UNIVERSIDADE
FEDERAL DO CEARÁ

Cibersegurança em Ambientes DevOps

Uma Revisão Sistemática da Literatura

Roberto Carlos Bautista Ramos Sang Guun Yoo

Escuela Politécnica Nacional – Quito, Equador

Baseado no artigo: *Cybersecurity in DevOps Environments: A Systematic Literature Review*

Julho de 2025

Roteiro da Apresentação

Introdução

- **Paradigma DevOps:** Solução para acelerar a entrega de valor, melhorando a qualidade do software e a colaboração entre equipes de Desenvolvimento (Dev) e Operações (Ops).
- **Flexibilidade e Complexidade:** A agilidade operacional do DevOps aumentou a complexidade da superfície de ataque, tornando a cibersegurança um desafio central.
- **Limitações da Segurança Tradicional:** Abordagens reativas são insuficientes em ambientes com múltiplos deploys diários. A segurança precisa ser integrada desde o início.
- **Surgimento do DevSecOps:** Adiciona a segurança como um elemento recorrente e automatizado em todo o ciclo de vida do software, promovendo a cultura de "shift-left security".

- **Novos Vetores de Ataque:** Ferramentas como Kubernetes, Docker e pipelines de CI/CD (Jenkins, GitLab CI) introduziram novas vulnerabilidades.
- **Riscos Críticos:** Ameaças incluem configurações incorretas de infraestrutura, cadeias de suprimentos comprometidas (ex: SolarWinds) e exposição acidental de segredos.
- **Conhecimento Fragmentado:** A literatura científica sobre o tema é vasta, mas dispersa e com diferentes níveis de validação empírica.

Justificativa

Esta revisão sistemática visa consolidar o conhecimento, analisando os desafios de segurança em DevOps, identificando estratégias de mitigação e avaliando seu impacto no desempenho dos sistemas.

Objetivo Geral

Realizar uma revisão sistemática da literatura para analisar os desafios de cibersegurança em ambientes DevOps, identificando ameaças, vetores de ataque, vulnerabilidades e as estratégias de mitigação documentadas.

Objetivos Específicos (Baseados nas Questões de Pesquisa)

1. Mapear as principais ciberameaças e vetores de ataque, e as abordagens para mitigar seu impacto.
2. Identificar as vulnerabilidades inerentes aos ambientes DevOps e as medidas corretivas implementadas.
3. Analisar como as estratégias de mitigação influenciam o desempenho do sistema e quais se mostram mais eficazes.

Metodologia

- Protocolo rigoroso baseado nas diretrizes de **Kitchenham & Charters (2007)**.
- Processo estruturado e replicável para garantir a validade dos achados.

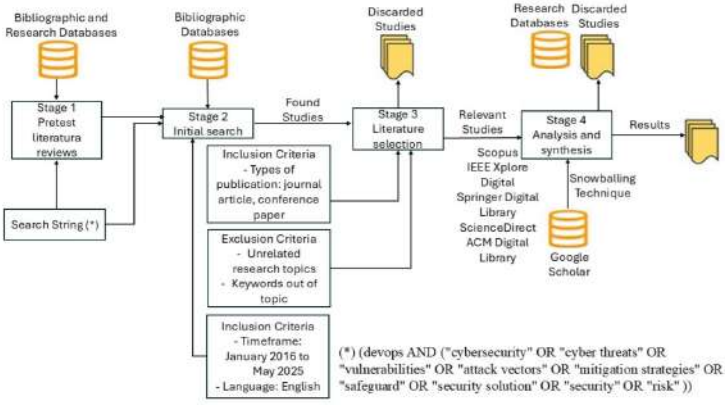

Figura: Fases do Processo Metodológico da RSL (Adaptado de Bautista Ramos & Yoo, 2025).

Fontes de Dados

- Scopus
- IEEE Xplore
- SpringerLink
- ScienceDirect
- ACM Digital Library

Período de Análise

Janeiro de 2016 a Maio de 2025.

