos as opções das questões referente à métrica disponibilidade.

Tabela 5 - Métricas de disponibilidade

Id	Nome da métrica
1	Disponibilidade de acesso
2	Disponibilidade de login
3	Disponibilidade de permanência de registro do sistema (Log)

Fonte: Adaptado de SAPTARINI et al

Já na Tabela 6 podem ser vistos as opções das questões referente à métrica autenticidade.

Tabela 6 - Métricas de autenticidade

Id	Nome da métrica
1	Protocolo de autenticação
2	Registro de usuário
3	Gerenciamento de senha do usuário
4	Gerenciamento de privilégio de usuário
5	Restrição de acesso de informação

Fonte: Adaptado de SAPTARINI et al.

4 RESULTADOS DA EXECUÇÃO DAS FERRAMENTAS

Neste capítulo são apresentados os resultados da execução das ferramentas. Na Tabela 7 podem ser vistos os resultados apresentados por cada uma das ferramentas.

Tabela 7 - resultados dos resultados por projeto

Projeto	SAST	DAST	OSS	GitLab
Semana Omnistack	7	60	6	4
AluraFlix	0	16	1	0
JSExpert	9	24	6	61

Fonte: Autores

Na Tabela 8 pode ser vista a distribuição entre as vulnerabilidades descobertas e a classificação da Owasp et al. (2017), considerando a classificação das 10 vulnerabilidades mais graves e recorrentes em sistemas web. Pode ser observado que a vulnerabilidade com o maior número de ocorrências é a A10, seguido de A2 e A1. A utilização da letra A, seguida do número se refere a cada uma das vulnerabilidades citadas na Seção 2, sendo descritas abaixo:

- A1 - Injeção;
- A2 - Quebra de autenticação;
- A3 -Exposição de Dados Sensíveis;
- A4 - Entidades Externas de XML (XXE);
- A5 - Quebra de Controle de Acessos;
- A6 -Configurações de Segurança Incorretas;
- A7 - *Cross-Site Scripting* (XXS);
- A8 - Desserialização Insegura;
- A9 - Utilização de Componentes Vulneráveis;
- A10 - Registro e Monitorização Insuficiente.

Tabela 8 - Vulnerabilidades de acordo com classificação de (OWASP et al., 2017)

Vulnerabilidades	SAST	DAST	OSS	GitLab
A1	3	0	24	169
A2	0	0	0	0
A3	0	0	0	0
A4	0	0	5	0
A5	4	71	115	34
A6	9	50	0	0
A7	0	0	11	0
A8	0	0	0	0
A9	0	0	2	0
A10	0	0	0	0

Fonte: Autores

Na Tabela 9 podem ser observadas as distribuições das vulnerabilidades mostradas na Tabela 4 considerando o curso de curta duração na qual a mesma foi detectada, ainda considerando a notação anterior.

Tabela 9 - Tabela de Resultados por projeto

Projeto	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Semana Omnistack	19	0	0	5	121	30	11	0	2	0
AluraFlix	3	0	0	0	34	8	0	0	0	0
JSExpert	174	0	0	0	69	21	0	0	0	0

Fonte: Autores

Na Tabela 9 pode ser visto também o mapeamento entre as vulnerabilidades e os projetos analisados de acordo com sua classificação perante o top-10 2017 da OWASP.

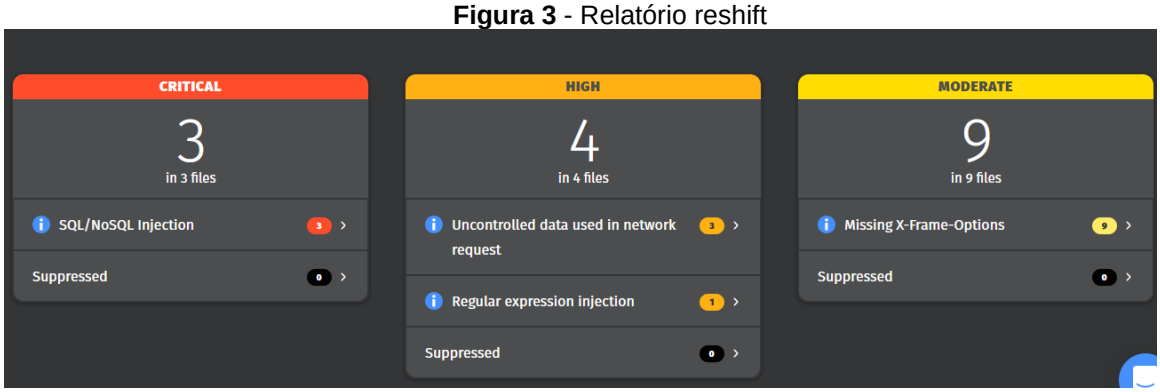
4.1 RESULTADOS DAS FERRAMENTAS SAST

Nesta seção serão apresentados os resultados das ferramentas SAST, as quais foram selecionadas Reshit e LGMT para esse tipo de teste.

4.1.1 Ferramenta Reshit

Reshit é uma ferramenta que usa análise de código estático para verificar vulnerabilidades e usa aprendizado de máquina para fornecer uma previsão de falsos positivos. Esta ferramenta suporta Java, NodeJS e JavaScript. Os projetos selecionados foram feitos em JavaScript. Na Figura 3 podem ser vistos os resultados classificados entre: crítica, alta e moderada.

Figura 3 - Relatório reshift



Fonte: Autores

Na Figura 3 pode ser vista uma falha crítica com classificação A1, ou seja, uma falha de injeção. Falhas de injeção, tais como injeções de SQL, OS e LDAP ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta legítima. Os dados *hostis* do atacante podem enganar o interpretador o levando a executar comandos não pretendidos ou a aceder a dados sem a devida autorização.

Para a solução de vulnerabilidades desse tipo a OWASP indicar uma folha de dicas de defesa contra injeção de SQL, listados a seguir:

Uso de declarações preparadas (com consultas parametrizadas): este método permite que o banco de dados reconheça o código e o diferencie dos dados de entrada. A entrada do usuário é analisada automaticamente e não causará a alteração da intenção da consulta SQL; portanto, esse estilo de codificação ajuda a mitigar um ataque de injeção de SQL.

Uso de procedimentos armazenados: exigem que o desenvolvedor agrupe uma ou mais instruções SQL em uma unidade lógica para criar um plano de execução. As execuções subsequentes permitem que as instruções sejam parametrizadas automaticamente. As instruções podem ser armazenadas para execução posterior. Nesse sentido, quando for preciso executar uma consulta, em vez de escrevê-la indefinidamente, você pode apenas chamar o procedimento armazenado.

Validação de entrada da lista branca: o processo de validação visa verificar se a categoria de entrada enviado por um usuário é permitido ou não. A validação da entrada garante que seja o tipo, comprimento, formatos aceitos e assim por diante. Apenas os valores que passam na validação podem ser processados. Essa abordagem ajuda a neutralizar quaisquer comandos inseridos na *string* de entrada. Fazendo uma relação com o mundo real, a validação da entrada se assemelha a verificar quem está batendo na porta antes de abri-la.

A validação não deve ser aplicada apenas a campos que permitam aos usuários digitarem uma entrada, também devem ser considerados as situações seguintes na mesma medida:

- Use expressões regulares como listas de permissões para dados estruturados (como nome, idade, renda, resposta à pesquisa, código postal) para garantir uma validação de entrada forte.
- No caso de um conjunto fixo de valores (como lista suspensa, botão de rádio), determine qual valor é retornado. Os dados de entrada devem corresponder exatamente a uma das opções oferecidas.

Escapar de todas as entradas fornecidas pelo usuário: sempre use funções de escape de caractere para entrada fornecida pelo usuário, fornecida para cada sistema de gerenciamento de banco de dados (DBMS). Isso é feito para garantir que o DBMS nunca o confunda com a instrução SQL, fornecida pelo usuário. Por exemplo, use mysql_real_escape_string() em PHP para evitar caracteres que podem levar a um comando SQL não intencional.

4.1.2 Ferramenta LGTM

LGTM é uma plataforma de análise que verifica automaticamente códigos em busca de CVEs reais e vulnerabilidades. Ao combinar a pesquisa profunda de código semântico com *insights* de ciência de dados, o LGTM classifica os resultados mais relevantes para mostrar apenas os alertas que importam. A ferramenta oferece ideias de uma grande comunidade de pesquisadores de segurança para ajudar os desenvolvedores a enviar código seguro, mostrando erros e possíveis soluções.

Na Figura 4, 5 e 6, respectivamente, pode ser vista a CWE-089, sendo a mesma falha da categoria A1 de injeção. Se uma consulta de banco de dados (como uma consulta SQL ou NoSQL) for criada a partir de dados fornecidos pelo usuário sem sanitização suficiente, um usuário mal-intencionado poderá executar consultas mal-intencionadas de banco de dados, como discutido anteriormente. A maioria das bibliotecas de conectores de banco de dados oferecem maneiras de evitar a inserção de dados não confiáveis em uma consulta por parâmetros de consulta ou instruções preparadas. Para consultas NoSQL, por exemplo, no MongoDB, deve-se usar um operador como $ eq para garantir que dados não confiáveis sejam interpretados como um valor literal e não como um objeto de consulta.

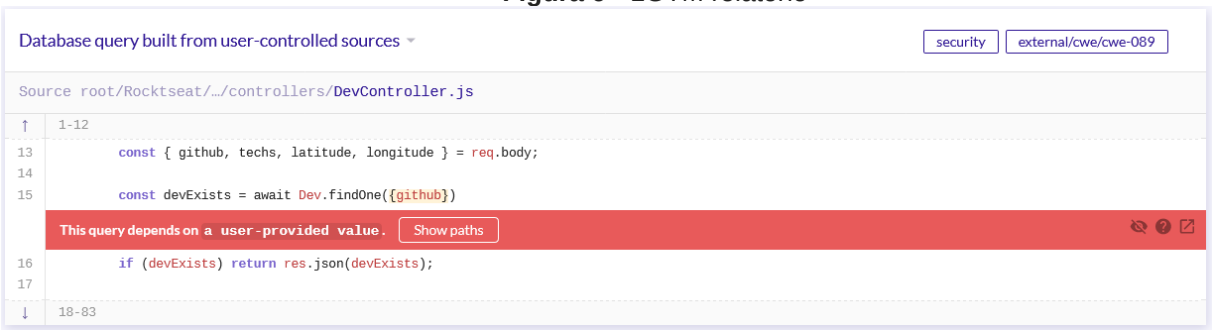
Figura 4 - LGTM relatório

Fonte: Autores

Figura 5 - LGTM relatório

Fonte: Autores

Figura 6 - LGTM relatório



Fonte: Autores

Já na Figura 7 pode ser vista a CWE-730 e uma CWE-400, que remetem a uma falha da categoria A9, sendo uma negação de serviço. Esse problema pode ser ocasionado por uma expressão regular com entrada do usuário não analisada. Neste caso, um usuário mal-intencionado pode ser capaz de modificar o significado da expressão. Em particular, esse usuário pode ser capaz de fornecer um fragmento de expressão regular que leva tempo exponencial no pior caso e usá-lo para realizar um ataque de negação de serviço.

Figura 7 - LGTM relatório

Fonte: Autores

A falha a cima pode proporcionar uma negação de serviço de expressão regular (ReDoS) que é um ataque de negação de serviço, no qual explora que a maioria das implementações de expressão regular pode atingir situações extremas que fazem com que funcionem muito lentamente (relacionado exponencialmente ao tamanho da entrada). Desse modo, um invasor pode fazer com que um programa usando uma expressão regular entre nessas situações extremas e, em seguida, pare por um longo tempo.

A sugestão para esses defeitos é usar funções de limpeza como lodash _.escapeRegExp para escapar metacaracteres com significado especial antes de usar a entrada do usuário em expressões regulares. Em vez disso, os parâmetros da solicitação devem ser processados primeiro, por exemplo, usando a função _.escapeRegExp no pacote lodash. Isso garante que os usuários não possam inserir caracteres com significado especial em expressões regulares.

