

Universidade de Brasília – UnB
Faculdade UnB Gama – FGA
Nome do Curso

Título: Subtítulo do Trabalho

Autor: Nome do Autor
Orientador: Titulação Acadêmica e Nome do Orientador

Brasília, DF
2013



Nome do Autor

Título: Subtítulo do Trabalho

Monografia submetida ao curso de graduação
em Nome do Curso da Universidade de Bra-
sília, como requisito parcial para obtenção do
Título de Bacharel em Nome do Curso.

Universidade de Brasília – UnB

Faculdade UnB Gama – FGA

Orientador: Titulação Acadêmica e Nome do Orientador

Coorientador: quando houver, Titulação Acadêmica e Nome do
Orientador

Brasília, DF

2013

Nome do Autor

Título: Subtítulo do Trabalho/ Nome do Autor. – Brasília, DF, 2013-
69 p. : il. (algumas color.) ; 30 cm.

Orientador: Titulação Acadêmica e Nome do Orientador

Trabalho de Conclusão de Curso – Universidade de Brasília – UnB
Faculdade UnB Gama – FGA , 2013.

1. Palavra-chave01. 2. Palavra-chave02. I. Titulação Acadêmica e Nome do
Orientador. II. Universidade de Brasília. III. Faculdade UnB Gama. IV. Título:
Subtítulo do Trabalho

CDU 02:141:005.6

Errata

Elemento opcional da [ABNT \(2011, 4.2.1.2\)](#). **Caso não deseje uma errata, deixar todo este arquivo em branco.** Exemplo:

FERRIGNO, C. R. A. **Tratamento de neoplasias ósseas apendiculares com reimplantação de enxerto ósseo autólogo autoclavado associado ao plasma rico em plaquetas**: estudo crítico na cirurgia de preservação de membro em cães. 2011. 128 f. Tese (Livre-Docência) - Faculdade de Medicina Veterinária e Zootecnia, Universidade de São Paulo, São Paulo, 2011.

| Folha | Linha | Onde se lê | Leia-se |
|-------|-------|---------------|--------------|
| 1 | 10 | auto-conclavo | autoconclavo |

Nome do Autor

Título: Subtítulo do Trabalho

Monografia submetida ao curso de graduação em Nome do Curso da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Nome do Curso.

Trabalho aprovado. Brasília, DF, 01 de junho de 2013 – Data da aprovação do trabalho:

Titulação Acadêmica e Nome do Orientador
Orientador

Titulação e Nome do Professor Convidado 01
Convidado 1

Titulação e Nome do Professor Convidado 02
Convidado 2

Brasília, DF
2013

**A dedicatória é opcional. Caso não deseje uma, deixar todo este arquivo em
branco.**

*Este trabalho é dedicado às crianças adultas que,
quando pequenas, sonharam em se tornar cientistas.*

Agradecimentos

A inclusão desta seção de agradecimentos é opcional, portanto, sua inclusão fica a critério do(s) autor(es), que caso deseje(em) fazê-lo deverá(ão) utilizar este espaço, seguindo a formatação de *espaço simples e fonte padrão do texto (sem negritos, aspas ou itálico)*.

Caso não deseje utilizar os agradecimentos, deixar toda este arquivo em branco.

A epígrafe é opcional. Caso não deseje uma, deixe todo este arquivo em
branco.

*“Não vos amoldeis às estruturas deste mundo,
mas transformai-vos pela renovação da mente,
a fim de distinguir qual é a vontade de Deus:
o que é bom, o que Lhe é agradável, o que é perfeito.
(Bíblia Sagrada, Romanos 12, 2)*

Resumo

O resumo deve ressaltar o objetivo, o método, os resultados e as conclusões do documento. A ordem e a extensão destes itens dependem do tipo de resumo (informativo ou indicativo) e do tratamento que cada item recebe no documento original. O resumo deve ser precedido da referência do documento, com exceção do resumo inserido no próprio documento. (...) As palavras-chave devem figurar logo abaixo do resumo, antecidas da expressão Palavras-chave:, separadas entre si por ponto e finalizadas também por ponto. O texto pode conter no mínimo 150 e no máximo 500 palavras, é aconselhável que sejam utilizadas 200 palavras. E não se separa o texto do resumo em parágrafos.

Palavras-chave: latex. abntex. editoração de texto.

Abstract

This is the english abstract.

Key-words: latex. abntex. text editoration.

Lista de ilustrações

| | |
|---|----|
| Figura 1 – Abordagem GQM | 29 |
| Figura 2 – Atividades da Primeira Etapa | 31 |
| Figura 3 – Cronograma da Primeira Etapa | 32 |
| Figura 4 – Abordagem GQM | 34 |
| Figura 5 – Seleção dos Artigos | 36 |
| Figura 6 – Volume Anual de Artigos entre 2009 e 2025 | 39 |
| Figura 7 – Artigos Publicados em Revistas | 39 |
| Figura 8 – Quantidade de Artigos com Validação Experimental | 46 |
| Figura 9 – Tipos de Validação Experimental dos Artigos | 46 |
| Figura 10 – Wavelets correlation coefficients | 51 |

Lista de tabelas

| | |
|--|----|
| Tabela 1 – GQM Adaptado | 29 |
| Tabela 2 – GQM Adaptado | 35 |
| Tabela 3 – Protocolo de Busca | 40 |
| Tabela 4 – Continuação do Protocolo de Busca | 41 |
| Tabela 5 – Artigos Seleccionados | 42 |
| Tabela 6 – Continuação dos Artigos Seleccionados | 43 |
| Tabela 7 – Continuação dos Artigos Seleccionados (cont.) | 44 |
| Tabela 8 – Continuação dos Artigos Seleccionados (cont.) | 45 |
| Tabela 9 – Vulnerabilidades Reduzidas | 45 |
| Tabela 10 – Propriedades obtidas após processamento | 52 |

Lista de abreviaturas e siglas

Fig. Area of the i^{th} component

456 Isto é um número

123 Isto é outro número

lauro cesar este é o meu nome

Lista de símbolos

| | |
|-----------|----------------------------|
| Γ | Letra grega Gama |
| Λ | Lambda |
| ζ | Letra grega minúscula zeta |
| \in | Pertence |

Sumário

| | | |
|------------|---|-----------|
| 1 | INTRODUÇÃO | 27 |
| 1.1 | Contexto | 27 |
| 1.2 | Problema | 28 |
| 1.3 | Questão de Pesquisa | 28 |
| 1.4 | Objetivos | 29 |
| 1.5 | Estrutura do Trabalho | 30 |
| 1.6 | Cronograma e Atividades | 30 |
| 1.6.1 | Primeira Etapa | 30 |
| 2 | REVISÃO ESTRUTURADA DA LITERATURA | 33 |
| 2.1 | Protocolo | 33 |
| 2.1.1 | String de Busca | 33 |
| 2.2 | Seleção dos Artigos | 35 |
| 2.3 | Resultados | 36 |
| 2.3.1 | Which DevSecOps practices are most prevalent in organizations? | 36 |
| 2.3.2 | Which security models are most commonly employed in DevSecOps environments? | 37 |
| 2.3.3 | Which measures are commonly used for security evaluation? | 37 |
| 2.3.4 | How are security practices evaluated? | 38 |
| 2.3.5 | In what ways are security measures evaluated in organizations? | 38 |
| 2.3.6 | What types of vulnerabilities are mitigated by DevSecOps practices? | 38 |
| 2.3.7 | What tools and technologies are used in DevSecOps? | 38 |
| 2.3.8 | What is the annual volume of DevSecOps publications from 2009 to 2025? | 38 |
| 2.3.9 | How many articles were published in academic journals? | 38 |
| 2.3.10 | How many studies have experimental validation? | 38 |
| 2.3.11 | If the study has experimental validation, what type? | 38 |
| I | TEXTO E PÓS TEXTO | 47 |
| 3 | ELEMENTOS DO TEXTO | 49 |
| 3.1 | Corpo do Texto | 49 |
| 3.2 | Títulos de capítulos e seções | 49 |
| 3.3 | Notas de rodapé | 49 |
| 3.4 | Equações | 50 |
| 3.5 | Figuras e Gráficos | 50 |