String de Busca Principal

```
(devops AND (‘‘cybersecurity’’ OR ‘‘cyber
threats’’ OR ‘‘vulnerabilities’’ OR ‘‘attack
vectors’’ OR ‘‘mitigation strategies’’ OR
‘‘safeguard’’ OR ‘‘security solution’’ OR
‘‘security’’ OR ‘‘risk’’))
```

Critérios de Seleção

- Artigos de periódicos e conferências revisados por pares.
- Publicações em inglês.
- Foco explícito em cibersegurança no contexto DevOps.

Metodologia: Fluxo de Seleção dos Estudos

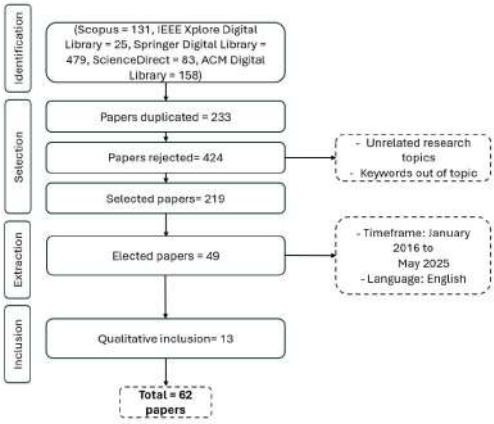

Figura: Diagrama de fluxo da identificação e seleção dos artigos (Adaptado de Bautista Ramos & Yoo, 2025).

- **Busca Inicial:** 876 artigos encontrados.
- **Após Remoção de Duplicatas e Triagem:** 219 artigos selecionados.
- **Após Leitura Completa e Avaliação:** 49 artigos eleitos.
- **Adicionados via Snowballing:** 13 artigos.
- **Corpus Final:** 62 estudos primários.

Resultados

Resultados: Principais Ameaças Identificadas

- **Configurações Incorretas em IaC e Contêineres:** Principal fonte de exposição de serviços críticos.
- **Gerenciamento Inadequado de Acessos Privilegiados:** Causa escalonamento de privilégios e acesso indevido a recursos.
- **Ataques à Cadeia de Suprimentos (Supply Chain):** Injeção de malware através de dependências e ferramentas de terceiros.
- **Falta de Autenticação entre Microsserviços:** Facilita movimentos laterais dentro de arquiteturas distribuídas.
- **Fator Humano (Shadow IT):** Uso de ferramentas não autorizadas que introduzem vetores de ataque não auditados.

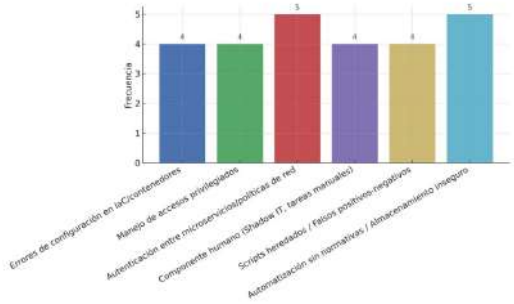

Figura: Frequência das Ameaças Identificadas na Literatura.

- **Injeção de Código em Pipelines CI/CD:** Permite a execução automatizada de comandos maliciosos.
- **Credenciais Embutidas ou Mal Gerenciadas:** Exposição de segredos que dão acesso persistente a recursos críticos.
- **Acesso Não Controlado a Repositórios Públicos:** Exfiltração de código-fonte, tokens e chaves de API.
- **Movimento Lateral entre Serviços:** Exploração da falta de segmentação de rede para se mover dentro da infraestrutura.
- **Inclusão de Dependências Vulneráveis:** Principal ponto de entrada para ataques de supply chain.

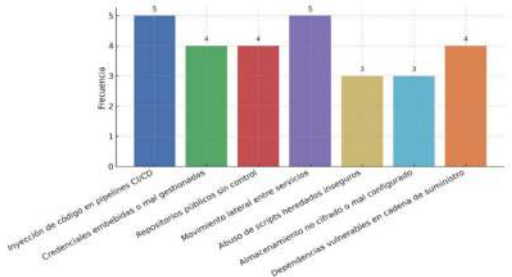

Figura: Frequência dos Vetores de Ataque Identificados.