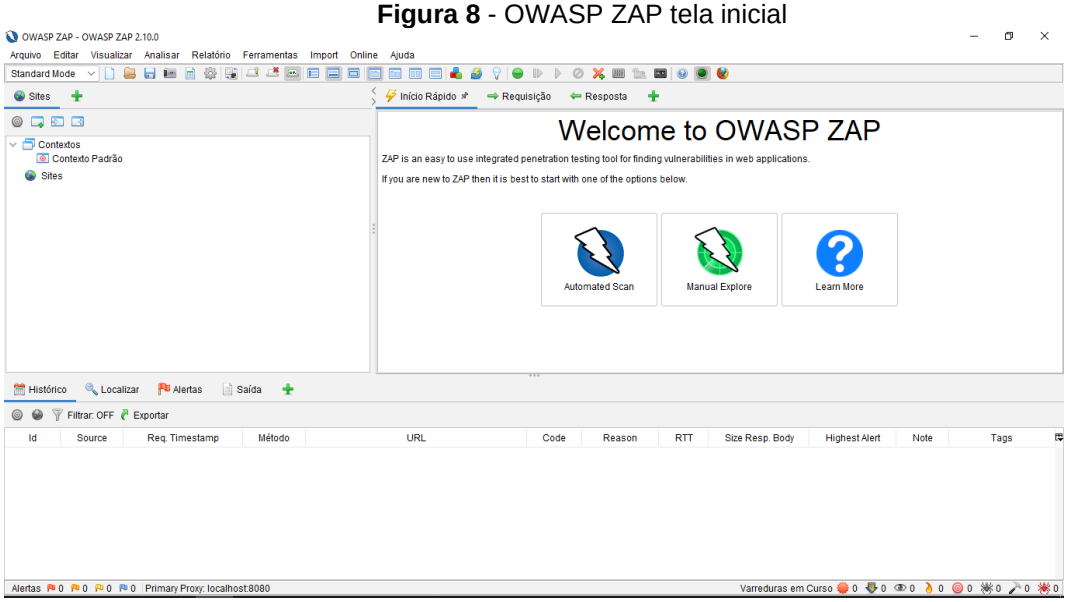
4.2 RESULTADOS DAS FERRAMENTAS DAST

Nesta seção serão apresentados os resultados da ferramenta escolhida do tipo DAST; a ferramenta selecionada foi o OWASP ZAP para esse tipo de teste.

4.2.1 OWASP ZAP

Na Figura 8 pode ser vista a tela inicial da ferramenta OWASP ZAP, que nos demonstra duas opções de *scan* que são automática e manual.

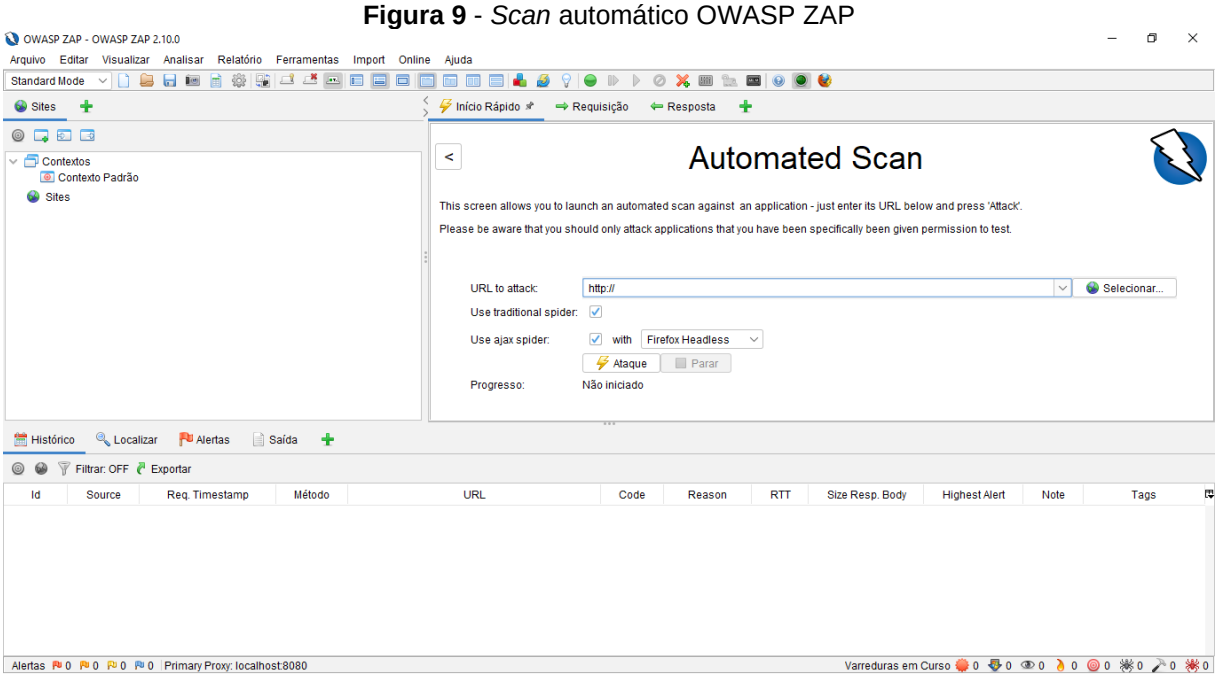
Figura 8 - OWASP ZAP tela inicial



Fonte: Autores

Na Figura 9 pode ser vista a tela do *scan* automático, o qual foi utilizado para identificar as vulnerabilidades nos projetos estudados.

Figura 9 - *Scan* automático OWASP ZAP



Fonte: Autores

Na Figura 10 pode ser visto o relatório do OWASP ZAP. Nessa figura é demonstrada a quantidade de falhas e a gravidade da mesma, classificada em Alta, Média, baixa e informal; logo abaixo é relatado as possíveis falhas e, respectivamente, seu grau de ofensividade.

Figura 10 - Relatório OWASP ZAP

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	2
Informational	1

Alerts

Name	Risk Level	Number of Instances
Cross-Domain Misconfiguration	Medium	3
X-Frame-Options Header Not Set	Medium	2
Incomplete or No Cache-control and Pragma HTTP Header Set	Low	3
X-Content-Type-Options Header Missing	Low	3
Information Disclosure - Suspicious Comments	Informational	4

Fonte: Autores

Por sua vez, na Figura 11 podem ser vistas as falhas que foram detectadas pelo escaneamento automático com um nível de detalhamento completo, pois ele indica se existe uma CWE para a vulnerabilidade que foi encontrada, fornece também uma possível solução para o problema e também uma descrição da vulnerabilidade, caso ela seja conhecida.

Figura 11 - Relatório OWASP ZAP

Alert Detail

Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://alura-ministrante.vercel.app
Method	GET
Evidence	access-control-allow-origin: *
URL	https://alura-ministrante.vercel.app/
Method	GET
Evidence	access-control-allow-origin: *
URL	https://alura-ministrante.vercel.app/robots.txt
Method	GET
Evidence	access-control-allow-origin: *
Instances	3
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html
CWE Id	264
WASC Id	14
Source ID	3

Fonte: Autores

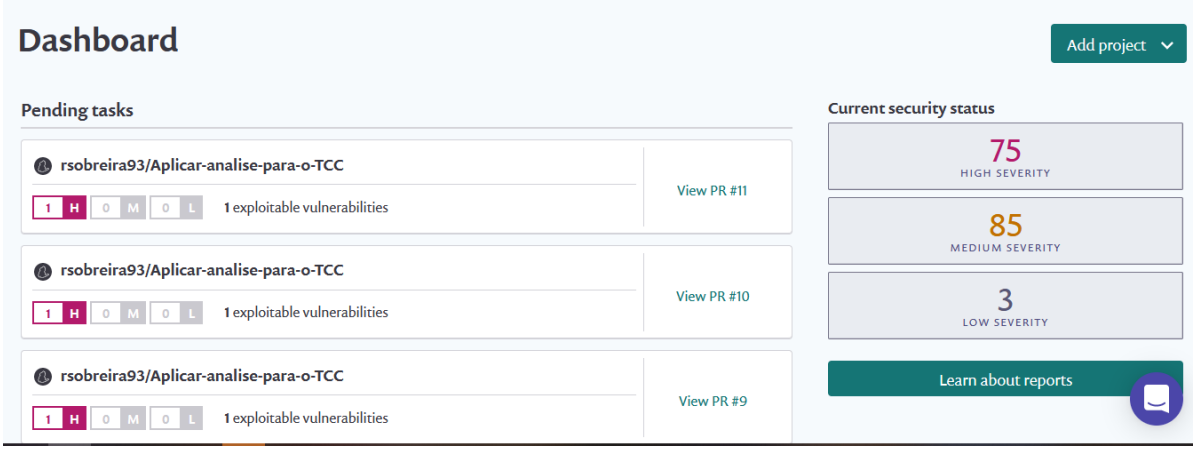
4.3 RESULTADOS DA FERRAMENTA OSS

Nesta seção serão apresentados os resultados da ferramenta escolhida do tipo OSS; a ferramenta selecionada foi o Snyk para esse tipo de teste.

4.3.1 Ferramenta snyk

A snyk é uma ferramenta comercial, mas gratuita para projetos de código aberto. Ela analisa se as dependências têm vulnerabilidades conhecidas e também fornece informações detalhadas e orientações de correção para vulnerabilidades conhecidas.

Figura 12 - Synk relatório



Fonte: Autores

Na Figura 12 pode ser visto o *dashboard* da ferramenta, que lista a quantidade de vulnerabilidades. Dentre as vulnerabilidades se destacam as CWE-400, que já foi mencionada anteriormente; já a CWE-094 e a CWE-078 serão mencionadas logo abaixo.

A CWE-094 é da categoria A1. A vulnerabilidade está relacionada à injeção de código arbitrário. Especificamente, o problema relatado está relacionado ao uso da biblioteca serialize-javascript. O serialize-javascript é um pacote para serializar JavaScript em um superconjunto de JSON, que inclui expressões regulares e funções. Para resolver essa vulnerabilidade basta atualizar o serialize-javascript para a versão 3.1.0 ou superior.

A CWE-078 também é da categoria A1, neste caso injeção de comando. Especificamente, o problema relatado está associado ao uso da biblioteca lodash. A lodash é uma biblioteca de utilitários JavaScript moderna que oferece modularidade, desempenho e extras. As versões afetadas deste pacote são vulneráveis à injeção de comando via modelo. Para resolver essa falha é preciso atualizar o lodash para a versão 4.17.21 ou superior.

Considerando as vulnerabilidades destacadas anteriormente é importante destacar a diferença entre injeção de código e injeção de comando, destacadas a seguir:

- **Injeção de código:** a injeção de código é um estilo específico de ataque de injeção em que uma instrução de programa executável é feita envolvendo a entrada do usuário em uma superfície de ataque que se torna vulnerável quando pode ser manipulada de uma maneira imprevista para invocar uma funcionalidade que será usada para causar danos. A injeção de código pode

ser um risco com linguagens que executam ou interpretam *scripts* devido à conveniência de executar uma string como uma instrução executável ou instruções em tempo de execução. Por exemplo, as linguagens que possuem essa capacidade incluem JavaScript, Perl, Python e Ruby.

- **Injeção de comando:** no caso de injeção de comando, a vulnerabilidade se deve à construção desajeitada de um comando shell que inclui dados de tempo de execução que o invasor pode influenciar. Essa classe de ataques de injeção também é chamada de “injeção de casca”.

A essência desses ataques é que a entrada maliciosa de uma superfície de ataque é empregada para coagir um comando construído a realizar ações prejudiciais imprevistas quando executado por um *shell* que o programa invoca. A diferença na nomenclatura é simplesmente entre o significado alterado do comando ou o efeito alterado do processo do *shell* executando o mesmo comando.

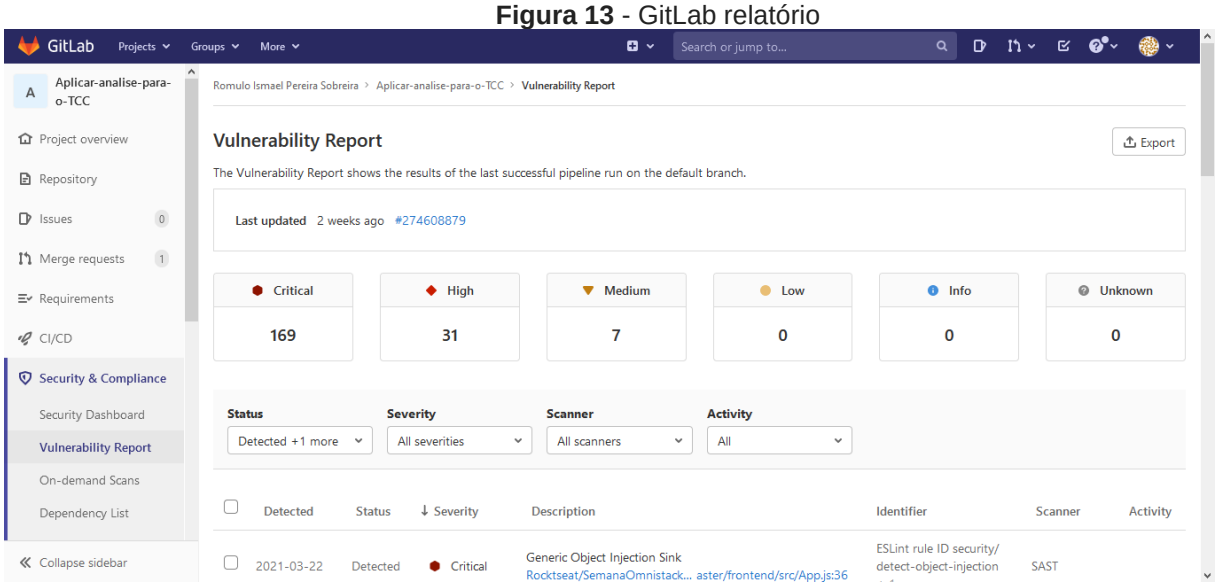
4.4 PLATAFORMA GITLAB

A plataforma GitLab é um repositório de código. Esta plataforma está aperfeiçoando uma ferramenta de segurança, que está evoluindo rapidamente. A plataforma está reunindo as melhores ferramentas de código aberto gratuitas que podem ser encontradas e as estão integrando no *pipeline* de integração contínua CI (do inglês *Continuous Integration*) do GitLab para facilitar sua ativação. Isso inclui muitas categorias de segurança. A imagem abaixo é referente aos resultados obtidos após a execução da ferramenta de segurança, onde a classificação das vulnerabilidades são: crítica, alta, média, baixa, informação (aviso de mau uso ou coisa do tipo) e vulnerabilidades desconhecidas.