| | | |
|-----|--|----|
| 3.6 | Tabela | 52 |
| 3.7 | Citação de Referências | 53 |
| 4 | ELEMENTOS DO PÓS-TEXTO | 55 |
| 4.1 | Referências Bibliográficas | 55 |
| 4.2 | Anexos | 55 |
| | REFERÊNCIAS | 57 |
| | APÊNDICES | 59 |
| | APÊNDICE A – PRIMEIRO APÊNDICE | 61 |
| | APÊNDICE B – SEGUNDO APÊNDICE | 63 |
| | ANEXOS | 65 |
| | ANEXO A – PRIMEIRO ANEXO | 67 |
| | ANEXO B – SEGUNDO ANEXO | 69 |

1 Introdução

Este capítulo introduz os conceitos fundamentais que norteiam este trabalho: experimentação em Engenharia de Software, segurança de produtos de software e DevSecOps. Adicionalmente, são apresentados o escopo do problema, a questão de pesquisa que guia a investigação e a estrutura geral do documento e das atividades.

1.1 Contexto

Avaliar os fatores de qualidade de um software é de suma importância no desenvolvimento de software e, para isso, faz-se necessária a utilização de um modelo que guie a avaliação, de forma a sistematizar o processo e reduzir subjetividades (SIAVVAS et al., 2021). Nesse sentido, o modelo proposto por McCall (MCCALL; RICHARDS; WALTERS, 1977) foi o primeiro modelo hierárquico para analisar a qualidade, no qual os diferentes fatores eram analisados por critérios e avaliados por métricas. Subsequentemente, o modelo de Boehm (BOEHM, 1978) evoluiu as ideias de McCall, e ambos se tornaram modelos seminais, servindo de referência para os modelos subsequentes.

A partir da ISO/IEC 9126 (2001), estabeleceu-se um padrão internacional para a qualidade de software que decompunha essa qualidade em características e subcaracterísticas, em um modelo hierárquico, além de definir os termos técnicos da área. A ISO/IEC 25010 (2011) surgiu como uma evolução da ISO 9126, expandindo seus conceitos e adaptando o modelo para a nova realidade da qualidade de software moderno. Diferentemente da ISO 9126, na ISO 25010 a segurança já é definida como um dos pilares da qualidade, e não como uma subcaracterística.

Como padrão internacional de segurança da informação, tem-se a ISO/IEC 27001 (2022). Ela se difere das normas de qualidade de software na medida em que seu foco está na especificação dos requisitos necessários para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI).

Contudo, tanto a ISO/IEC 25010 (2011) quanto a ISO/IEC 27001 (2022) não fornecem um método para avaliar a segurança de software de maneira quantitativa. Assim, torna-se necessário recorrer a outros modelos e ferramentas que ofereçam uma abordagem numérica para medir a segurança, por meio da definição de métricas, do seu cálculo e do estabelecimento de valores de referência para avaliá-las.

O DevOps é um paradigma que visa remover as barreiras entre os times de desenvolvimento e operações, a fim de construir um ambiente colaborativo e integrado (RAJAPAKSE et al., 2021). Seu objetivo é reduzir o ciclo de vida do desenvolvimento de

software, permitindo entregas mais frequentes. As principais práticas de DevOps são a Integração Contínua (CI), que consiste em integrar o código desenvolvido na ramificação principal com validação de build e testes de forma automática para detectar falhas, e a Entrega/Implantação Contínua (CD), que consiste em deixar o software pronto para entrar em produção e realizar o seu lançamento de forma automatizada (RAJAPAKSE et al., 2021).

Já o DevSecOps integra os princípios e práticas do DevOps, adicionando o time de segurança ao processo. Esse paradigma implementa uma abordagem de segurança chamada Shift-Left, na qual os processos de segurança são realizados desde o início do desenvolvimento, com o objetivo de evitar problemas decorrentes de uma avaliação tardia. Além disso é formado por práticas de segurança como treinamento da equipe, testes de segurança automatizados e feedback contínuo (RAJAPAKSE et al., 2021).

Nesse sentido, o modelo de maturidade de segurança OWASP DSOMM (DevSecOps Maturity Model) é uma importante ferramenta na construção e avaliação de projetos DevSecOps. Ele define atividades, métricas e tecnologias que devem ser usadas para construir um ambiente DevSecOps, além de proporcionar o acompanhamento da maturidade da segurança do projeto em cinco dimensões: Build and Deployment, Culture and Organization, Implementation, Information Gathering e Test and Verification (LANGE; KUNZ, 2024).

1.2 Problema

Medir a segurança de software representa um grande desafio (RAJAPAKSE et al., 2021). A literatura atual carece de modelos que apresentem formas sistematizadas de avaliação da segurança; frequentemente, os métodos são baseados em critérios subjetivos, como a análise manual por especialistas, e não possuem validação empírica, o que afeta a confiabilidade dos resultados (SIAVVAS et al., 2021).

No contexto DevOps, esse desafio se torna ainda mais difícil. Métodos tradicionais de análise de segurança são impraticáveis devido à velocidade das entregas (RAJAPAKSE et al., 2021). A medição da segurança se torna ainda mais desafiador ao lidar ciclos contínuos de lançamento. A segurança é uma propriedade multifacetada, emergente e dependente do contexto, o que complica sua quantificação (KUDRIAVTSEVA; GADYATSKAYA, 2024).

1.3 Questão de Pesquisa

A definição da questão de pesquisa foi elaborada utilizando a abordagem Goal Question Metric (GQM). Essa é uma abordagem que tem como objetivo definir, de ma-

neira top-down e hierárquica, os objetivos a serem alcançados, as perguntas a serem respondidas para cumprir tais objetivos e as métricas necessárias para responder a cada pergunta de forma quantitativa, como mostra a Figura 1. Essa estrutura foi adaptada para o contexto da pesquisa, conforme a Tabela 1, resultando na seguinte questão:

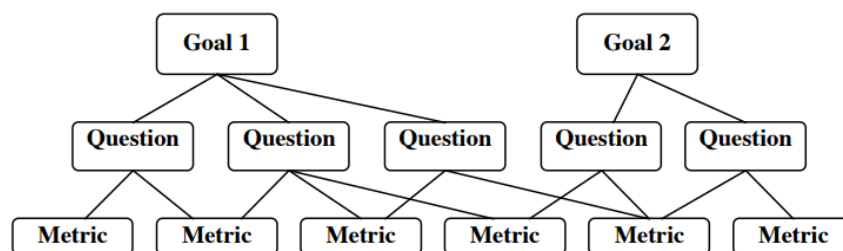
Tabela 1 – GQM Adaptado

| Característica | Valor |
|-----------------------|--|
| Analisar | A característica de qualidade de produto de software: segurança |
| Subcaracterísticas | Confidencialidade, integridade, autenticidade, responsabilidade, etc. |
| Visões | Interna e externa |
| Com o propósito de | Caracterizar |
| Com respeito a | Desenvolvimento e operação de produtos de software seguros (DevSecOps) |
| Do ponto de vista de | Pesquisador |
| No contexto de | Desenvolvimento de aplicações web seguras (software livre, organizações públicas e privadas) |

Fonte: Adaptado de BASILI, CALDIERA e ROMBACH (1994)

Como analisar a característica de segurança no desenvolvimento contínuo de sistemas web, considerando as visões de qualidade interna e externa?