- **Falta de Testes de Segurança Automatizados:** Permite que falhas críticas cheguem aos ambientes de produção.
- **Exposição e Má Gestão de Segredos:** Principalmente em pipelines de CI/CD e repositórios de código.
- **Configurações Inseguras em Contêineres:** Privilégios elevados, falta de limites de recursos e exposição de portas de rede.
- **Práticas de Desenvolvimento Inseguras:** Falta de padrões de codificação segura e uso de scripts legados.
- **Falta de Monitoramento de Cibersegurança em Tempo Real:** Impede a detecção de ataques em andamento.

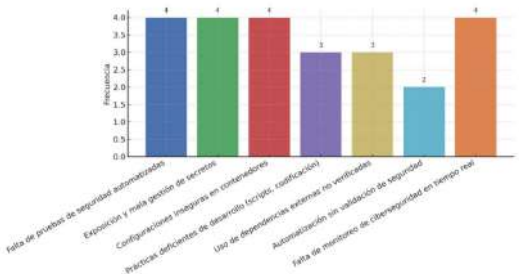

Figura: Frequência das Vulnerabilidades Identificadas.

- **Automação de Testes (SAST/DAST/IAST):** Integração de scanners de segurança no pipeline de CI/CD para detecção precoce.
- **Gestão Automatizada de Segredos:** Uso de cofres (vaults) como HashiCorp Vault para gerenciar credenciais e tokens.
- **Validação de Infraestrutura como Código (IaC):** Ferramentas como OPA e Terraform Validator para garantir configurações seguras.
- **Segmentação e Autenticação Mútua (mTLS):** Para controlar o tráfego e prevenir movimento lateral.
- **Proteção da Cadeia de Suprimentos:** Análise de composição de software (SCA) e assinatura de artefatos.

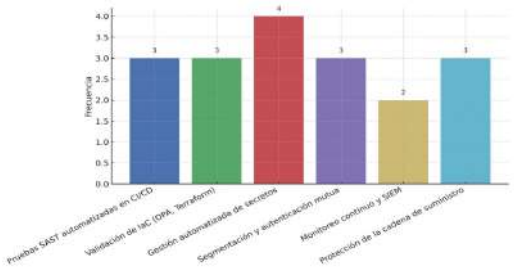

Figura: Frequência das Estratégias de Mitigação Documentadas.

Discussão e Conclusão

- **Impacto no Desempenho:** A maioria dos estudos concorda que estratégias de mitigação automatizadas, quando bem implementadas, **não degradam o desempenho**. Pelo contrário, fortalecem a estabilidade e a resiliência.
- **Foco da Literatura:** Há uma grande concentração de estudos em identificar ameaças e vetores, mas menos em validar empiricamente as soluções propostas.
- **Principal Lacuna Identificada:** Falta de validação empírica rigorosa e métricas comparativas de eficácia para as estratégias de mitigação em ambientes de produção reais.
- **Impacto na Tríade de Segurança (CIA):** A análise mostra que a **Integridade** (31%) é o pilar mais afetado, seguido pela **Rastreabilidade** (21%) e **Confidencialidade** (20%).

Síntese

Esta revisão sistemática mapeou com sucesso o ecossistema de cibersegurança em DevOps, identificando as principais ameaças, vetores de ataque e vulnerabilidades. Foram documentadas mais de 30 estratégias de mitigação.

Principal Conclusão

A automação e a integração da segurança (DevSecOps) são cruciais. Estratégias bem alinhadas ao ciclo DevOps fortalecem a segurança sem sacrificar a agilidade. No entanto, a falta de validação empírica na literatura é uma limitação crítica que precisa ser abordada.

Trabalhos Futuros

- **Extensão para a Internet das Coisas (IoT):** Aplicar os princípios de DevSecOps em ambientes IoT, que possuem desafios únicos:
  - Heterogeneidade de dispositivos.
  - Conectividade intermitente e recursos limitados.
  - Necessidade de atualizações remotas seguras (FOTA).
- **Frameworks de Avaliação Comparativa:** Desenvolver frameworks para avaliar empiricamente e comparar a eficácia de diferentes estratégias de DevSecOps em contextos híbridos (Cloud-Edge-IoT).
- **DevSecOps para Tecnologia Operacional (OT):** Adaptar as práticas para ambientes de automação industrial, onde a continuidade operacional e a segurança física são primordiais.

Obrigado!