Esta ferramenta executa testes para as categorias SAST, DAST e OSS, mas neste caso ela executou os testes do tipo SAST, pois os DAST necessitavam que os alvos estivessem *on-line*, ou seja, estivessem disponíveis em um servidor.

Na Figura 13 podem ser vistas as vulnerabilidades encontradas pela ferramenta de segurança do GitLab. As análises feitas pela ferramenta do GitLab encontraram problemas críticos de segurança relatados e documentados pela CWE-094, uma falha A1. O GitLab também identificou falhas altas (*high*), documentadas pela CWE-400, vulnerabilidade A5, e falhas médias (*medium*), relatadas pela CWE-185, também uma falha A5.

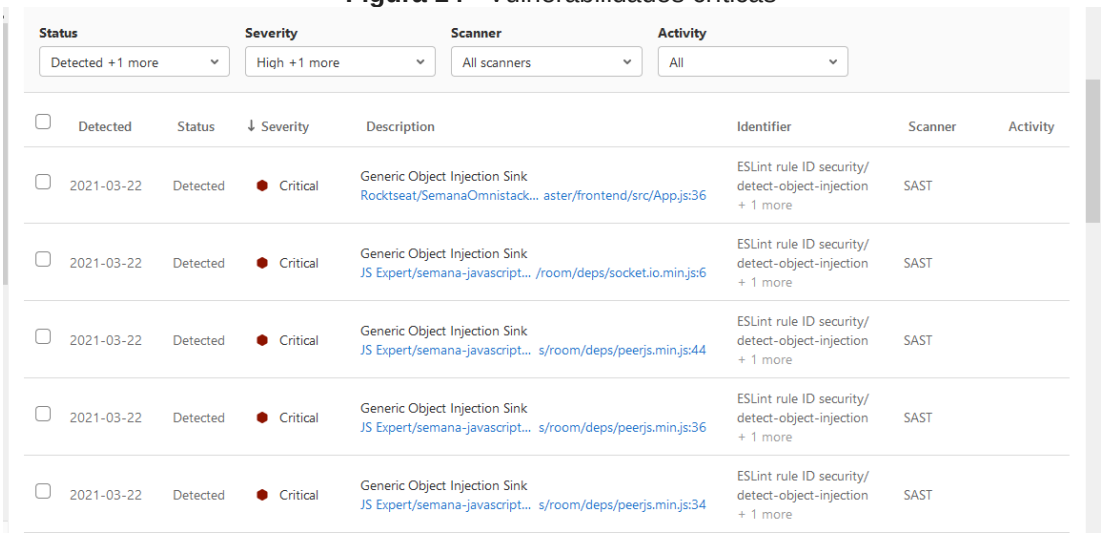
Figura 13 - GitLab relatório



Fonte: Autores

O GitLab também encontrou vulnerabilidades críticas relatadas como uma vulnerabilidade CWE-094, uma vulnerabilidade A1. Esses resultados podem ser vistos na Figura 14.

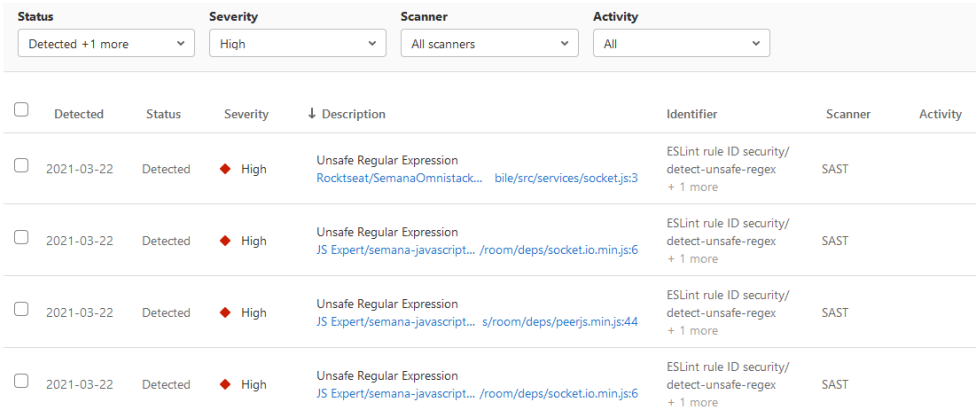
Figura 14 - Vulnerabilidades críticas



Fonte: Autores

Nos projetos analisados também foram encontradas vulnerabilidades classificadas como de alto risco, como pode ser visto na Figura 15. As falhas encontradas são relacionadas a CWE-400, uma vulnerabilidade A9.

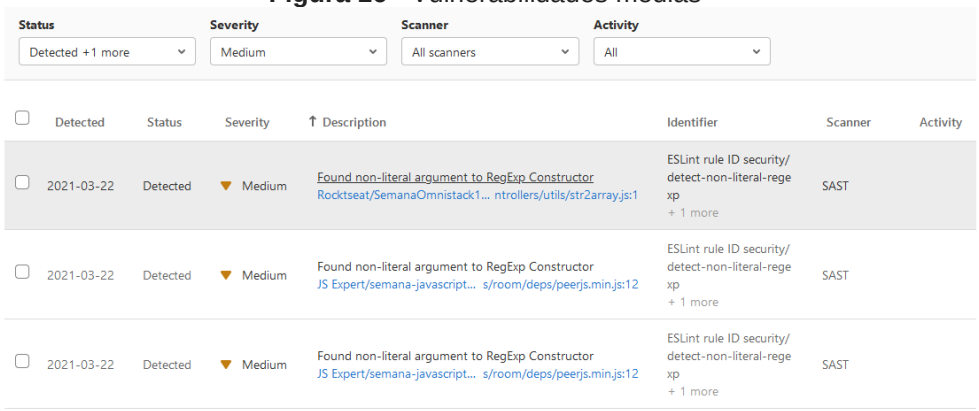
Figura 15 - Vulnerabilidades altas



Fonte: Autores

Também foram identificadas vulnerabilidades consideradas de risco médio, nos projetos analisados pela ferramenta. Essas falhas são relacionadas a CWE-185, como pode ser visto na Figura 16.

Figura 16 - Vulnerabilidades médias



Fonte: Autores

As CWE-400 e CWE-094 já foram discutidas anteriormente. Por sua vez, a CWE-185 está relacionada a uma vulnerabilidade em que o software especifica uma expressão regular de uma forma que possibilita que os dados sejam correspondidos ou comparados incorretamente.

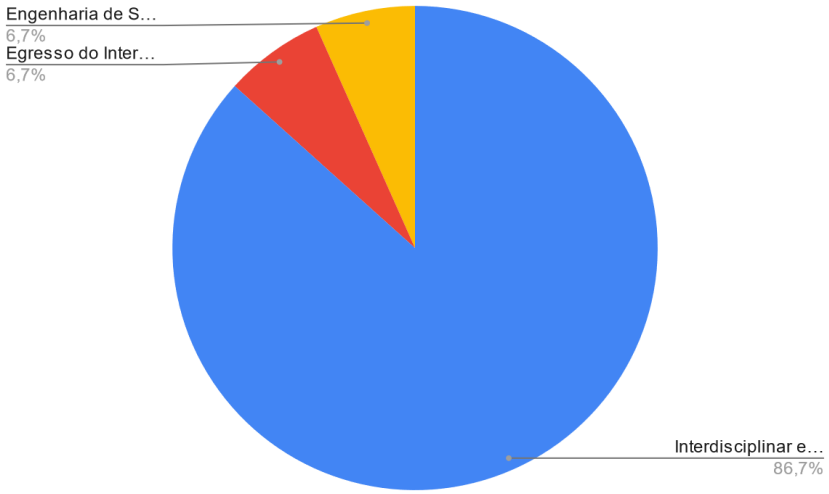
5 RESULTADOS DO QUESTIONÁRIO

O questionário foi enviado para os graduandos do campus Pau dos Ferros da UFERSA (Universidade Federal Rural do Semi-Árido) e tem a função de identificar se os cursos de curta duração abordam questões de segurança da informação. Para criar o questionário foi utilizada a aplicação Google *Forms*, que é um gerenciador de pesquisas da empresa Google. Saptarini et al. (2016) também investigou características de segurança associada a ISSO/IEC 25010. No estudo, eles apontaram as falhas de segurança de um sistema especifico antes e depois da reengenharia deste sistema. A abordagem utilizada neste trabalho é distinta já que aborda vários sistemas desenvolvidos por participantes de cursos de curta duração durante os cursos e também em suas práticas profissionais.

5.1 CARACTERÍSTICAS GERAIS DOS PARTICIPANTES

O questionário recebeu respostas de uma amostra de 15 (quinze), graduandos da UFERSA. Das 15 respostas obtidas, 87,7% são do curso Interdisciplinar em Tecnologia da Informação (BTI), 6,7% do curso de Engenharia de Software e 6,7% de egressos do BTI, alunos que iniciaram o curso Interdisciplinar em Tecnologia da Informação e não deram continuidade ou concluíram o curso. Essas informações podem ser vistas no Gráfico 4.

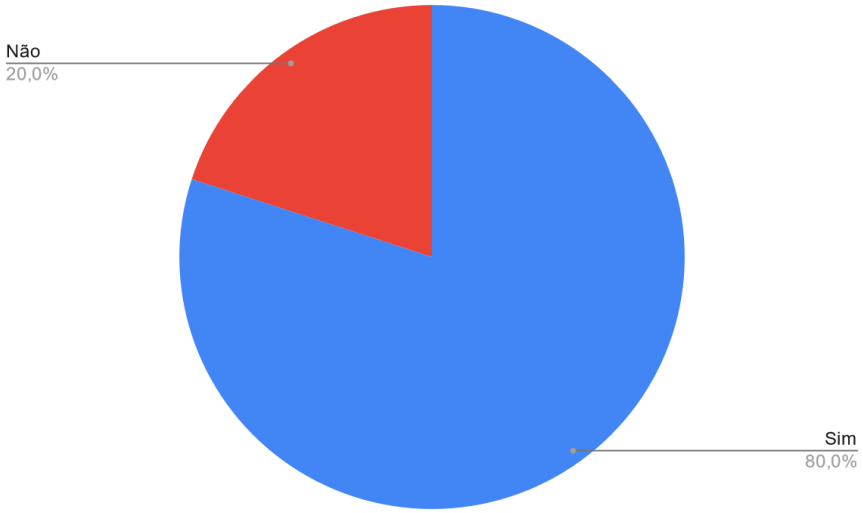
Gráfico 4 - Cursos



Fonte: Autores

Referente ao questionamento se o participante teria participado de cursos de curta duração, 80% dos participantes responderam que sim e 20% respondeu que não. Como é demonstrado no Gráfico 5.

Gráfico 5 - Participação em cursos de curta duração

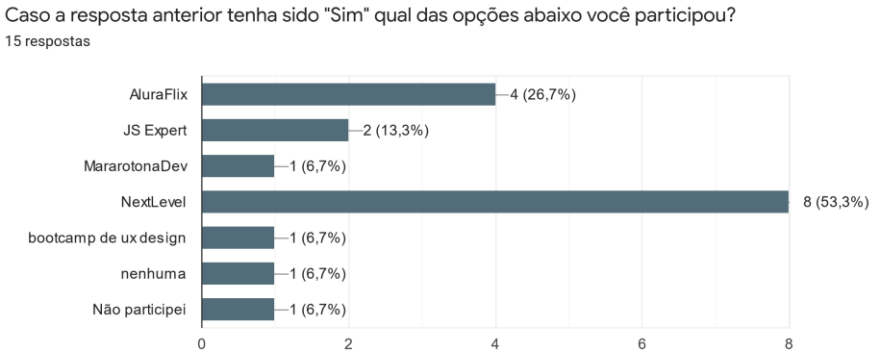


Fonte: Autores

Como é possível observar, a maioria dos participantes da pesquisa já participaram de algum curso de curta duração, foco principal da pesquisa.