Figura 1 – Abordagem GQM



Fonte: Adaptado de BASILI, CALDIERA e ROMBACH (1994)

1.4 Objetivos

O objetivo geral deste trabalho consiste em avaliar o impacto das práticas DevSecOps na qualidade interna e externa de um produto de software, por meio de uma análise quantitativa. Para alcançar este propósito, foram definidos os seguintes objetivos específicos:

- Fundamentar teoricamente os conceitos de DevSecOps, modelos de segurança e metodologias de desenvolvimento seguro.

- Incorporar um conjunto de práticas DevSecOps ao ciclo de desenvolvimento do produto de software sob análise.
- Planejar um estudo de caso focado na observação das práticas implementadas.
- Conduzir o estudo de caso, realizando a coleta e a análise das métricas de qualidade de software.
- Apresentar as conclusões e os insights resultantes desta investigação.

1.5 Estrutura do Trabalho

A seguir, são apresentados os capítulos que compõem a estrutura deste trabalho.

- Introdução: apresenta a contextualização do trabalho, o problema de pesquisa, a definição da questão de pesquisa e dos objetivos do trabalho. Por fim, descreve a estrutura das atividades realizadas.
- Revisão Estruturada da Literatura: explicita o processo empregado para seleção que fundamentam este trabalho incluindo o protocolo de pesquisa e filtragem dos estudos e os resultados obtidos.
- Referencial Teórico: estabelece a fundamentação teórica da monografia, abordando os tópicos centrais da pesquisa: DevSecOps, qualidade de software, segurança de software e modelos de avaliação de maturidade.
- Estudo de caso: descreve o protocolo utilizado para a condução do estudo de caso, detalhando seus objetivos, perguntas de pesquisa, atividades e resultados alcançados.
- Conclusão: consolida os achados obtidos ao final do estudo e como esses resultados respondem à questão de pesquisa principal, bem como as limitações do estudo e as possibilidades de aprofundamento de trabalhos futuros.

1.6 Cronograma e Atividades

1.6.1 Primeira Etapa

Esta subseção detalha as atividades desenvolvidas na primeira etapa da monografia. A Figura 2 ilustra o fluxo das atividades, enquanto a Figura 3 apresenta o cronograma correspondente.

Figura 2 – Atividades da Primeira Etapa



Fonte: Autor

- Contextualização sobre Engenharia de Software Experimental: Estudo sobre os métodos de pesquisa empírica em Engenharia de Software, como revisão sistemática da literatura, survey, experimentos e estudo de caso (WOHLIN et al., 2024), fundamentais para a condução do trabalho.
- Definição do GQM: Aplicação da abordagem Goal Question Metric (GQM) (BASILI; CALDIERA; ROMBACH, 1994) para a construção da questão principal de pesquisa, suas subquestões e as métricas que orientarão a revisão da literatura.
- Elaboração do Protocolo de Revisão: Estruturação de um protocolo de revisão sistemática da literatura (KITCHENHAM; BRERETON, 2013) para pesquisar, selecionar e analisar os artigos. Este processo inclui a definição da string de busca (baseada no framework PICO), a elaboração de sinônimos, a definição dos critérios de inclusão e exclusão e o método para extração de dados.
- Seleção dos Artigos: Execução da filtragem dos estudos por meio da leitura de títulos, resumos e palavras-chave, com a aplicação dos critérios de inclusão e exclusão definidos.
- Análise do Material Selecionado: Leitura completa dos artigos selecionados para aprofundar o conhecimento sobre o estado da arte em métodos de avaliação de segurança de sistemas web e práticas de desenvolvimento seguro.
- Definição da Proposta de Solução: Definição os modelos de segurança, as ferramentas e as atividades do estudo de caso.

Figura 3 – Cronograma da Primeira Etapa



Fonte: Autor

- Redação da Monografia: Escrita do texto da monografia, conforme a estrutura presente na Seção 1.5.
- Revisão: Realização das correções e dos ajustes solicitados pelo orientador.
- Defesa: Preparação do material e apresentação do trabalho final para a banca examinadora.

2 Revisão Estruturada da Literatura

Este capítulo destina-se a documentar o processo realizado para selecionar o conjunto de obras acadêmicas que compõe a bibliografia desta monografia. Para isso, a base de dados Scopus foi escolhida devido à sua característica de indexar diversos artigos da área da computação, muitos publicados nos principais meios de divulgação científica (ELSEVIER, 2025).

2.1 Protocolo

O protocolo utilizado para realizar a revisão estruturada da literatura foi baseado no modelo proposto por Kitchenham e Brereton (2013). Seu objetivo é tornar possível que outros pesquisadores, partindo do mesmo ponto, cheguem aos mesmos resultados, facilitando a replicabilidade em estudos futuros e permitindo a conferência dos resultados obtidos.

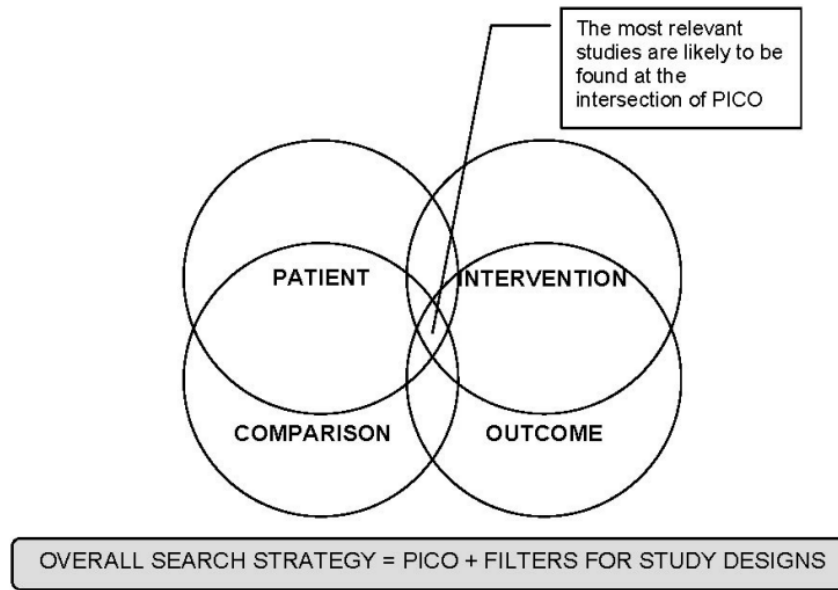
2.1.1 String de Busca

A busca em bases de dados acadêmicas requer o uso de um protocolo, pois elas indexam grande quantidade de artigos de várias áreas. Seu uso incorreto pode acarretar em um número excessivo de artigos sem relação com o tema da pesquisa ou, inversamente, retornar um volume insuficiente de estudos para responder à questão de pesquisa.

Por essa razão, o protocolo PICO foi utilizado para guiar a elaboração de uma string de busca adequada às necessidades da monografia. O protocolo, no entanto, precisou ser adaptado, pois sua origem é na medicina e nem todos os seus elementos se adequam ao nosso escopo. Uma representação visual que facilita a compreensão do protocolo pode ser vista na Figura 4 (PAI et al., 2004).

