
# Proposta de Implementação do S-SDLC e Pipeline DevSecOps

Engenharia de Segurança de Aplicações

# Contexto e Desafio

## Cenário Atual de Ameaças

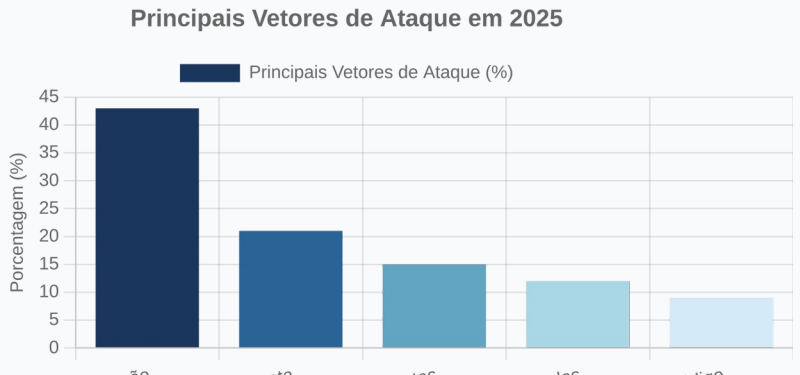
Aumento exponencial de ataques cibernéticos e vulnerabilidades em aplicações, com custos médios de violações de dados ultrapassando R$ 5 milhões por incidente.

## Segurança como Requisito

Necessidade de integrar segurança desde a concepção do software, não como um componente adicional ou verificação final.

## Transformação Digital

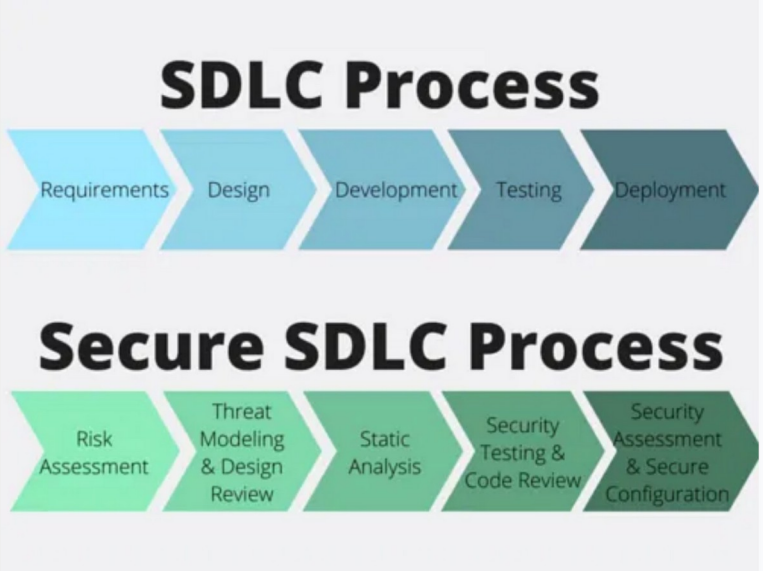
Pressão por entregas mais rápidas e frequentes sem comprometer a segurança, exigindo automação e integração contínua.

# As 7 Fases do S-SDLC

O S-SDLC integra segurança em cada etapa do desenvolvimento, transformando-a de um gargalo para um acelerador de inovação.

1. **Planning (Planejamento)**
   Definição de requisitos de segurança e avaliação de riscos.
2. **Analysis (Análise)**
   Análise de ameaças e modelagem de segurança.
3. **Design (Projeto)**
   Criação de arquiteturas seguras e padrões de codificação.
4. **Implementation (Implementação)**
   Desenvolvimento de código seguindo práticas de segurança.
5. **Testing (Testes)**
   Testes de segurança (SAST, DAST, SCA) e revisão de código.
6. **Deployment (Implantação)**
   Implantação segura com configurações protegidas.
7. **Maintenance (Manutenção)**
   Monitoramento contínuo e gestão de vulnerabilidades.