Para os respondentes que participaram de cursos de curta duração, foi questionado qual curso ele teria feito; foram listadas múltiplas escolhas com as opções Next Level Week, AluraFlix, JsExpert. O participante também poderia informar outros cursos que não foram listados. Os resultados podem ser vistos no Gráfico 6.

Gráfico 6 - Cursos quais participaram

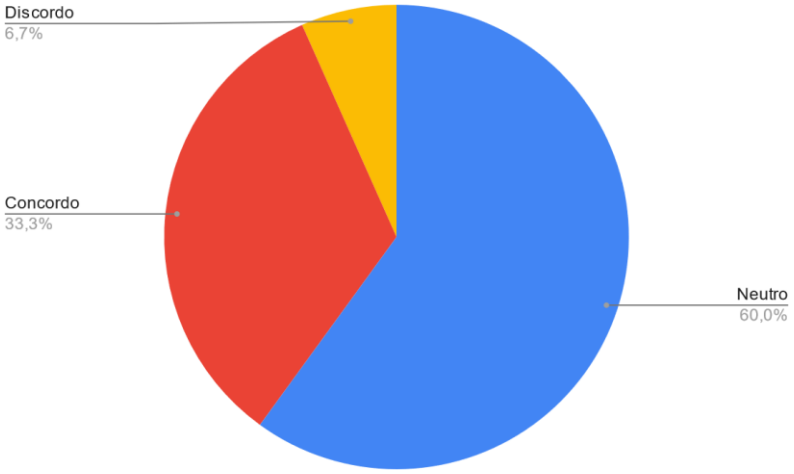


Fonte: Autores

Como pode ser observado, a maioria dos respondentes participou do curso da NextLevel (53,3%), seguido do curso AluraFlix (26,7%).

Em seguida, foi questionado se o participante aplica os conhecimentos adquiridos nos cursos em suas práticas profissionais. Nesta direção, 60% informaram ser neutros, 33,3% afirmando que sim, utilizam o conhecimento em suas atividades profissionais e 6,7% afirmaram que não usam esses conhecimentos em suas práticas para profissionais, como pode ser visto no Gráfico 7.

Gráfico 7 - Utilização dos conhecimentos dos cursos de curta duração em âmbito profissional

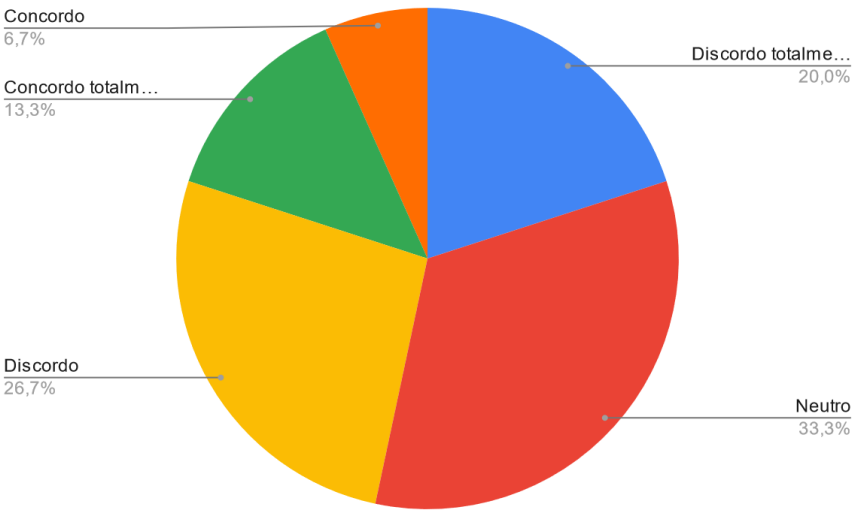


Fonte: Autores

Como é possível observar, a minoria afirmou não usar os conhecimentos adquiridos nos cursos. Neste sentido, caso os sistemas desenvolvidos nestes ambientes contiverem problemas de segurança, esses problemas podem ser levados para o código em produção.

Referente à segurança da informação é preciso investigar se esses cursos tratam a segurança da informação nos projetos desenvolvidos. Neste sentido, foi perguntado se os cursos tratavam nas práticas desenvolvidas; a maioria dos participantes (33,3%) informaram neutralidade; 26,7% discordam; 20% discordam totalmente; 13,3% concordam totalmente e 6,7% concordam. Esse resultado pode ser observado no Gráfico 8.

Gráfico 8 - Cursos tratavam sobre segurança da informação



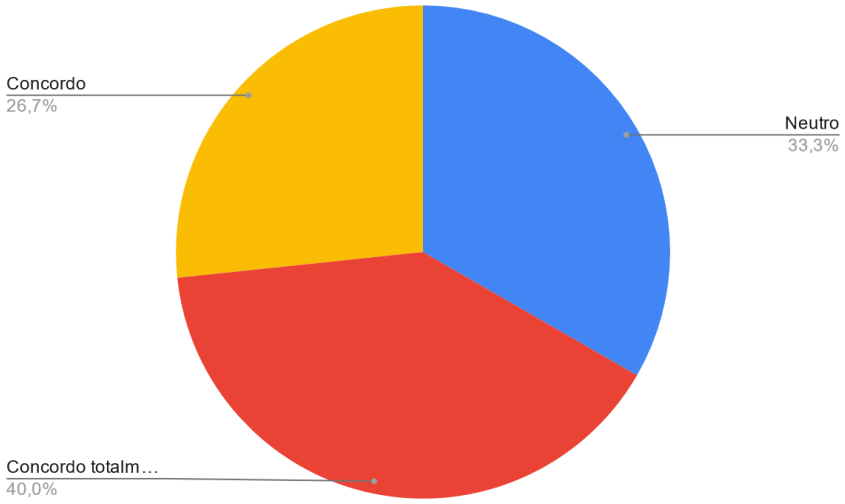
Fonte: Autores

Nesta direção, há uma tendência de discordância dos participantes referente a

afirmação que os cursos de curta duração abordam a questão de segurança durante o desenvolvimento das aplicações sugeridas. Neste sentido, vulnerabilidades podem ser inseridas nas práticas profissionais dos participantes, caso usem as soluções como aplicadas nos cursos.

Logo em seguida, foi questionado se os participantes costumam abordar questões de segurança durante o desenvolvimento de software. A maioria dos participantes (40%) concorda totalmente quanto a considerar as questões de segurança no desenvolvimento; 33,3% informaram ser neutros quanto às boas práticas de segurança e 26,7% concordam que consideram as práticas de segurança no desenvolvimento de software. Os resultados podem ser observados no Gráfico 9.

Gráfico 9 - Questões de segurança em consideração quando desenvolve suas práticas profissionais

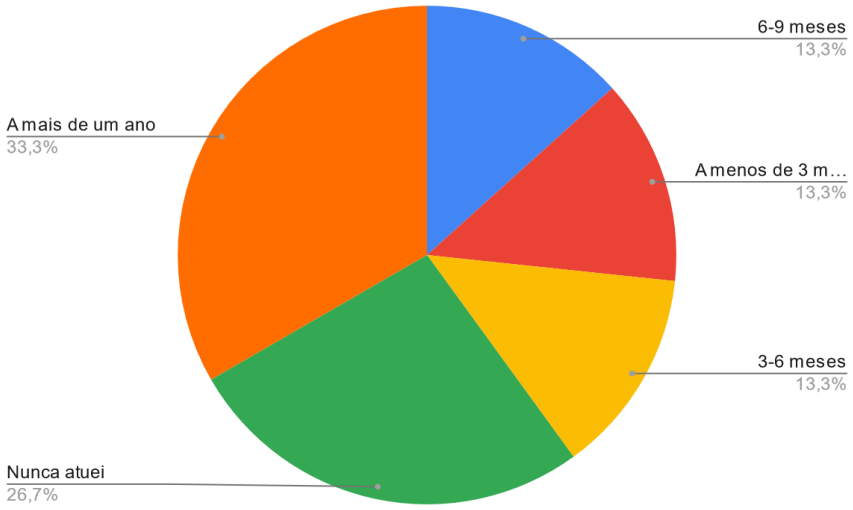


Fonte: Autores

Apesar de a maioria dos participantes concordar que a resolução de problemas de segurança é fundamental, muitos deles (um terço da população) ainda são propícios a permitir a inclusão de problemas de segurança nos sistemas desenvolvidos.

Também foi questionado aos participantes há quanto tempo trabalham com desenvolvimento de software. Esses resultados podem ser vistos no Gráfico 10. Apenas 26,7% dos participantes trabalham a mais de um ano com desenvolvimento.

Gráfico 10 - Tempo de trabalho



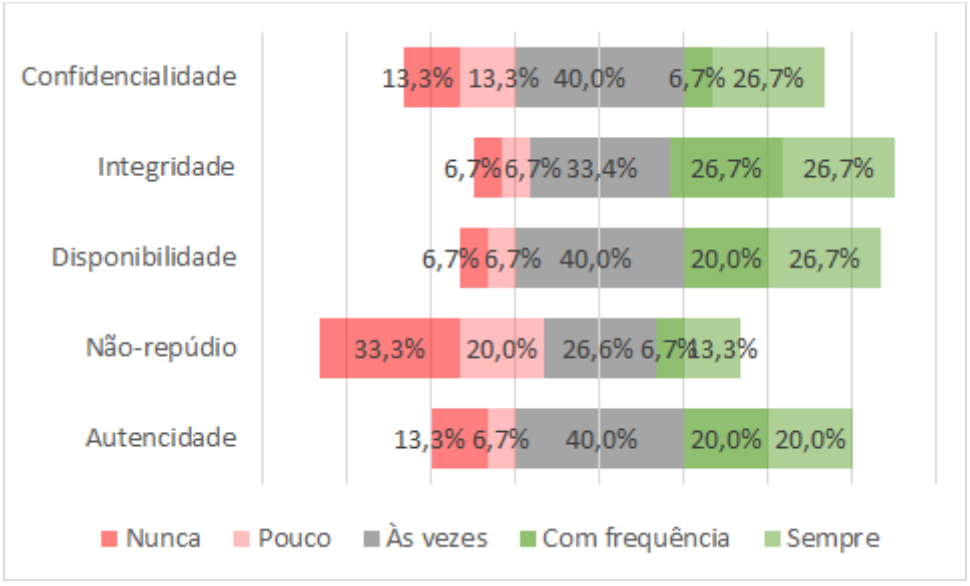
Fonte: Autores.

Neste sentido, os participantes podem deixar problemas de segurança em seus códigos.

5.2 PILARES DE SEGURANÇA SEGUNDO A ISO 25010

Para identificar a presença de problemas de segurança segundo a ISO 25010, foram analisados os atributos de qualidade estabelecidos nesta ISO, no sentido de identificar se os cursos abordam ou abordaram os pilares de segurança. No Gráfico 11 pode ser visto o quanto os cursos de curta duração abordaram cada um dos pilares de segurança da informação.

Gráfico 11 - Confidencialidade



Fonte: Autores

Como pode ser percebido no Gráfico 11, 40% dos participantes afirmaram que

os cursos de curta duração às vezes utilizam-se do pilar de confidencialidade; já 26,7% declaram que os cursos de curta duração abordam esse pilar, 13,3% dos participantes afirmaram que nos cursos de curta duração nunca se fazem uso desse pilar, 13,3% dos participantes declaram que os cursos de curta duração abordam esse pilar e apenas 8,7% dos participantes dizem que os cursos de curta duração fazem uso com frequência do pilar de confidencialidade.

Como pode ser visto no Gráfico 11, 33,3% dos participantes dizem que os cursos de curta duração às vezes utilizam-se de do pilar de integridade, já 26,7% declaram que os cursos de curta duração sempre usam o pilar de integridade, 26,7% dos participantes afirmaram que os cursos de curta duração abordam esse pilar, 6,7% dos participantes afirmaram que os cursos de curta duração fazem pouco uso deste pilar e 6,7% dos participantes afirmaram que os cursos de curta duração fazem uso com frequência do pilar de integridade.

Como pode ser visto no Gráfico 11, 40% dos participantes afirmaram que os cursos de curta duração às vezes usam o pilar de disponibilidade, já 26,7% declaram que os cursos de curta duração sempre fazem uso do pilar de disponibilidade, 20% dos membros participantes afirmaram que os cursos de curta duração com frequência fazem uso deste pilar, 6,7% dos participantes informaram que os cursos de curta duração fazem pouco uso deste pilar e 6,7% dos participantes afirmaram que os cursos de curta duração uso nunca usam o pilar de disponibilidade.

Ainda referente ao Gráfico 11, 33,3% dos participantes afirmaram que os cursos de curta duração nunca utilizam o pilar do não-repúdio; já 26,7% declaram que os cursos de curta duração às vezes usam o pilar de não-repúdio, 20% dos participantes afirmaram que os cursos de curta duração fazem pouco uso, 13,3% dos participantes afirmaram que os cursos de curta duração sempre usam o pilar e apenas 8,7% dos participantes afirmaram que os cursos de curta duração fazem uso com frequência do pilar não-repúdio.