Ao adaptar o modelo PICO para o presente trabalho, suas definições adquirem um novo significado no contexto da Engenharia de Software. Por exemplo, Patient, outrora usado para indicar o perfil do paciente, passa a representar a área de aplicação, neste caso, o desenvolvimento de software. Intervention também sofre adaptação, deixando de significar "tratamento médico" para se referir à metodologia avaliada. Não obstante, Outcome mantém seu sentido original, referindo-se aos efeitos ou consequências observadas. Por fim, Comparison que está relacionada a investigar como a intervenção proposta se relaciona com outras propostas de intervenção não pode ser adotada, devido a estar muito mais alinhada com os objetivos da medicina que da engenharia de software. Assim, a definição de cada um dos elementos usados do modelo estão definidos na Tabela 2.

Figura 4 – Abordagem GQM



Fonte: (PAI et al., 2004)

Desta maneira, a string de busca foi construída usando o operador lógico OR entre os termos de cada elemento, com o objetivo de englobar todos os termos da pesquisa. Já o operador AND foi usado para conectar os diferentes elementos do protocolo PICO, assim restringindo a busca apenas aos estudos que apresentam os termos necessários para responder as perguntas de pesquisa. Ademais, foram adicionados os termos próprios da base de dados para a realização da consulta, resultando na seguinte string de busca:

```
TITLE-ABS-KEY ( ( "software development"OR "software developments"OR "software
system"OR "software systems"OR "online system"OR "online systems"OR "software
application"OR "software applications"OR "system development"OR "systems
development"OR "application development"OR "applications development") AND (
"DevSecOps"OR "cybersecurity practice"OR "cybersecurity practices"OR "security
automation"OR "security automations"OR "secure software development"OR "secure
software developments"OR "CI/CD"OR "continuous integration"OR "continuous
integrations"OR "continuous deployment"OR "continuous deployments"OR "continuous
delivery"OR "continuous deliveries"OR "DevOps"OR "security development culture"OR
"security development cultures") AND ( "security quality"OR "security qualities"OR
"software security"OR "software securities"OR "application security"OR "application
securities"OR "security improvement"OR "security improvements"OR "security
assurance"OR "security assurances"OR "vulnerability reduction"OR "vulnerability
reductions"OR "protection against threat"OR "protection against threats"OR "system
security"OR "system securities"OR "OWASP"OR "CWE"OR "common weakness"OR
"common weaknesses") )
```

Tabela 2 – GQM Adaptado

| Elementos | Termo Central | Sinônimos e Termos Relacionados |
|--------------|----------------------|--|
| Population | software development | software systems, online systems, software applications, systems development, application development |
| Intervention | DevSecOps | cybersecurity practices, security automation, secure software development, CI/CD, continuous integration, continuous deployment, continuous delivery, DevOps, security development culture |
| Outcome | security quality | software security, application security, security improvement, security assurance, vulnerability reduction, protection against threats, system security, owasp, cwe, common weakness |

Fonte: Autor

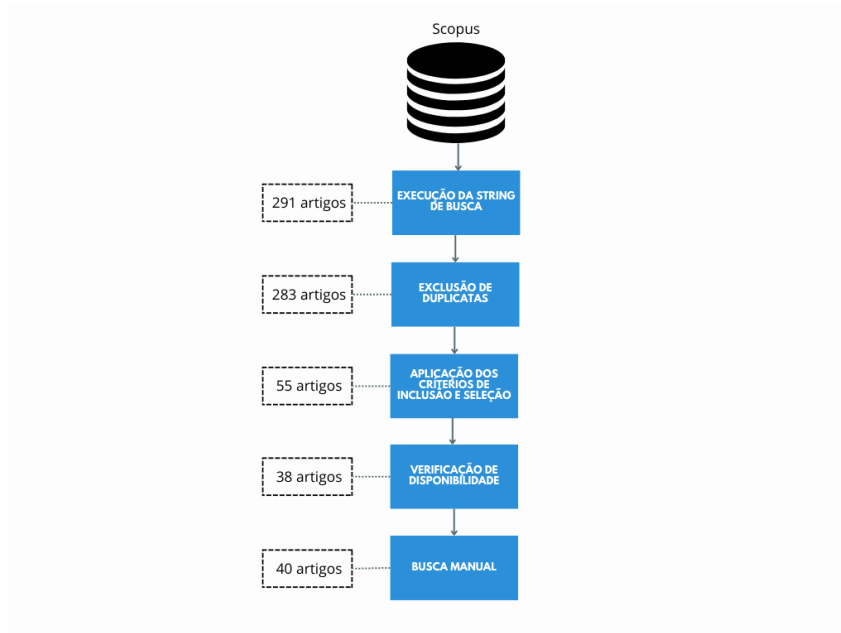
2.2 Seleção dos Artigos

Com a string de busca criada, foram estabelecidos os critérios de inclusão e exclusão visando selecionar apenas os artigos relacionados ao contexto da pesquisa. Além disso, em primeiro momento, foram lidos o título, resumo e palavras-chave de todos os artigos resultantes da execução da string de busca, isso se deu para selecionar com maior rigor aqueles estudos que por ventura não correspondessem ao objetivo do trabalho. Posteriormente, os artigos que aprovados pelos critérios de escolha foram lidos e os dados relevantes para a formulação das respostas das perguntas de pesquisa foram extraídos em um formulário. A Tabela 3 e Tabela 4 contém o protocolo completo.

Ao todo foram analisados 291 artigos resultantes da string de busca, desses 38 foram aceitos e lidos de maneira integral, sendo que esses artigos foram obtidos na base de dados Scopus (ELSEVIER, 2025) no dia 7 de maio de 2025. Afim de complementar os artigos selecionados de forma automatizada foi realizada uma busca manual com o objetivo de responder de maneira mais assertiva as perguntas de pesquisa, resultando em mais dois artigos, Accelerate State of DevOps 2024 (DORA, 2024) e Quantitative DevSecOps Metrics for Cloud-Based Web Microservices (ZHANG; ZHANG, 2024), usados para compor o referencial teórico, totalizando 40 artigos. Os artigos selecionados estão

dispostos nas Tabela 5, 6, 7 e 8. Para facilitar a compreensão do protocolo de seleção de artigos pode-se verificar a Figura 5, que ilustra todas as etapas explanadas anteriormente.

Figura 5 – Seleção dos Artigos



Fonte: Autor

2.3 Resultados

Esta seção apresentará os resultados obtidos com a leitura do material coletado. Durante o processo de leitura, com o objetivo de facilitar a elaboração das respostas da perguntas de pesquisa e para possibilitar a aferição da revisão da literatura, foi construída uma planilha ¹ contendo todos os dados extraídos dos artigos, a planilha está separada em várias páginas, pois cada página está relacionada com uma pergunta de pesquisa ou um conjunto de perguntas de pesquisa semelhantes, desse modo, possibilitando que o leitor consiga enxergar como cada artigo responde as perguntas de pesquisa. Assim, com os dados extraídos dos artigos foi possível estruturar o conhecimento para responder as perguntas de pesquisa baseado no estado da arte sobre o tema.

Nas subseções a seguir são apresentadas as respostas para as perguntas de pesquisa.