## Princípios Fundamentais

- Segurança intrínseca
- Processo contínuo
- Defesa em profundidade
- Segurança balanceada

# Ferramentas e Tecnologias

## CI/CD

- GitHub Actions
- GitLab CI
- Jenkins

## Análise Estática (SAST)

- SonarQube
- Checkmarx
- Fortify

## Análise de Composição (SCA)

- Snyk
- Dependabot
- OWASP Dependency-Check

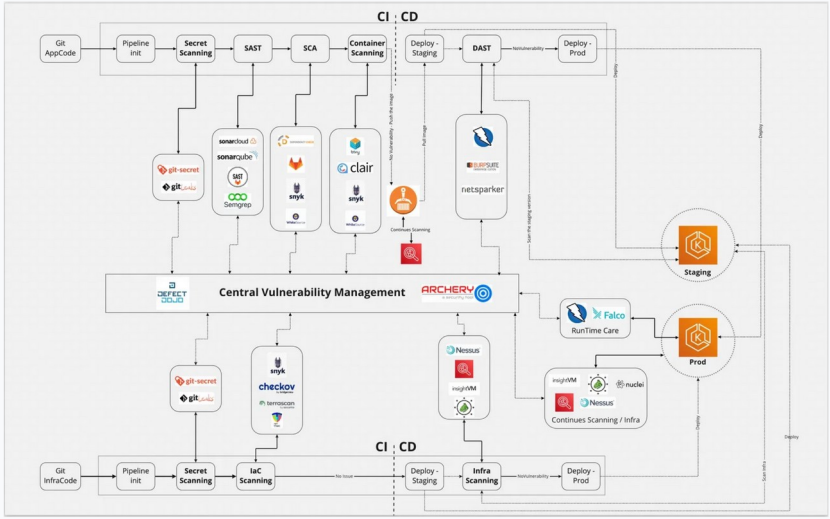
## Testes Dinâmicos (DAST)

- OWASP ZAP
- Burp Suite
- Acunetix

## IaC Security

- Terraform Sentinel

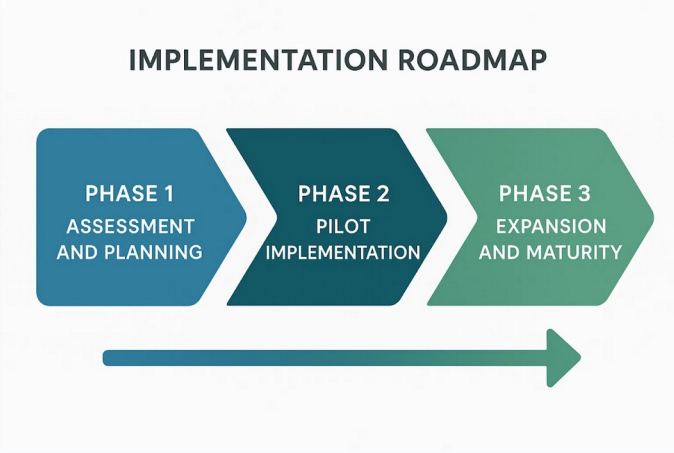
## Monitoramento e Gestão




## Critérios de Seleção de Ferramentas

- Integração com pipeline existente
- Capacidade de automação e APIs

# Roadmap de Implementação




## Fase 1

### Avaliação e Planejamento (1-2 meses)

- Avaliação da maturidade atual de segurança
- Definição de requisitos e políticas de segurança

## Fase 2

### Implementação Piloto (2-3 meses)

- Configuração do pipeline DevSecOps
- Integração de ferramentas de segurança
- Aplicação em projetos piloto

## Fase 3

### Expansão e Maturidade (3-6 meses)

- Expansão para todos os projetos
- Refinamento de métricas e KPIs
- Melhoria contínua dos processos
- Cultura de segurança consolidada