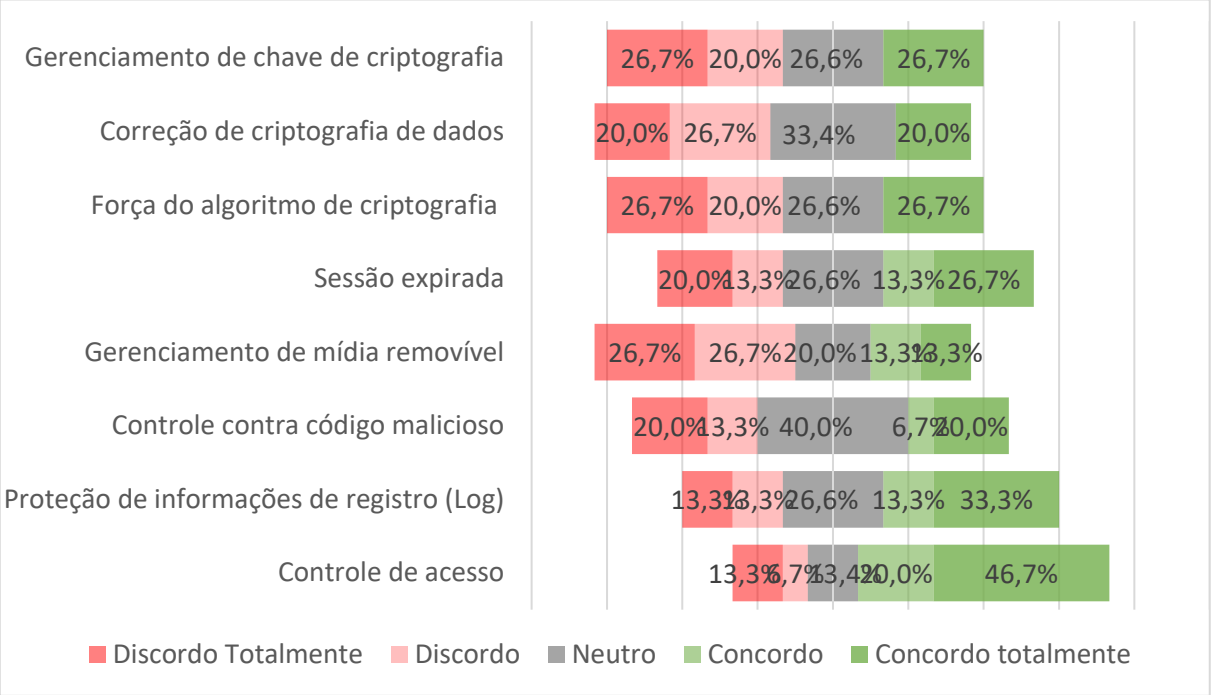
Também como pode ser visto no Gráfico 11, 40% dos participantes afirmaram que os cursos de curta duração às vezes utilizam o pilar da autenticidade; já 20% declaram que os cursos de curta duração sempre usam o pilar de autenticidade, 20% dos participantes afirmaram que os cursos de curta duração utilizam com frequência esse pilar, 13,3% dos participantes apontaram que nos cursos de curta duração nunca usam o pilar e apenas 6,7% dos participantes afirmaram que os cursos de curta duração fazem pouco uso do pilar de não-repúdio.

5.2.1 Pilares voltados à confidencialidade

Nesta seção são destacados fatores que afetam o atributo de qualidade confidencialidade. As perguntas são relacionadas a essa métrica segundo a norma ISO/IEC 25010.

No Gráfico 12 pode ser vista a percepção dos usuários com respeito a métrica de controle de acesso. Nesta direção, 61,4% dos participantes afirmaram que os cursos de curta duração abordaram a métrica de controle de acesso.

Gráfico 12 -Métricas de confiabilidade



Fonte: Autores

Ainda no Gráfico 12 podem ser vistas as respostas dos participantes referente a métrica proteção de informações de registro. A maioria dos participantes (49%) demonstraram que os cursos de curta duração aplicam a métrica de proteção de informações de registro (*log*).

Referente ao controle contra código malicioso, somando os participantes que votaram entre a nota 4 e 5 é chegado ao total de 43,2%, como pode ser visto no Gráfico 12. Neste sentido, há indícios de que os cursos de curta duração aplicam essa métrica.

Já no tocante ao gerenciamento de mídias removíveis, os participantes que votaram entre 4 e 5 somam um total de 45,7%, conforme o Gráfico 12. Dessa forma também há indícios que os cursos de curta duração implementam essa métrica em

seus projetos.

Como pode ser visto no Gráfico 12, a maioria dos participantes afirmou que os cursos de curta duração fazem utilização da métrica de sessão expirada, tendo 42,6% votado 5 e 17% votado 4, somando um total de 59,6%, demonstrando que os cursos de curta duração fazem uso dessa métrica.

Por outro lado, no Gráfico 12 os cursos de curta duração utilizam algoritmos de criptografia fortes (47,6%).

A força da criptografia é determinada pelo tamanho da chave, como mostra a tabela abaixo:

Tabela 10 - força do algoritmo de criptografia

Tamanho (bits)	Força
1024	Baixa
2048	Média
4096	Alta

Fonte: ibm.com

Referente a correção de criptografia de dados, 36,6% afirmam que os cursos de curta duração abordam essa característica, como pode ser visto no Gráfico 12.

No tocante ao gerenciamento de chaves de criptografia, 47,6% dos participantes afirmaram que os cursos de curta duração abordam essa característica, como pode ser visto no Gráfico 12.

Resumo das métricas de confidencialidade

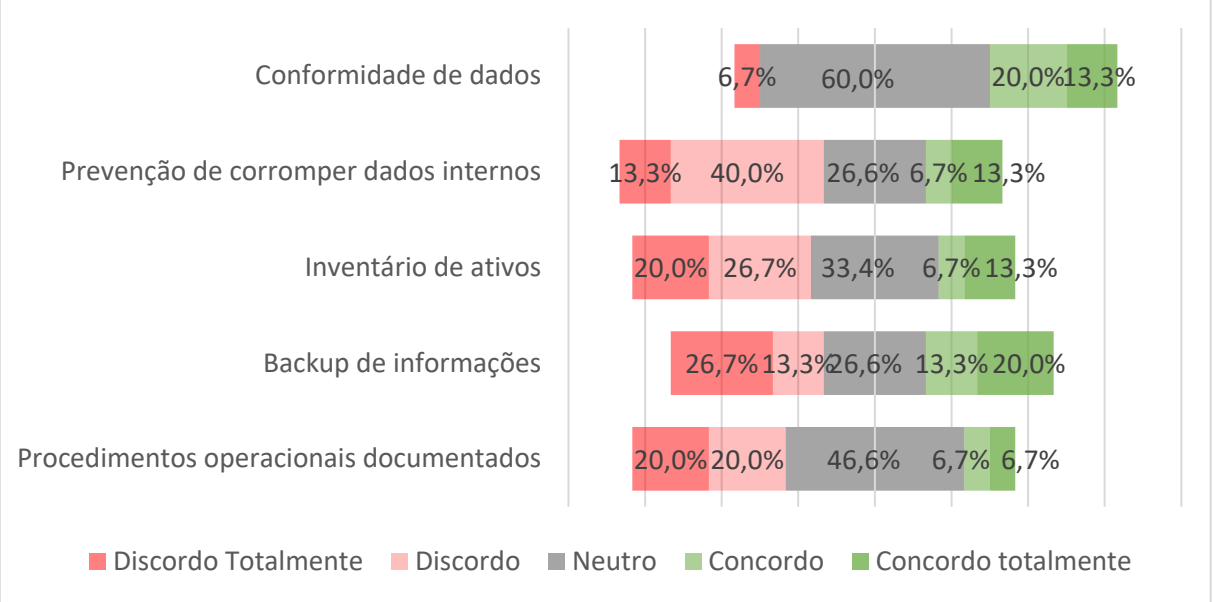
Conforme dados do Gráfico 12, a maioria dos participantes afirmou que os cursos de curta duração usam as métricas de confidencialidade para a garantia de segurança e de qualidade segundo a ISO/IEC 25010.

5.2.2 Pilares voltados à integridade

Nesta seção aborda-se o segundo pilar de segurança apontado pela norma ISO 25010, a integridade.

Referente a métrica de conformidade de dados, como pode ser visto no Gráfico 13, 54% dos participantes julgou com neutro o uso deste aspecto; 24% concordou, 20% concordou totalmente e apenas 2% discordou totalmente.

Gráfico 13 - Conformidade de dados



Fonte: Autores

Já referente a prevenção de corrupção de dados internos, 30,8% dos participantes afirmaram ser neutros à aplicação desta métrica nos cursos de curta duração; já 30,8% discordou com a afirmação, 20,5% concordam que a métrica é aplicada neste contexto, 12,8% concordaram totalmente com a afirmativa e apenas 5,1% discordam totalmente que esse aspecto é considerado nos cursos de curta duração.

Referente ao uso de inventários de ativos, 37.5% dos participantes informaram ser neutros a aplicação desta métrica nos cursos de duração; 25% dos integrantes concordaram totalmente, 20% discordaram da aplicação da métrica, 10% concordou com a aplicação da métrica e apenas 7,5% discorda totalmente do uso da métrica nos cursos de curta duração. Esses resultados podem ser vistos no Gráfico 13.

No tocante ao *backup* de informações aplicado nos cursos de curta duração, 34,9% dos participantes concordaram totalmente que a métrica foi aplicada; já 27,9% julgou como neutra a aplicação da métrica, 18,6% concordam que a métrica é aplicada nos cursos de curta formação, 9,3% discordam com a afirmação e 9,3% discordam totalmente que a métrica é aplicada nos cursos de curta duração, como pode ser visto no Gráfico 13.

Por fim, referente a métrica Integridade, 53,8% dos participantes julgou como neutra a aplicação da métrica de procedimentos operacionais documentados; já 15,4% discordou de que a métrica foi utilizada nos cursos de curta duração, 12,8% concorda totalmente que a métrica foi aplicada, 10,3% dos participantes concordam

que a métrica é aplicada nos cursos de curta duração e apenas 7,7% discorda totalmente de que a métrica de procedimentos operacionais documentados é aplicada nestas temáticas. Esses resultados podem ser vistos no Gráfico 13.

Resumo da métrica integridade

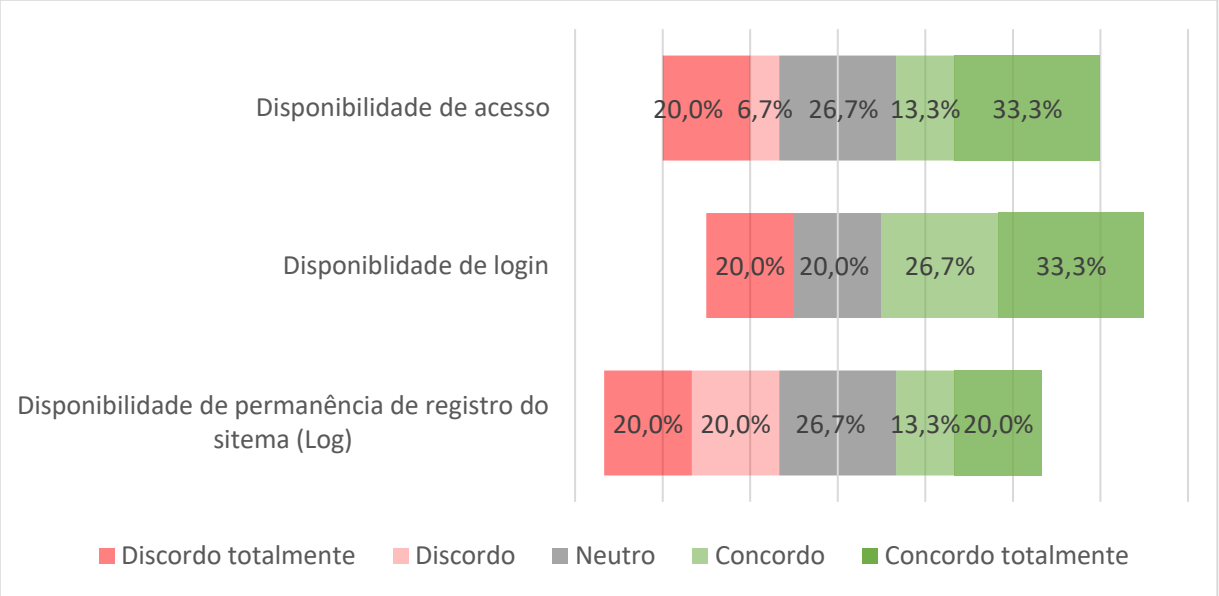
Como podemos ver no Gráfico 13, a maioria dos participantes afirmou que nos cursos de curta duração o uso das métricas de integridade são neutras para a garantia de segurança e de qualidade segundo a ISO/IEC 25010.