2.3.1 Which DevSecOps practices are most prevalent in organizations?

- Metodologias e Cultura: Segundo Shift Security Left eh o principio fundamental do DevSecOps, Continuous Integration, Continuous Delivery, Continuous Deployment, Continuous Feedback, Continuous Vulnerability Assessment

¹ Planilha com o resultado da revisão: <https://docs.google.com/spreadsheets/d/1HdgzzRaP8YIS_08hZhIKaUKV9HKP2dTaq4xWVKFzh84/edit?usp=sharing>

- Testes de Segurança: SAST, DAST, IAST, Fuzz testing, BDST, WAST, SAS
- Infraestrutura e Operações: IaC, Secure Infrastructure, Container Security,
- Acompanhamento: Automation, Monitoring, Logging

2.3.2 Which security models are most commonly employed in DevSecOps environments?

- OWASP SAMM
- OWASP DSOMM
- BSIMM
- DORA

2.3.3 Which measures are commonly used for security evaluation?

- Non-Comment Lines of Code
- Design Defect Ratio
- Shared or Unknown Library Ratio
- Technical Debt Ratio
- Continuous Deployment Cycles Score
- Mean Change Lead Time
- Mean Time to Recover
- Mean Number of Test Cases Per Parameter
- Points of Environmental Risk
- Time for Response
- Throughput
- Errors Per Time Unit
- Change lead time
- Deployment frequency
- Change fail percentage
- Failed deployment recovery time

2.3.4 How are security practices evaluated?

- auditorias
- avaliação da maturidade
- avaliação de métricas

2.3.5 In what ways are security measures evaluated in organizations?

- Impacto das métricas nos KPIs
- Dashboards e relatórios automatizados
- Adaptação ao compliance/regulação

2.3.6 What types of vulnerabilities are mitigated by DevSecOps practices?

2.3.7 What tools and technologies are used in DevSecOps?

- Monitoramento: Prometheus, Grafana, Loki
- Infraestrutura: Terraform, Kubernetes, Docker
- CI/CD: Jenkins, GitLab CI/CD, GitHub Actions, Tekton, ArgoCD
- Testes: SonarQube, FindBugs, Snyk, OWASP Dependency-Check, OWASP ZAP, Trivy, Detect Secrets, Asylo, StackHawk, JMeter, Selenium

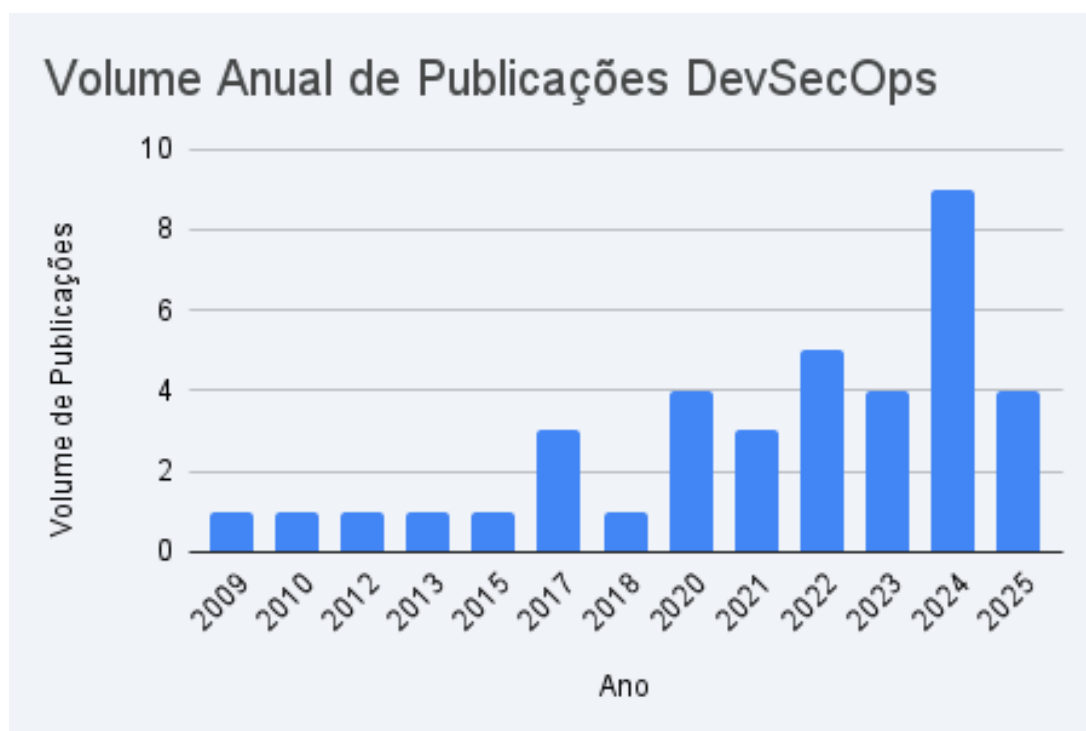
2.3.8 What is the annual volume of DevSecOps publications from 2009 to 2025?

2.3.9 How many articles were published in academic journals?

2.3.10 How many studies have experimental validation?

2.3.11 If the study has experimental validation, what type?

Figura 6 – Volume Anual de Artigos entre 2009 e 2025



Fonte: Autor

Figura 7 – Artigos Publicados em Revistas



Fonte: Autor

Tabela 3 – Protocolo de Busca

| | |
|-----------------------|---|
| Perguntas de Pesquisa | <ol style="list-style-type: none"> 1. How can the security aspect in the continuous development of web systems be analyzed considering internal and external quality perspectives? 2. Which DevSecOps practices are most prevalent in organizations? 3. Which security models are most commonly employed in DevSecOps environments? 4. Which measures are commonly used for security evaluation? 5. How are security practices evaluated? 6. In what ways are security measures evaluated in organizations? 7. What types of vulnerabilities are mitigated by DevSecOps practices? 8. What tools and technologies are used in DevSecOps? 9. What is the annual volume of DevSecOps publications from 2009 to 2025? 10. How many articles were published in academic journals? 11. How many studies have experimental validation? 12. If the study has experimental validation, what type? |
| String de Busca | Tabela 2 |
| Critérios de Inclusão | <ol style="list-style-type: none"> 1. Addresses the use of secure development practices 2. Emphasizes the security quality of web systems 3. Evaluates quality models with a focus on security 4. Focuses on software products 5. Includes experimental validation |

Fonte: Autor

Tabela 4 – Continuação do Protocolo de Busca

| | |
|------------------------|---|
| Perguntas de Exclusão | <ol style="list-style-type: none"> 1. Articles in languages other than English or Portuguese 2. Duplicate publication 3. Publications with a release date prior to 2009 4. Studies focusing on hardware, mobile, IoT security, or other topics unrelated to web systems. |
| Formulário de Extração | <ol style="list-style-type: none"> 1. Title 2. Abstract 3. Publication Year 4. Publication Source 5. Authors 6. Keywords 7. Prevalent DevSecOps Practices 8. Security Models Employed 9. Security Evaluation Measures 10. Security Practices Evaluation 11. Security Models Analysis 12. Organizational Security Evaluation 13. Mitigated Vulnerabilities 14. Tools and Technologies 15. Published in Academic Journal 16. Experimental Validation 17. Type of Experimental Validation 18. Secondary Research |

Fonte: Autor

Tabela 5 – Artigos Selecionados

| Nº | Título | Publicado em Revista | Validação Experimental |
|----|---|----------------------|------------------------|
| 1 | Development of Secure Software Based on the New DevSecOps Technology | Sim | Não |
| 2 | Automating Security in a Continuous Integration Pipeline | Não | Não |
| 3 | Extensive Review of Threat Models for DevSecOps | Sim | Não |
| 4 | Implementing and Automating Security Scanning to a DevSecOps CI/CD Pipeline | Sim | Não |
| 5 | Automating Static Code Analysis Through CI/CD Pipeline Integration | Sim | Sim |
| 6 | Design and Practice of Security Architecture via DevSecOps Technology | Sim | Sim |
| 7 | Implementation of DevSecOps by Integrating Static and Dynamic Security Testing in CI/CD Pipelines | Sim | Não |
| 8 | Research of Static Application Security Testing Technique Problems and Methods for Solving Them | Sim | Não |
| 9 | A Large-scale Fine-grained Empirical Study on Security Concerns in Open-source Software | Sim | Sim |
| 10 | Evolution of secure development lifecycles and maturity models in the context of hosted solutions | Não | Não |

