



# KPIs Usuais



A capability de Developer Autonomy & DevSecOps é fundamental para promover uma abordagem moderna e eficaz no desenvolvimento de software, enfatizando a integração da segurança desde o início do ciclo de desenvolvimento.

A fim de gerenciar e avaliar efetivamente essa capability, é essencial monitorar os Indicadores-Chave de Desempenho (KPIs) apropriados.

No contexto do CIO Codex Capability Framework, uma lista dos principais KPIs usuais para Developer Autonomy & DevSecOps:

- Taxa de Automação de Testes de Segurança (Security Test Automation Rate): Mede a proporção de testes de segurança automatizados em relação ao total de testes de segurança realizados.
- Tempo Médio para Integração de Segurança (Average Security Integration Time): Calcula o tempo médio necessário para integrar considerações de segurança no ciclo de desenvolvimento.
- Quantidade de Vulnerabilidades Identificadas (Vulnerabilities Identified Count): Contabiliza o número de vulnerabilidades de segurança identificadas durante o desenvolvimento.
- Tempo Médio para Correção de Vulnerabilidades (Average Vulnerability Resolution Time): Avalia o tempo médio necessário para corrigir vulnerabilidades de segurança após a identificação.
- Taxa de Adesão às Práticas DevSecOps (DevSecOps Practices Adoption Rate): Mede a adoção das práticas DevSecOps pelas equipes de desenvolvimento.
- Quantidade de Treinamentos de Segurança Realizados (Security Training Count): Contabiliza o número de programas de treinamento de segurança realizados para desenvolvedores.
- Taxa de Falhas de Segurança em Produção (Security Failures in Production Rate): Reflete a proporção de falhas de segurança que ocorrem em ambiente de produção após o lançamento.
- Nível de Colaboração entre Equipes (Team Collaboration Level): Avalia o grau de colaboração entre as equipes de desenvolvimento, operações e segurança.
- Taxa de Conformidade com Padrões de Segurança (Security Standards Compliance Rate): Mede o grau de conformidade com os padrões de segurança estabelecidos.
- Quantidade de Código Revisado por Pares (Code Reviewed by Peers Count): Contabiliza a quantidade de código revisado por outros desenvolvedores em busca de vulnerabilidades.
- Eficiência do Processo de Correção (Correction Process Efficiency): Avalia a eficiência do processo de correção de vulnerabilidades de segurança.
- Taxa de Retorno de Investimento em Segurança (Security Return on Investment Rate): Mede o retorno sobre o investimento em medidas de segurança.
- Quantidade de Vulnerabilidades Corrigidas Antes do Lançamento (Pre-Launch

Vulnerabilities Fixed Count): Contabiliza o número de vulnerabilidades corrigidas antes do lançamento de uma versão.

· Nível de Satisfação dos Desenvolvedores com as Ferramentas de Segurança (Developer Satisfaction with Security Tools Level): Avalia a satisfação dos desenvolvedores com as ferramentas de segurança disponibilizadas.

· Tempo Médio para Implantação Contínua (Average Continuous Deployment Time): Calcula o tempo médio necessário para implantar atualizações de software de forma contínua.

;

Esses KPIs desempenham um papel crucial na gestão da capability de Developer Autonomy & DevSecOps, assegurando que a integração de segurança seja realizada de maneira eficiente e eficaz desde o início do ciclo de desenvolvimento.

O monitoramento regular desses indicadores é essencial para o sucesso na entrega de software seguro e eficiente.

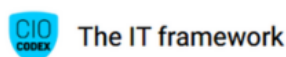
;

;



### **CIO Codex**

Com o advento da era digital, a Tecnologia da Informação assumiu um papel de destaque dentro das estratégias corporativas das empresas dos mais diversos portes e setores de atuação. O CIO Codex Framework foi concebido com o propósito de oferecer uma visão integrada dos conceitos de uma área de tecnologia pronta para a era digital.



O conteúdo apresentado neste website, incluindo o framework, é protegido por direitos autorais e é de propriedade exclusiva do CIO Codex. Isso inclui, mas não se limita a, textos, gráficos, marcas, logotipos, imagens, vídeos e demais materiais disponíveis no site. Qualquer reprodução, distribuição, ou utilização não autorizada desse conteúdo é estritamente proibida e sujeita às penalidades previstas na legislação aplicável