5.2.3 Pilares voltados à responsabilidade

Nesta seção discutimos aspectos relacionados a métrica responsividade da ISO 25010.

Referente a métrica disponibilidade de acesso, 50% dos participantes concordam totalmente que os cursos de curta duração recorrem à métrica; já 24% são neutros ao uso dessa métrica nos cursos de curta duração, 16% concordam com essa afirmação, 6% discordam totalmente com esse aspecto e apenas 4% discordam que os cursos consideram esta característica, como pode ser observado no Gráfico 14.

Gráfico 14 -Métricas de responsabilidade



Fonte: Autores

No tocante a métrica disponibilidade de login, 47,2% concordam totalmente que a métrica é aplicada nos cursos de curta duração; já 30% concordam que a métrica é aplicada nesta temática, 17% dos participantes são neutros a aplicação da métrica e apenas 5,7% discordam totalmente da afirmação, como pode ser visto no Gráfico 14.

Por fim, no tocante à responsabilidade, foi analisada a disponibilidade de permanência de registro do sistema. No Gráfico 14 pode ser visto que 34,1% dos participantes concordam totalmente que esta métrica foi aplicada, 18,2% concordam com a afirmação; já 27,3% são neutros, 13,6% discordam que essa métrica é aplicada e apenas 6,8% discordam totalmente que esta métrica é aplicada em cursos de curta duração.

Resumo da métrica responsabilidade

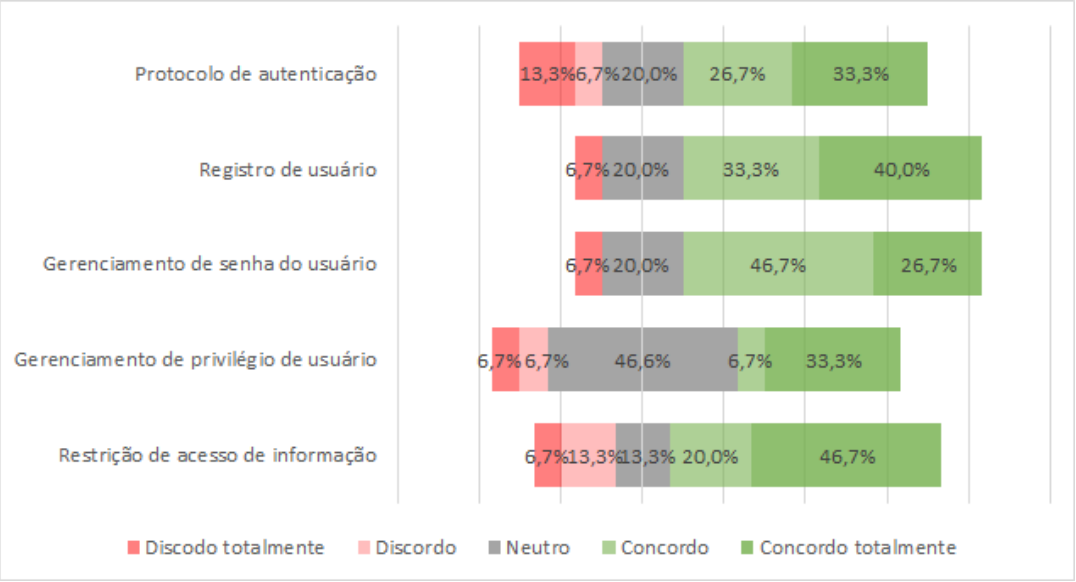
Como pode ser visto no Gráfico 14, a maioria dos participantes afirmou que os cursos de curta duração usam métricas de responsabilidade para a garantia de segurança dos sistemas desenvolvidos, segundo a ISO/IEC 25010.

5.2.4 Pilares voltados à autenticidade

Nesta seção é abordada a métrica autenticidade de acordo com a ISO 25010. Dentro da autenticidade é possível trabalhar várias características, conforme detalhado a seguir.

Uma das características da aplicação de autenticidade é o uso de protocolos de autenticação. Nesta direção, 46,3% dos participantes concordam totalmente que a métrica de protocolo de autenticação é usada; já 29,6% dos participantes concordam que a métrica é aplicada, 16,7% dos participantes são neutros, 3,7% discordam da utilização da métrica e 3,7% discordaram totalmente da utilização desta métrica, como pode ser visto no Gráfico 15.

Gráfico 15 -Métricas de autenticidade



Fonte: Autores

Referente à métrica de registro de usuário, 50% dos participantes concordam totalmente que os cursos de curta duração aplicam esta métrica; já 33,3% concordaram que ela é aplicada nesta temática, 15% julgaram como neutra a utilização da métrica e apenas 1,7% discordaram totalmente com a afirmação, como o Gráfico 15.

No tocante à métrica de gerenciamento de senha do usuário, 48,3% dos participantes concordam que a métrica foi aplicada. Outros 34,5% concordam totalmente que a métrica é aplicada, 15,5% julgaram como neutra a utilização da métrica nos cursos de curta duração e apenas 1,7% dos participantes discordam totalmente desta afirmação, como pode ser visto no Gráfico 15.

Referente à métrica de gerenciamento de privilégio de usuário, 47,2% dos participantes concordam totalmente que os cursos de curta duração aplicam essa métrica; já 39,6% são neutros a aplicação da métrica, 7,5% concordam que os cursos abordam essa temática, 3,8% dos participantes discordam que a métrica é aplicada nos cursos de curta duração e apenas 1,9% discordam totalmente como a afirmação, como pode ser visto no Gráfico 15.

No tocante à métrica de restrição de acesso de informação, 60,3% concordam totalmente que os cursos de curta duração abordam essa métrica e 20,7% dos participantes concordam que a métrica é utilizada; outros 10,3% são neutros, 6,9% discordaram da afirmação e apenas 1,7% dos participantes discordaram totalmente deste aspecto, como pode ser visto no Gráfico 15.

Resumo da métrica autenticidade

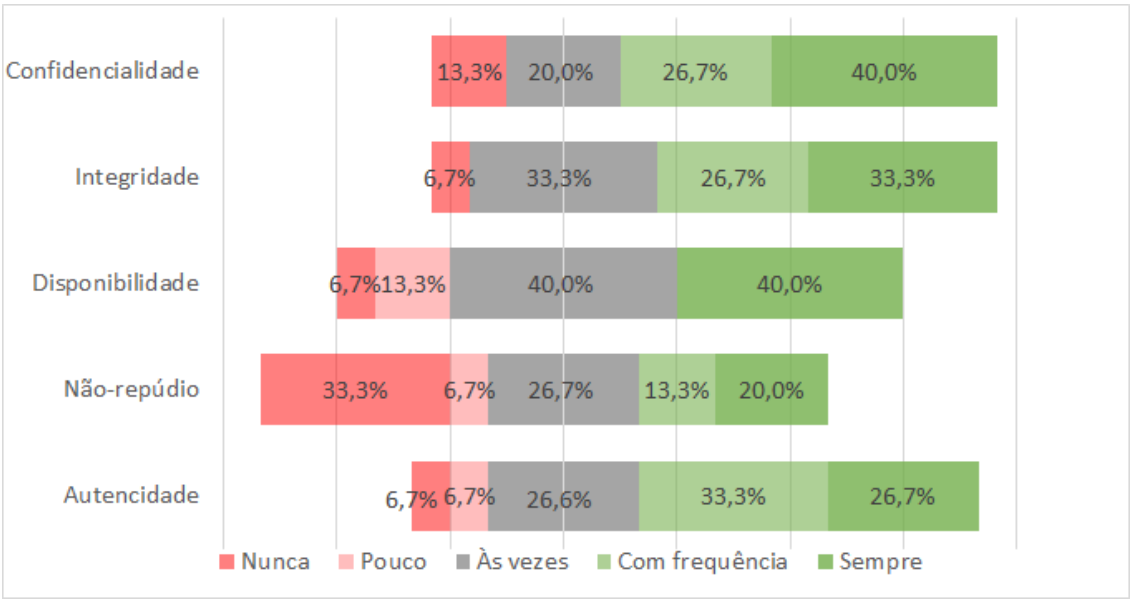
Como pode ser visto no Gráfico 15, a maioria dos participantes afirmou que os cursos de curta duração usam métricas de autenticidade para a garantia de segurança dos sistemas desenvolvidos, segundo a ISO/IEC 25010.

5.3 USO DOS PILARES E DAS MÉTRICAS NO ÂMBITO PROFISSIONAL

Tendo em vista que na área de desenvolvimento de software o aprendizado é constante. Neste sentido, precisa-se buscar conhecimentos em meios, tais como os cursos de curta duração. No entanto, algumas práticas de segurança não são foco dos cursos, conforme discutido anteriormente. Dessa forma, foram elencadas perguntas para identificar o uso das práticas de segurança na atuação profissional dos participantes.

Os resultados referentes ao uso dos diferentes pilares de segurança podem ser vistos no Gráfico 16.

Gráfico 16 - Uso dos pilares da segurança da informação



Fonte: Autores

De modo geral, os participantes tendem a utilizar o pilar de confidencialidade, 40,0% sempre que utilizam o pilar de confiabilidade no seu espaço de trabalho; já 26,7% usa com frequência o pilar de confidencialidade; outros 20,0% afirmar que às vezes usa a confidencialidade no trabalho e apenas 13,3% nunca usam a confidencialidade nas suas práticas profissionais.

Já referente ao pilar de integridade, 33,3% dos participantes sempre usam o pilar de integridade no ambiente de trabalho; já 26,7% usam com frequência a integridade, 33,4% às vezes usam o pilar de integridade no recinto de trabalho e apenas 6,7% nunca utilizaram o pilar de integridade no seu trabalho.

No que tange ao pilar de disponibilidade, 40,0% dos participantes sempre fazem uso desse pilar em seu âmbito de trabalho; já 40,0% dos participantes da pesquisa às vezes usam o pilar de disponibilidade; outros 13,3% dos participantes afirmaram fazer pouco uso do pilar de disponibilidade no meio profissional e apenas 6,7% dos participantes dizem que nunca usam o pilar de disponibilidade no âmbito profissional.

No que se refere ao pilar de não-repúdio, 33,3% dos participantes votaram em que nunca usaram o pilar de não-repúdio em suas práticas profissionais; já 26,7% dos integrantes da pesquisa afirmaram que às vezes utilizam o pilar; outros 20,0% dos participantes sempre usam o pilar, 13,3% usam com frequência o pilar e apenas 6,7%

dos participantes afirmam fazer pouco uso do pilar de não-repúdio no seu âmbito de trabalho.

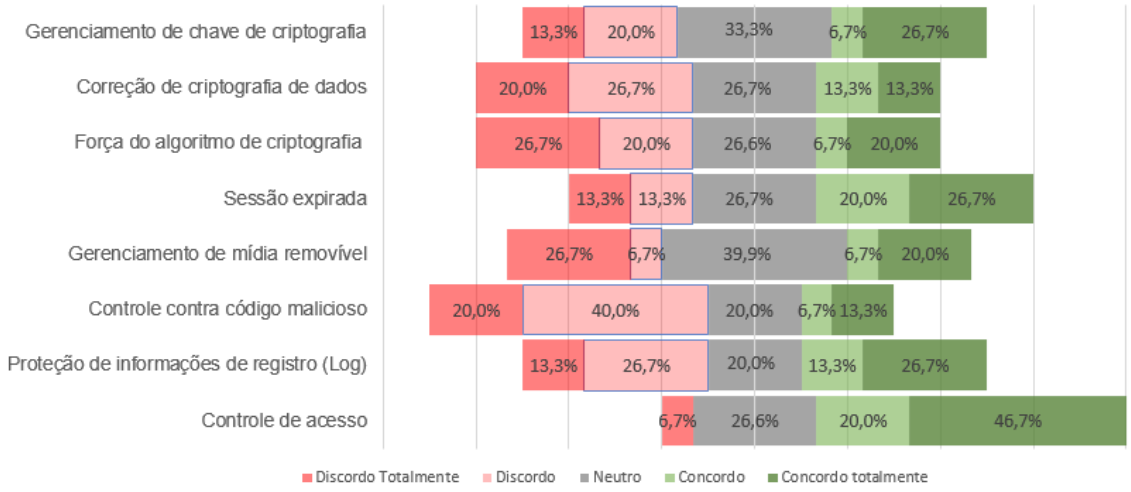
Já no último dos pilares elencados, 33,3% dos participantes utilizam com frequência o pilar de autenticidade; já 26,7% dos integrantes da pesquisa afirmam sempre usar o pilar de autenticidade; outros 26,7% afirmaram ser neutro quanto a aplicação do pilar em seu ambiente profissional; outros 6,7% usam pouco o pilar em seu cotidiano trabalhista e 6,7% nunca usaram o pilar em seu âmbito profissional.