Fonte: Autor

Tabela 6 – Continuação dos Artigos Seleccionados

| Nº | Título | Publicado em Revista | Validação Experimental |
|----|--|----------------------|------------------------|
| 11 | Automation and DevSecOps: Streamlining Security Measures in Financial System | Sim | Não |
| 12 | Securing the development and delivery of modern applications | Sim | Não |
| 13 | You cannot improve what you do not measure: A triangulation study of software security metrics | Sim | Sim |
| 14 | On DevSecOps and Risk Management in Critical Infrastructures: Practitioners' Insights on Needs and Goals | Sim | Sim |
| 15 | Container Security in Cloud Environments: A Comprehensive Analysis and Future Directions for DevSecOps | Não | Sim |
| 16 | Microservices-based DevSecOps Platform using Pipeline and Open Source Software | Não | Não |
| 17 | Securing the Digital Frontier: A Proactive Approach to Software Development | Sim | Não |
| 18 | A Secure Software Development Methodology for Enterprise Business Applications | Sim | Sim |
| 19 | Building Resilient CI/CD Pipelines: A DevOps Security-First Framework | Sim | Não |
| 20 | Review of Techniques for Integrating Security in Software Development Lifecycle | Não | Não |

Fonte: Autor

Tabela 7 – Continuação dos Artigos Seleccionados (cont.)

| Nº | Título | Publicado em Revista | Validação Experimental |
|----|--|----------------------|------------------------|
| 21 | A hierarchical model for quantifying software security based on static analysis alerts and software metrics | Sim | Sim |
| 22 | A preventive secure software development model for a software factory: A case study | Sim | Sim |
| 23 | Security impacts of sub-optimal DevSecOps implementations in a highly regulated environment | Sim | Sim |
| 24 | A survey and comparison of secure software development standards | Sim | Sim |
| 25 | Continuous Security Testing: A Case Study on Integrating Dynamic Security Testing Tools in CI/CD Pipelines | Sim | Sim |
| 26 | Infiltrating Security into Development: Exploring the World's Largest Software Security Study | Não | Sim |
| 27 | Challenges and solutions when adopting DevSecOps: A systematic review | Sim | Não |
| 28 | Systematic Mapping Study on Security Approaches in Secure Software Engineering | Sim | Não |
| 29 | Systematic Literature Review on Security Risks and its Practices in Secure Software Development | Sim | Não |
| 30 | BP: Security concerns and best practices for automation of software deployment processes: An industrial case study | Sim | Sim |

Fonte: Autor

Tabela 8 – Continuação dos Artigos Selecionados (cont.)

| Nº | Título | Publicado em Revista | Validação Experimental |
|----|---|----------------------|------------------------|
| 31 | Static analysis for web service security - Tools & techniques for a secure development life cycle | Sim | Não |
| 32 | Security characterization for evaluation of software architectures using ATAM | Sim | Sim |
| 33 | Software security | Sim | Não |
| 34 | Using the ISO/IEC 27034 as reference to develop an application security control library | Sim | Sim |
| 35 | Hunting for aardvarks: Can software security be measured? | Não | Não |
| 36 | Francois Raynaud on DevSecOps | Sim | Não |
| 37 | Integrating application security into software development | Sim | Não |
| 38 | Busting a myth: Review of agile security engineering methods | Sim | Não |

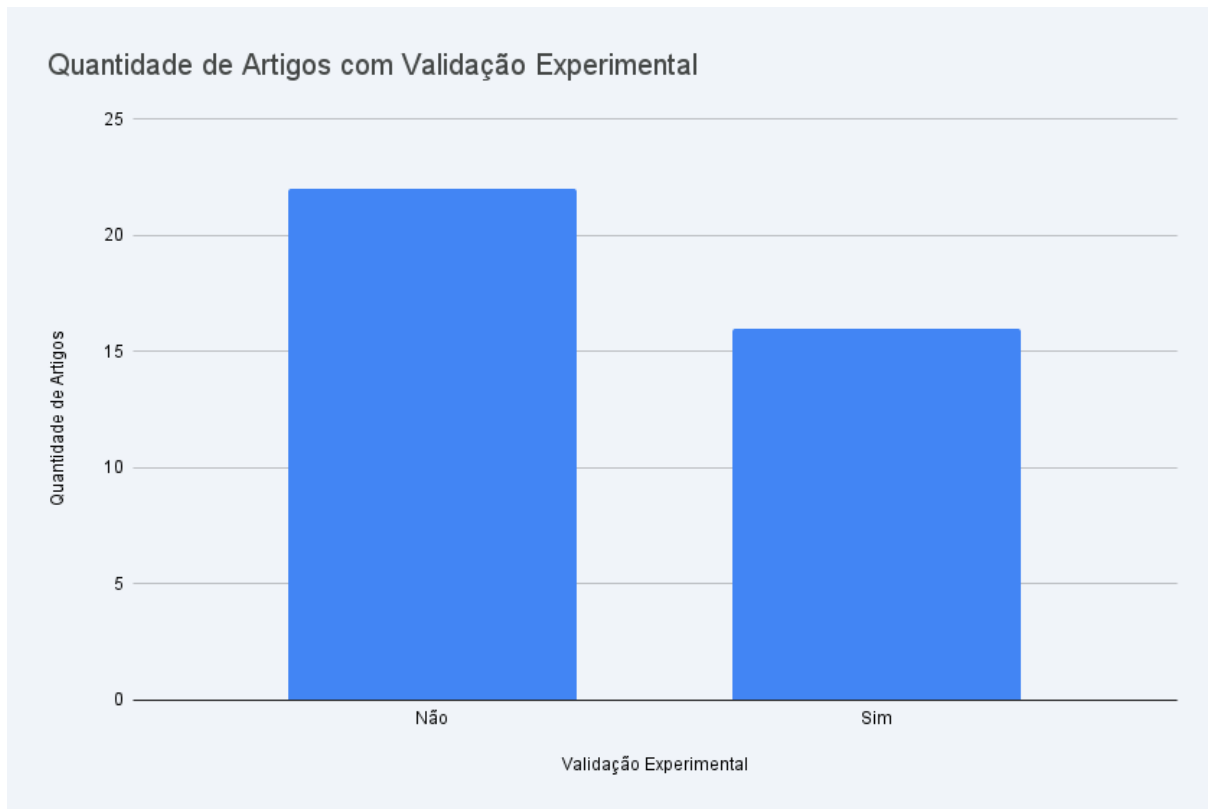
Fonte: Autor

Tabela 9 – Vulnerabilidades Reduzidas

| Vulnerabilidade | Descrição | Referência |
|---------------------------|-----------|------------|
| SQL Injection | - | - |
| Command Injection | - | - |
| XSS | - | - |
| XXE | - | - |
| Buffer Overflow | - | - |
| CSRF | - | - |
| DDoS | - | - |
| MITM | - | - |
| Broken Authentication | - | - |
| Broken Access Control | - | - |
| Security Misconfiguration | - | - |
| Session Hijacking | - | - |
| SSRF | - | - |

Fonte: Autor

Figura 8 – Quantidade de Artigos com Validação Experimental



Fonte: Autor

Figura 9 – Tipos de Validação Experimental dos Artigos



Fonte: Autor

Parte I

Texto e Pós Texto

3 Elementos do Texto

3.1 Corpo do Texto

O estilo de redação deve atentar a boa prática da linguagem técnica. Para a terminologia metrological usar o Vocabulário Internacional de Termos Fundamentais e Gerais de Metrologia (INMETRO, 2013).

Grandezas dimensionais devem ser apresentadas em unidades consistentes com o Sistema Internacional de Unidades (SI). Outras unidades podem ser usadas como unidades secundárias entre parênteses se necessário. Exceções são relacionadas a unidades não-SI usadas como identificadores comerciais como pro exemplo “disquete de 3¹/₂ polegadas”.

Na apresentação de números ao longo do texto usar vírgula para separar a parte decimal de um número. Resultados experimentais devem ser apresentados com sua respectiva incerteza de medição.

3.2 Títulos de capítulos e seções

Recomendações de formatação de seções (texto informativo: o L^AT_EX já formata as seções automaticamente, se utilizado o comando `\section{Nome da Seção}`):

1 SEÇÃO PRIMÁRIA - MAIÚSCULAS; NEGRITO; TAMANHO 12;

1.1 SEÇÃO SECUNDÁRIA – MAIÚSCULAS; NORMAL; TAMANHO 12;

1.1.1 Seção terciária - Minúsculas, com exceção da primeira letra; negrito; tamanho 12;

1.1.1.1 Seção quaternária - Minúsculas, com exceção da primeira letra; normal tamanho 12;

1.1.1.1.1 Seção quinária - Minúsculas, com exceção da primeira letra; itálico; tamanho 12.

3.3 Notas de rodapé

Notas eventualmente necessárias devem ser numeradas de forma seqüencial ao longo do texto no formato 1, 2, 3... sendo posicionadas no rodapé de cada página na qual a nota é utilizada.¹

¹ Como, por exemplo, esta nota. O L^AT_EX tomará conta da numeração automaticamente.

3.4 Equações

Equações matemáticas devem ser numeradas sequencialmente e alinhadas a esquerda com recuo de 0,6 cm. Usar numerais arábicos entre parênteses, alinhado a direita, no formato Times New Roman de 9 pts. para numerar as equações como mostrado na Eq. 3.1 (novamente, o \LaTeX formata as equações automaticamente).

Referências a equações no corpo do texto devem ser feitas como “Eq. 3.1” quando no meio de uma frase ou como “Equação 3.1” quando no início de uma sentença. Um espaçamento de 11 pontos deve ser deixado acima, abaixo e entre equações subsequentes. Para uma apresentação compacta das equações deve-se usar os símbolos e expressões matemáticos mais adequados e parênteses para evitar ambigüidades em denominadores. Os símbolos usados nas equações citados no texto devem apresentar exatamente a mesma formatação usada nas equações.

$$\frac{d\mathbf{C}}{dw} = \frac{du}{dw} \cdot \mathbf{F}_u + \frac{dv}{dw} \cdot \mathbf{F}_v \quad (3.1)$$

O significado de todos os símbolos mostrados nas equações deve ser apresentado na lista de símbolos no início do trabalho, embora, em certas circunstâncias o autor possa para maior clareza descrever o significado de certos símbolos no corpo do texto, logo após a equação.

Se uma equação aparecer no meio do parágrafo, como esta

$$x^n + y^n = z^n, \quad (3.2)$$

onde $x, y, z, n \in \mathbf{N}$, o texto subsequente faz parte do parágrafo e não deve ser indentado.

3.5 Figuras e Gráficos

As figuras devem ser centradas entre margens e identificadas por uma legenda alinhada a esquerda com recuo especial de deslocamento de 1,8 cm, com mostrado na Fig. (10). O tamanho das fontes empregadas nos rótulos e anotações usadas nas figuras deve ser compatível com o usado no corpo do texto. Rótulos e anotações devem estar em português, com todas as grandezas mostradas em unidades do SI (Sistema Internacional de unidades) (mais uma vez, o \LaTeX cuidará dos aspectos de formatação e fonte das figuras).

Todas as figuras, gráficos e fotografias devem ser numeradas e referidas no corpo do texto adotando uma numeração sequencial de identificação. As figuras e gráficos devem ser claras e com qualidade adequada para eventual reprodução posterior tanto em cores quanto em preto-e-branco.

As abscissas e ordenadas de todos os gráficos devem ser rotuladas com seus respectivos títulos em português seguida da unidade no SI que caracteriza a grandeza entre colchetes.

A referência explícita no texto à uma figura deve ser feita como “Fig. 10” quando no meio de uma frase ou como “Figura 10” quando no início da mesma. Referências implícitas a uma dada figura devem ser feitas entre parênteses como (Fig. 10). Para referências a mais de uma figura as mesmas regras devem ser aplicadas usando-se o plural adequadamente. Exemplos:

- “Após os ensaios experimentais, foram obtidos os resultados mostrados na Fig. 10, que ...”
- “A Figura 10 apresenta os resultados obtidos, onde pode-se observar que ...”
- “As Figuras 1 a 3 apresentam os resultados obtidos, ...”
- “Verificou-se uma forte dependência entre as variáveis citadas (Fig. 10), comprovando ...”

Cada figura deve ser posicionada o mais próxima possível da primeira citação feita à mesma no texto, imediatamente após o parágrafo no qual é feita tal citação, se possível, na mesma página. Em \LaTeX o comando `\label` deve suceder o comando `\caption` para que as referências às figuras fiquem com a numeração correta.

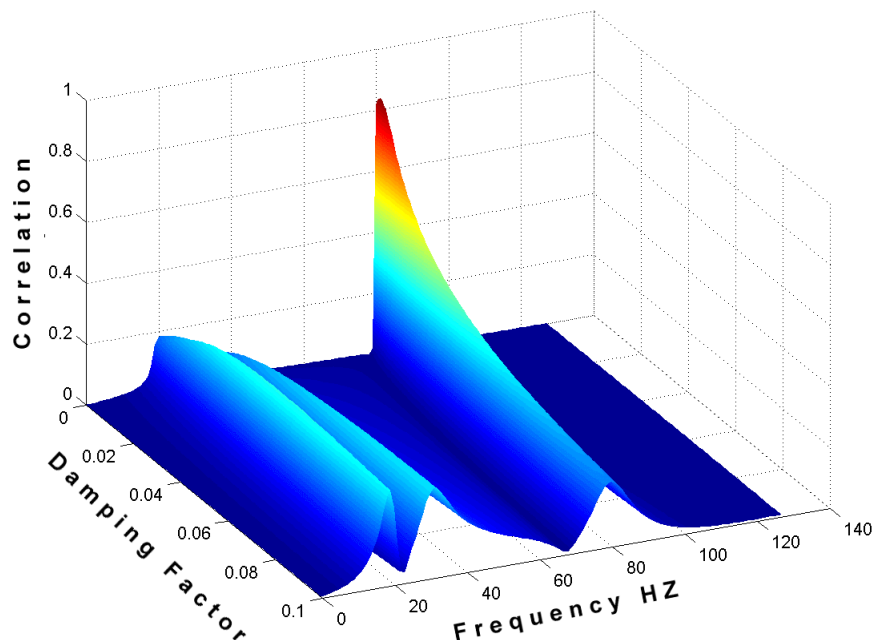


Figura 10 – Wavelets correlation coefficients

3.6 Tabela

As tabelas devem estar centradas entre margens e identificadas por uma legenda alinhada a esquerda, com recuo especial de deslocamento de 1,8 cm, posicionada acima da tabela com mostrado na Tab. 10, a título de exemplo. O tamanho das fontes empregadas nos rótulos e anotações usadas nas tabelas deve ser compatível com o usado no corpo do texto. Rótulos e anotações devem estar em português. Um espaçamento de 11 pts deve ser deixado entre a legenda e a tabela, bem como após a tabela. A numeração, a fonte e a formatação são automáticas quando se usa o L^AT_EX.