Visto que na maioria dos casos os participantes aplicam os pilares de segurança da informação, viu-se a necessidade de investigar se eram aplicadas as métricas para garantia da qualidade de acordo com a ISO/IEC 25010.

5.3.1. Aplicação do pilar confidencialidade na prática profissional

Foi questionado se os integrantes da pesquisa abordam ou já abordaram as métricas de confidencialidade conforme a ISO/IEC 25010. Esses resultados podem ser vistos no Gráfico 17.

Gráfico 17 - Métricas de confidencialidade



Fonte: Autores

No que diz a respeito da métrica de gerenciamento de chave de criptografia, 33,3% dos participantes foram neutros quanto a aplicação desta métrica no seu uso profissional; já 26,7% dos participantes da pesquisa concordam totalmente quanto a uso dessa métrica em seu recinto de trabalho; outros 20,0% discordam do uso da métrica em seu âmbito profissional; já 13,3% discordam totalmente do uso da métrica em seu trabalho e apenas 6,7% concordam com o uso da métrica em seu ambiente profissional.

No que se refere a métrica de correção de criptografia de dados, 26,7% discorda da aplicação da métrica no uso profissional; já 26,7% votaram neutro quanto a aplicação da métrica no âmbito profissional; outros 20,0% discordam totalmente do uso da métrica no recinto de trabalho, 13,3% dos participantes concordaram e 13,3% concordam totalmente com o uso da métrica no ambiente de trabalho.

No que se diz a respeito da métrica de força do algoritmo de criptografia, 26,7% dos participantes discordam totalmente do uso da métrica; já 26,6% dos participantes dizem ser neutros a aplicação da métrica em seu cotidiano; outros 20,0% dos integrantes discordam do uso da métrica em seu recinto de trabalho, 20,0% deles concordam totalmente com o uso da métrica no seu âmbito profissional e apenas 6,7% concordam com o uso da métrica no seu ambiente de trabalho.

No tocante a métrica de sessão expirada, 26,7% dos integrantes da pesquisa concordaram totalmente com o uso da métrica em seu ambiente profissional; já 26,7 julgam como neutra a aplicação da métrica em âmbito profissional; outros 20,0% concordam com o uso da métrica, 13,3% dos participantes discordam da aplicação da métrica no trabalho e 13,3% discordam totalmente da aplicação da métrica no seu recinto de trabalho.

No que se refere a métrica de gerenciamento de mídia removível, 39,9% dos participantes julgam como neutro o uso da métrica; já 26,4% discordam totalmente do uso da métrica; outros 20,0% concordam totalmente com uso da métrica, 6,7% dos participantes concordam totalmente com o uso da métrica e 6,7% discordam do uso da métrica em âmbito profissional.

No que diz respeito à métrica de controle contra código malicioso, 40,0% dos participantes discordam do uso da métrica no ambiente profissional; já 20,0% discorda totalmente do uso da métrica; outros 20,0% julgam como neutro o uso da métrica; já 13,3% dos membros participantes concordam totalmente com o uso da métrica e apenas 6,7% dos integrantes da pesquisa concordam com uso da métrica no seu meio profissional.

No que diz a respeito da métrica proteção de informações de registro (log), 26,7% concordam totalmente com o uso da métrica no meio profissional; já 26,7% discordam do uso da métrica; outros 20,0% julgam como neutro a aplicação da métrica; já 13,3% discordam totalmente da aplicação da métrica e 13,3% concordam com a utilização da métrica no âmbito profissional.

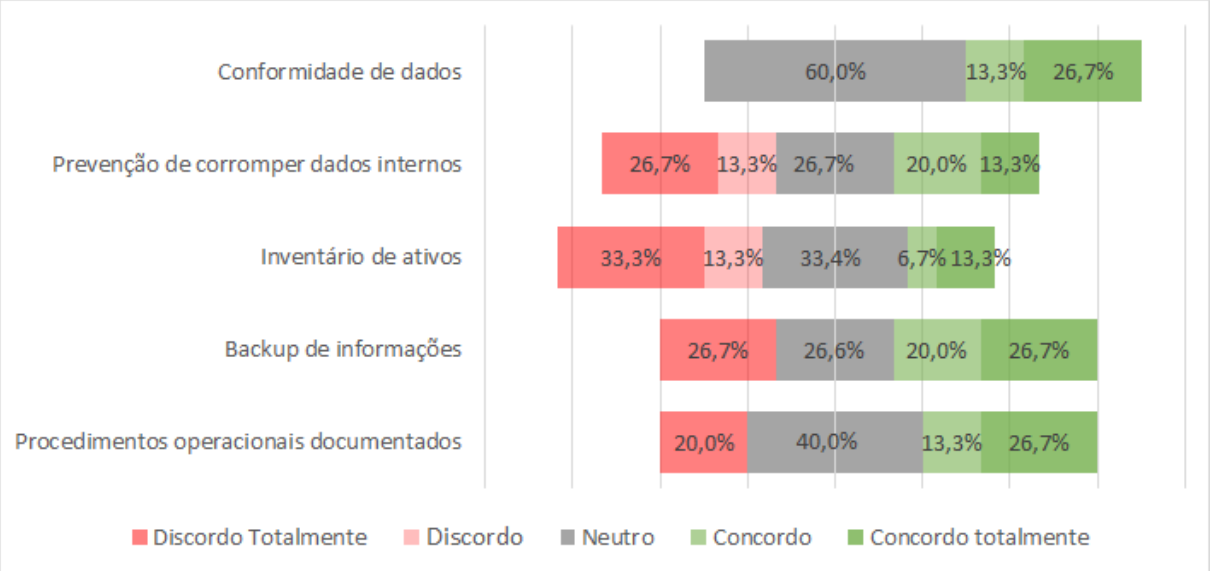
E por fim no que se refere a métrica de controle de acesso, 46,7% dos

participantes concordam totalmente com o uso da métrica em meio profissional; já 26,6% julgam como neutro a utilização da métrica; outros 20,0% concordam com a aplicação da métrica e apenas 6,7% discordam totalmente com o uso da métrica no âmbito profissional.

5.3.2. Aplicação do pilar integridade na prática profissional

Foi questionado se os integrantes da pesquisa abordam ou já abordaram as métricas de integridade de acordo com a ISO/IEC 25010. Os resultados podem ser vistos no Gráfico 18.

Gráfico 18 - Métricas de integridade



Fonte: Autores

No que se remete a métrica de conformidade de dados, 60,0% dos participantes julgaram como neutra a utilização da métrica no meio profissional, 26,7% concordaram totalmente com a utilização da métrica e apenas 13,3% concordam com o uso da métrica no âmbito profissional.

No que se refere a métrica de prevenção de corrompimento de dados internos, 26,7% discordam totalmente da aplicação da métrica no meio profissional; já 26,7 julgam como neutra a aplicação da métrica; outros 20,0% concordam com a utilização da métrica; já 13,3% discordam do uso da métrica no meio profissional e 13,3% concordam totalmente com a aplicação da métrica no âmbito profissional.

No que diz a respeito da métrica de inventário de ativos, 33,4% julgam como neutra a utilização da métrica no meio profissional; já 33,3% dos participantes discordam totalmente da aplicação da métrica; outros 13,3% discordam do uso da

métrica em meio profissional; já 13,3% concordam totalmente com a utilização da métrica e apenas 6,7% concordam com o uso da métrica no âmbito profissional.

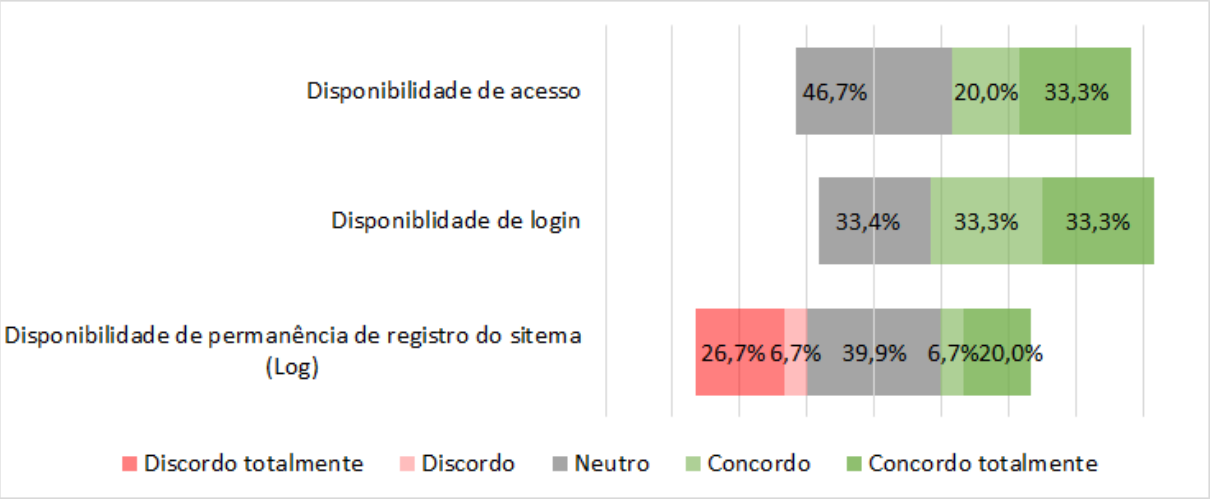
No tocante a métrica de *backup* de informações, 26,7% discordam totalmente do uso da métrica no meio profissional; já 26,7% concordam totalmente da utilização da métrica, outros 26,6% julgam como neutra a aplicação da métrica e apenas 20,0% dos integrantes concordam com a aplicação da métrica no âmbito de trabalho.

E por fim para a métrica de procedimentos operacionais documentados, 40,0% dos participantes julgam como neutra a utilização da métrica no meio profissional; já 26,7% concordam totalmente com a aplicação da métrica; já 26,7% concordam totalmente com a aplicação da métrica e apenas 13,3% concorda com o uso da métrica no âmbito de trabalho.

5.3.3. Aplicação do pilar disponibilidade na prática profissional

Foi questionado se os integrantes da pesquisa abordam ou já abordaram as métricas de disponibilidade de acordo com a ISO/IEC 25010. Os resultados referentes a esse pilar podem ser vistos no Gráfico 19.

Gráfico 19 - Métricas de disponibilidade



Fonte: Autores

No que remete a métrica de disponibilidade de acesso, 46,7% dos participantes julgam como neutra a utilização da métrica no meio profissional; já 33,3% dos integrantes da pesquisa concordam totalmente com a aplicação da métrica no seu recinto de trabalho e apenas 20,0% dos participantes concordam com a aplicação da métrica no âmbito profissional.

No que refere a métrica de disponibilidade de login, 33,4% dos participantes julgam como neutra o uso da métrica no meio de trabalho; já 33,3% dos integrantes

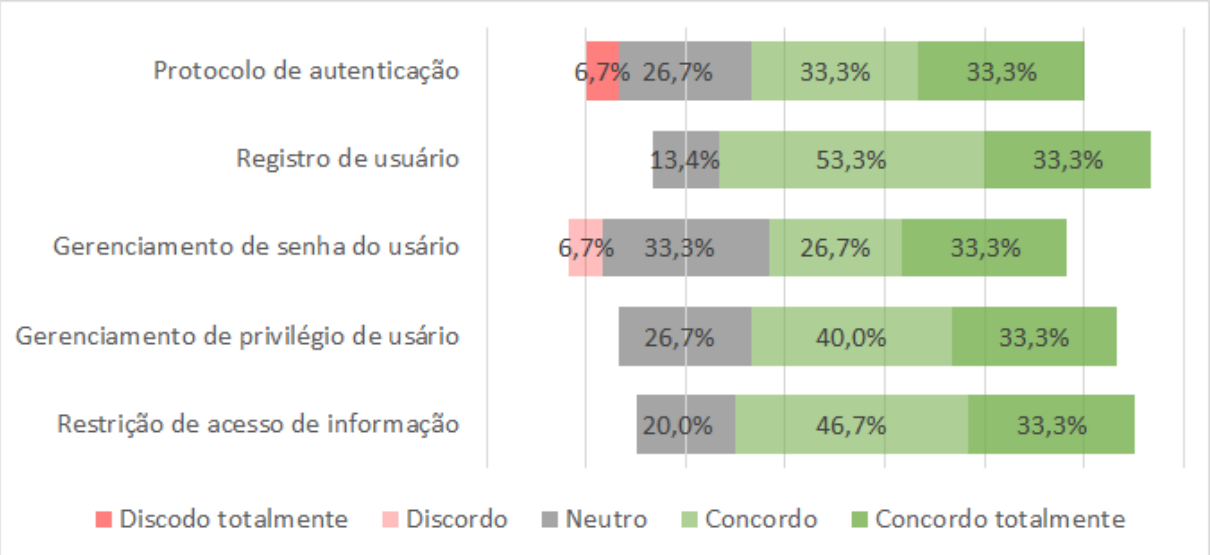
concordam com o uso da métrica e 33,3% concordam totalmente com a aplicação da métrica no seu âmbito de trabalho.