As grandezas dimensionais mostradas em cada tabela devem apresentar unidades consistentes com o SI. As unidades de cada variável devem ser mostradas apenas na primeira linha e/ou coluna da tabela, entre colchetes

A referência explícita no texto à uma dada tabela deve ser feita como “Tab. 10” quando no meio de uma frase ou como “Tabela 10” quando no início da mesma. Referências implícitas a uma dada tabela devem ser feitas entre parênteses como (Tab. 10). Para referências a mais de uma tabela as mesmas regras devem ser aplicadas usando-se o plural adequadamente. Exemplos:

- “Após os ensaios experimentais, foram obtidos os resultados mostrados na Tab. 10, que ...”
- “A Tabela 10 apresenta os resultados obtidos, onde pode-se observar que ...”
- “As Tabelas 1 a 3 apresentam os resultados obtidos, ...”
- “Verificou-se uma forte dependência entre as variáveis citadas (Tab. 10), comprovando ...”

Cada tabela deve ser posicionada o mais próxima possível da primeira citação feita à mesma no texto, imediatamente após o parágrafo no qual é feita a citação, se possível, na mesma página.

Tabela 10 – Propriedades obtidas após processamento

| Processing type | Property 1 (%) | Property 2 [μm] |
|-----------------|----------------|------------------------|
| Process 1 | 40.0 | 22.7 |
| Process 2 | 48.4 | 13.9 |
| Process 3 | 39.0 | 22.5 |
| Process 4 | 45.3 | 28.5 |

3.7 Citação de Referências

Referências a outros trabalhos tais como artigos, teses, relatórios, etc. devem ser feitas no corpo do texto devem estar de acordo com a norma corrente ABNT NBR 6023:2002 (ABNT, 2000), esta última baseada nas normas ISO 690:1987:

- “[Bordalo, Ferziger e Kline \(1989\)](#), mostraram que...”
- “Resultados disponíveis em ([COIMBRA, 1978](#)), ([CLARK, 1986](#)) e ([SPARROW, 1980](#)), mostram que...”

Para referências a trabalhos com até dois autores, deve-se citar o nome de ambos os autores, por exemplo: “[Soviero e Lavagna \(1997\)](#), mostraram que...”

Para citação direta, o texto deve estar em fonte 10 com recuo de 4cm da margem esquerda:

Foram desenvolvidos métodos eficazes de especificação, *design* e implementação de software. Novas notações e ferramentas reduziram o esforço necessário para produzir sistemas grandes e complexos ([SOMMERVILLE, 2007](#)).

4 Elementos do Pós-Texto

Este capítulo apresenta instruções gerais sobre a elaboração e formatação dos elementos do pós-texto a serem apresentados em relatórios de Projeto de Graduação. São abordados aspectos relacionados a redação de referências bibliográficas, bibliografia, anexos e contra-capá.

4.1 Referências Bibliográficas

O primeiro elemento do pós-texto, inserido numa nova página, logo após o último capítulo do trabalho, consiste da lista das referências bibliográficas citadas ao longo do texto.

Cada referência na lista deve ser justificada entre margens e redigida no formato Times New Roman com 11pts. Não é necessário introduzir uma linha em branco entre referências sucessivas.

A primeira linha de cada referência deve ser alinhada à esquerda, com as demais linhas da referência deslocadas de 0,5 cm a partir da margem esquerda.

Todas as referências aparecendo na lista da seção “Referências Bibliográficas” devem estar citadas no texto. Da mesma forma o autor deve verificar que não há no corpo do texto citação a referências que por esquecimento não foram incluídas nesta seção.

As referências devem ser listadas em ordem alfabética, de acordo com o último nome do primeiro autor. Alguns exemplos de listagem de referências são apresentados no Anexo I.

Artigos que ainda não tenham sido publicados, mesmo que tenham sido submetidos para publicação, não deverão ser citados. Artigos ainda não publicados mas que já tenham sido aceitos para publicação devem ser citados como “in press”.

A norma ([ABNT, 2000](#)), que regulamenta toda a formatação a ser usada na elaboração de referências a diferentes tipos de fontes de consulta, deve ser rigidamente observada. Sugere-se a consulta do trabalho realizado por ([ARRUDA, 2007](#)), disponível na internet.

4.2 Anexos

As informações citadas ao longo do texto como “Anexos” devem ser apresentadas numa seção isolada ao término do trabalho, após a seção de referências bibliográficas. Os anexos devem ser numerados sequencialmente em algarismos romanos maiúsculos (I,

II, III, ...). A primeira página dos anexos deve apresentar um índice conforme modelo apresentado no Anexo I, descrevendo cada anexo e a página inicial do mesmo.

A referência explícita no texto à um dado anexo deve ser feita como “Anexo 1”. Referências implícitas a um dado anexo devem ser feitas entre parênteses como (Anexo I). Para referências a mais de um anexo as mesmas regras devem ser aplicadas usando-se o plural adequadamente. Exemplos:

- “Os resultados detalhados dos ensaios experimentais são apresentados no Anexo IV, onde ...”
- “O Anexo I apresenta os resultados obtidos, onde pode-se observar que ...”
- “Os Anexos I a IV apresentam os resultados obtidos ...”
- “Verificou-se uma forte dependência entre as variáveis citadas (Anexo V), comprovando ...”

Referências

ARRUDA, M. B. B. Como fazer referências: bibliográficas, eletrônicas e demais formas de documentos. 2007. Disponível em: <<http://bu.ufsc.br/framerefer.html>>. Citado na página 55.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR 14724*: Informação e documentação — referências. Rio de Janeiro, 2000. Citado na página 55.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR 14724*: Informação e documentação — trabalhos acadêmicos — apresentação. Rio de Janeiro, 2011. 15 p. Citado na página 3.

BORDALO, S. N.; FERZIGER, J. H.; KLINE, S. J. The development of zonal models for turbulence. In: *Proceedings of the 10th Brazilian Congress of Mechanical Engineering*. [S.l.: s.n.], 1989. v. 1, p. 41–44. Citado na página 53.

CLARK, J. A. Private communication. University of Michigan, 1986. Citado na página 53.

COIMBRA, A. L. Lessons of continuum mechanics. São Paulo, Brazil, p. 428, 1978. Citado na página 53.

INMETRO. *Vocabulário internacional de termos fundamentais e gerais de metrologia*. Rio de Janeiro, Brasil, 2013. 75 p. Citado na página 49.

SOMMERVILLE, I. *Software Engineering*. 9th. ed. USA: Addison-Wesley Publishing Company, 2007. ISBN 978-0-321-31379-9, 0-321-31379-8. Citado na página 53.

SOVIERO, P. A. O.; LAVAGNA, L. G. M. A numerical model for thin airfoils in unsteady motion. In: *Journal of the Brazilian Society of Mechanical Sciences*. [S.l.: s.n.], 1997. v. 19, n. 3, p. 332–340. Citado na página 53.

SPARROW, E. M. Forced convection heat transfer in a duct having spanwise-periodic rectangular protuberances. In: *Numerical Heat Transfer*. [S.l.: s.n.], 1980. v. 3, p. 149–167. Citado na página 53.

Apêndices

APÊNDICE A – Primeiro Apêndice

Texto do primeiro apêndice.

APÊNDICE B – Segundo Apêndice

Texto do segundo apêndice.

Anexos

ANEXO A – Primeiro Anexo

Texto do primeiro anexo.

ANEXO B – Segundo Anexo

Texto do segundo anexo.