E por fim para a métrica de disponibilidade de permanência de registro do sistema (log), 39,9% dos participantes julgam como neutra a aplicação da métrica no cotidiano; já 26,7% discordam totalmente da aplicação da métrica; outros 20,0% concordam totalmente com a aplicação da métrica no meio de trabalho; já 6,7% dos participantes discordam da utilização da métrica e 6,7% dos participantes concordam com a aplicação da métrica no âmbito profissional.

5.3.4. Aplicação do pilar autenticidade na prática profissional

Foi questionado se os integrantes da pesquisa abordam ou já abordaram as métricas de autenticidade de acordo com a ISO/IEC 25010. Os resultados podem ser vistos no Gráfico 20.

Gráfico 20 - Métricas de autenticação



Fonte: Autores

No que refere a métrica de protocolo de autenticação, 33,3% dos participantes concordam totalmente com a utilização da métrica no meio profissional; já 33,3% dos participantes concorda com a aplicação da métrica; outros 26,7% dos integrantes julgam como neutro o uso da métrica e apenas 6,7% discordam totalmente do uso da métrica em âmbito de trabalho.

No que remete a métrica de registro de usuário, 53,3% dos participantes concordam com a utilização da métrica no meio profissional; já 33,3% dos integrantes concordam totalmente com a aplicação da métrica e apenas 13,4% dos participantes julgam como neutro o uso da métrica no âmbito profissional.

No tocante a métrica de gerenciamento de senha do usuário, 33,3% dos membros participantes julgam como neutro o uso da métrica no meio profissional; já 33,3% concordam totalmente com a aplicação da métrica; outros 26,7% concordam com a utilização da métrica e apenas 6,7% discordam do uso da métrica no âmbito de trabalho.

No que diz respeito a métrica de gerenciamento de privilégio de usuário, 40,0% concorda com o uso da métrica do meio profissional; já 33,3% concorda totalmente com o uso da métrica e apenas 26,7% dos participantes julgam como neutro o uso da métrica em âmbito profissional.

E por fim para a métrica de restrição de acesso de informação, 46,7% dos participantes concordam com a aplicação da métrica; já 33,3% dos integrantes da pesquisa concordam totalmente com a utilização da métrica e apenas 20,0% dos participantes julgam como neutro o uso da métrica no âmbito profissional.

6 CONCLUSÃO

Este trabalho analisou as vulnerabilidades dos projetos dos cursos de curta duração com seu nível de segurança e também se os participantes desses cursos utilizam do conhecimento adquirido nesses cursos em suas atuações profissionais.

A análise das vulnerabilidades, considerando sua severidade a partir da classificação (OWASP et al., 2017) permitiu a construção de uma classificação para os sites estudados. Através disso foi analisado que os cursos de curta duração não se atentam tanto para o desenvolvimento seguro, com isso os participantes podem levar desse conhecimento para o seu meio de trabalho, o que pode propagar vulnerabilidades. Por mais que os cursos de curta duração tenham um déficit na parte de segurança da informação ainda sim, é possível proteger essas aplicações com outros mecanismos que não seja apenas a codificação. Por exemplo, utilização de criptografia para proteger o pilar da confidencialidade, ou códigos hash na proteção da integridade das informações manipuladas pela aplicação, ou WAF para evitar ataques contra a disponibilidade da aplicação (evitar ataques, como o XML Bomb), etc.

Foi possível observar por meio dos resultados utilizando a metodologia de testagem, que mesmo em cursos ofertados por empresas da comunidade, sendo ministrados para milhares de pessoas ainda apresentam problemas, sejam eles mínimos até críticos, o que pode causar desde um vazamento de dados sensíveis até um acesso remoto ao servidor da aplicação, podendo assim prejudicar os usuários que querem usufruir de todos os recursos com plena confiança de que seus dados estejam seguros. Estes problemas poderiam ser evitados caso fossem seguidos os padrões de desenvolvimento.

Nesse sentido, a utilização do conhecimento adquirido nesses cursos no ambiente de desenvolvimento permite aos desenvolvedores tornarem suas aplicações mais seguras, levando o profissional a seguir mais padrões de segurança e zelar mais por seus futuros usuários.

7 REFERÊNCIAS

ABNT. ABNT NBR ISO/IEC 17799: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Tecnologia da informação - Técnicas de segurança - código de prática para a gestão da segurança da informação, p. 120, 2005.

ALEXANDRIA, João Carlos Soares de. Gestão de Segurança da informação-uma proposta para potencializar a efetividade da Segurança da informação em ambiente de pesquisa científica. 2009. Tese de Doutorado. Universidade de São Paulo.

BAPTISTA D. J. V. DOWNSIZING: da Teoria à Prática – O Processo de Descentralização da Prodabel. 1998. Dissertação (Mestrado). Escola de Governo – Fundação João Pinheiro. Belo Horizonte.

Carlos S Portela, Alexandre ML Vasconcelos, and Sandro RB Oliveira. Análise da relevância dos tópicos e da efetividade das abordagens para o ensino de engenharia de software. In Fórum de Educação em Engenharia de Software (FEES).In VI Congresso Brasileiro de Software: Teoria e Prática (CBSoft), 2015.

CERT.BR. **Estatísticas dos Incidentes Reportados ao CERT.br.** 2020. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 27 mar. 2020.

CERT.BR. **Incidentes Reportados ao CERT.br: tipos de ataques.** Tipos de ataques. 2020. Disponível em: https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html. Acesso em: 27 mar. 2020.

CERT.BR. **Incidentes Reportados ao CERT.br: totais mensais.** Totais mensais. 2020. Disponível em: https://www.cert.br/stats/incidentes/2019-jan-dec/total-mensal.html. Acesso em: 27 mar. 2020.

CERT.br Stats (janeiro a dezembro de 2019). Disponível em: <https://www.cert.br/stats/incidentes/2019-jan-dec/analise.html>. Acesso em: 24 abr. 2021.

CERT.br Stats (janeiro a junho de 2020). Disponível em: <https://www.cert.br/stats/incidentes/2020-jan-jun/analise.html>.

Claes Wohlin, Per Runeson, Martin Höst, Magnus C Ohlsson, Björn Regnell, andAnders Wesslén.Experimentation in software engineering. Springer Science &Business Media, 2012.

CWE - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (“SQL Injection”) (3.4.1). Disponível em: <https://cwe.mitre.org/data/definitions/89.html>.

DANTAS, Marcus Leal. **Segurança da informação: uma abordagem focada em gestão de riscos.** Olinda: Livro Rápido, 2011. 152 p.

FONTES, Edison Luiz Gonçalves. Segurança da informação. Editora Saraiva, 2017.

LEITE, Felipe Torres; COUTO, Jarbele; DE SOUSA, Reudismam Rolim. An

Experience Report About Challenges of Software Engineering as a Second Cycle Course. InSBES ’20: Simpósio Brasileiro de Engenharia de Software. Rio Grande do Norte: Natal, 2020. Disponível em: <https://dl.acm.org/doi/10.1145/3422392.3422487>. Acesso em: 21 abr. 2021.

MONTANHEIRO, Lucas Souza; CARVALHO, Ana Maria Martins. Primeiros passos para o Desenvolvimento Seguro de Aplicações Web. In: WORKSHOP DE TRABALHO DE INICIAÇÃO CIENTÍFICA E DE GRADUAÇÃO – SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 18. .2018, Natal. Anais Estendidos do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Porto Alegre: Sociedade Brasileira de Computação, out. 2018. P. 233 – 242.

OWASP, Top. Top 10-2017. *The Ten Most Critical Web Application Security Risks*. OWASP™ *Foundation*. *The free and open software security community*. URL: https://www. owasp. org/index. php/Top_10-2017_Top_10, 2017.

REDATOR. **SAST vs DAST – Entenda a diferença de uma vez por todas! | Real Protect**. Disponível em: <https://realprotect.net/sast-vs-dast-entenda-a-diferenca-de-uma-vez-por-todas/>. Acesso em: 9 maio. 2021.

ROLIM, R. et al. **Investigando as Dificuldades e Perspectivas sobre um Curso de Engenharia de Software de Dois Ciclos: Um Survey com a Visão Discente.** Pau dos Ferros, 04 abr. 2021. Disponível em: <https://sol.sbc.org.br/index.php/educomp/article/view/14471/14317>. Acesso em 30 abr. 2021.

SACRAMENTO, A. J. C. A. Uma Reflexão Sobre a Segurança nas Comunicações. Revista Militar /Nº2464. Maio de 2007, Portugal. Disponível em: Acesso em: 18 jan. 2020.

SAPTARINI, Istiningdyah; Rochimah, Siti; Yuhana, Umi Laili. Security Quality Measurement Framework for Academic Information System (AIS) Based on ISO/IEC 25010 Quality Model. 2. ed. Indonesia, Surabaya: Surabaya, 2016.

SOAPUI. **XML Bomb.** Disponível em: https://www.soapui.org/security-testing/security-scans/xml-bomb.html. Acesso em: 27 mar. 2020.

SOARES L. F. G.; LEMOS G. & COLCHE S. Redes de computadores: Das *LANs MANs* e *WANs* às Redes ATM. 2a Edição. Rio de Janeiro, R.J.: Editora Campus, 1995.

SILVA, Paulo; SERRAO, Carlos. **T10 OWASP Top 10 Riscos de Segurança Aplicacional - 2017**. 2019. Disponível em: https://github.com/OWASP/Top10/blob/master/2017/pt-pt/0x11-t10.md. Acesso em: 06 maio 2020.

SOMMERVILE, Ian. Engenharia de *Software*. São Paulo: Pearson Prentice Hall, 2011.

SPURGEON C. E. Ethernet – o guia definitivo. Rio de Janeiro, R.J.: Editora Campus, 2000.

Sullivan, B. (2008). “SDL *and the* OWASP Top 10”, https://blogs.microsoft.com/microsoftsecure/2008/05/01/sdl-and-the-owasp-top-ten/, May.

T10 OWASP Top 10 Riscos de Segurança Aplicacional - 2017. 13 fev. 2019. Disponível em: https://github.com/OWASP/Top10/blob/master/2017/pt-pt/0x11-t10.md. Acesso em: 20 mar. 2020.

TOFLER, A. *Power Shift: knowledge, wealth and violence at the edge of the 21st century*. *New York*: Bantam Books. Traduzido para Português como *powershift*: as mudanças do poder. São Paulo: Record, 1990.

VERONEZI, Felipe; GRAÇAS, Alex Pinheiro das. **Segurança e auditoria de sistemas**. Curitiba: Fael, 2017. 304 p.

GLOSSÁRIO

Backdoor - Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

Backup – O termo é usado para se referir às cópias de arquivos, feitas periodicamente, do disco rígido de um computador para fitas magnéticas ou outro tipo de mídia removível.

Billion Laughs - É um tipo de ataque de negação de serviço que visa analisadores de documentos XML. Também é conhecido como uma bomba XML ou como um ataque de expansão de entidade exponencial .

Código malicioso - Termo genérico que abrange todos os tipos de programas especificamente desenvolvidos para executar ações maliciosas em um computador.

Criptografia - Método usado para embaralhar ou codificar dados, de modo a impedir que usuários não autorizados leiam ou adulterem os dados.

DoS - Ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores.

Frameworks - É uma abstração que une códigos comuns entre vários projetos de software provendo uma funcionalidade genérica. Um framework pode atingir uma funcionalidade específica, por configuração, durante a programação de uma aplicação.

Hacking Técnicas e métodos utilizados para ganhar acesso não autorizado e explorar sistemas e redes de computadores. O hacking, consiste em entender o funcionamento dos sistemas de informação como um todo e então tirar vantagem dele.

Invasão – Acesso não autorizado a um sistema, software, arquivo, dispositivo ou serviço.

LDAP - É uma forma abreviada de falar Active Directory. LDAP, que significa Lightweight Directory Access Protocol, é um meio para consultar itens em qualquer serviço de diretório que a suporta.

Log - Termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

Pentest – É a abreviação de *Penetration Test* (Teste de Penetração, em tradução literal). É também conhecido como Teste de Intrusão. O teste de intrusão visa encontrar potenciais vulnerabilidades em um sistema, servidor ou, de forma geral, em uma estrutura de rede.

Shell - O shell é uma interface de linha de comando, o que significa que ele é baseado em texto.

APÊNDICE A – Link para o formulário aplicado como Investigando a adoção de práticas de segurança em cursos de curta duração e atuação profissional

Formulário para *website* de Pau dos Ferros - RN: https://forms.gle/exA53zoTgua8kwSN7

APÊNDICE B – Link para o repositório contendo os projetos utilizados para analisar a segurança nos cursos de curta duração.

Repositório do GitHub: https://github.com/rsobreira93/Aplicar-analise-para-o-TCC