Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

TRIBUNAL REGIONAL DO TRABALHO DA 10ª REGIÃO

CARGO 11: ANALISTA JUDICIÁRIO
ÁREA: APOIO ESPECIALIZADO
ESPECIALIDADE: TECNOLOGIA DA INFORMAÇÃO

Prova Discursiva

Aplicação: 16/03/2025

PADRÃO DE RESPOSTA DEFINITIVO

No desenvolvimento de aplicações modernas, a estratégia DevSecOps permite: (i) integrar as práticas de segurança ao longo de todo ciclo de vida de desenvolvimento de um *software*; (ii) estabelecer uma cultura na qual a segurança seja responsabilidade de todos os envolvidos no projeto; (iii) garantir que as práticas de segurança sejam aplicadas em cada estágio do desenvolvimento; (iv) identificar e corrigir vulnerabilidades e problemas de segurança rapidamente; ~~e~~ (v) promover a colaboração entre equipes de governança, *design*, verificação, desenvolvimento, operações e segurança; (vi) integrar medidas de segurança desde o início do processo de desenvolvimento, identificando e abordando vulnerabilidades precocemente; (vii) adotar "Left Shift" em DevSecOps, integrando a segurança desde as primeiras fases do desenvolvimento, a fim de evitar vulnerabilidades tardias e aumentar a eficiência; (viii) implementar testes automatizados estáticos e dinâmicos ao longo do ciclo de vida do desenvolvimento do *software* como pressuposto base do DevSecOps; e (ix) utilizar ferramentas de versionamento de código para manter a transparência e a colaboração entre as equipes. Com essa estratégia, a segurança não representa mero elemento adicional, mas é parte integrante desde o desenvolvimento até a entrega e manutenção do *software*.

No contexto do DevSecOps, o modelo OWASP SAMM (Software Assurance Maturity Model) ~~permite que as instituições:~~ tem como objetivos principais: (i) ~~avaliem e melhorem~~ avaliar e melhorar, de forma contínua, suas práticas de segurança de *software*; (ii) ~~obtenham~~ obter uma visão clara do estado atual da segurança dentro da organização; (iii) ~~analisem e mapeiem~~ analisar e mapear práticas existentes em segurança; (iv) ~~realizem~~ realizar comparações com as melhores práticas do setor; (v) ~~introduzam~~ introduzir melhorias de forma organizada, a fim de definir metas de segurança, medir o avanço ao longo do tempo e identificar áreas de melhoria, em perfeito alinhamento com os princípios de integração contínua e entrega contínua (CI/CD); (vi) realizar integração com testes de segurança DAST e SAST; (vii) gerir riscos, avaliando ameaças, desenvolvendo perfis de risco e modelando ameaças para mitigar adversidades, promovendo um ambiente seguro; (viii) implementar métricas eficazes para identificar, monitorar e responder rapidamente a ameaças à segurança, protegendo ativos digitais; (ix) definir ambientes de desenvolvimento, testes e produção bem estruturados e separados, evitando falhas de segurança; e (x) fortalecer os mecanismos de implementação, assegurando a aplicação das melhores práticas de segurança durante o desenvolvimento.

No DevSecOps, a integração e a entrega contínuas permitem: (i) melhoria na qualidade do *software*, ao se ~~identificarem e corrigirem~~ identificar e corrigir problemas de segurança e *bugs* de forma rápida e contínua; (ii) redução do tempo de lançamento desde a codificação inicial, passando por testes automatizados, *deploys*, até a implementação e o monitoramento em produção; (iii) otimização da produtividade do fluxo de trabalho, limitando-se a quantidade em andamento; (iv) comunicação constante e eficiente entre as equipes; ~~e~~ (v) redução de riscos de vulnerabilidades; (vi) garantia da manutenibilidade do código; (vii) realização da automação de incrementos de código como parte do *pipeline* de CI/CD, reduzindo erros manuais e aumentando a confiabilidade do processo; (viii) redução dos processos manuais em ambientes críticos; (ix) correções de segurança e melhorias sempre presentes na versão em produção, reduzindo a exposição a vulnerabilidades conhecidas; e (x) realizar automação de testes nas etapas de "code" e "build" para correção de erros e falhas. Assim sendo, no âmbito da integração continuada, qualquer vulnerabilidade ou problema de segurança pode ser identificado e corrigido rapidamente.

Com uma atuação colaborativa, as equipes de desenvolvimento, operações e segurança podem garantir que as aplicações sejam mais bem desenvolvidas, o que gera benefícios, como: (i) redução dos riscos de vulnerabilidades; (ii) melhoria geral da eficiência do processo de desenvolvimento; (iii) comunicação e alinhamento em torno das metas de segurança; (iv) trabalho conjunto das equipes; ~~e~~ (v) garantia de desenvolvimento das aplicações com foco na segurança; (vi) promoção da educação e orientação sobre práticas de segurança; (vii) diminuição de custos e a melhora da economicidade; (viii) aumento da capacitação, ou especialização, que permite um melhor desenvolvimento de boas práticas, incluindo a de segurança; (ix) mudança na cultura organizacional, promovendo o engajamento e a responsabilidade das equipes durante o processo; (x) adoção de controle de acesso baseado em funções (RBAC); (xi) fornecimento de diferentes visões sobre um mesmo *software* ou produto; (xii) abordagem holística sobre segurança em toda a organização; (xiii) maior valor agregado ao produto final ao integrar práticas de segurança desde as fases iniciais do desenvolvimento; (xiv) agilidade na resolução de problemas, permitindo a mitigação rápida de vulnerabilidades por meio de comunicação fluida entre equipes; e (xv) aprendizado compartilhado como benefício da colaboração promovida pelo SAMM.

QUESITOS AVALIADOS

QUESITO 2.1 Pressupostos fundamentais do DevSecOps
Conceito 0 – Não abordou nenhum pressuposto do DevSecOps.
Conceito 1 – Abordou, corretamente, somente um pressuposto fundamental do DevSecOps.
Conceito 2 – Abordou, corretamente, dois pressupostos fundamentais do DevSecOps.

QUESITO 2.2 Objetivos do OWASP SAMM no contexto do DevSecOps
Conceito 0 – Não abordou nenhum objetivo do OWASP SAMM no contexto do DevSecOps.
Conceito 1 – Abordou, corretamente, somente um objetivo do OWASP SAMM no contexto do DevSecOps.
Conceito 2 – Abordou, corretamente, dois objetivos do OWASP SAMM no contexto do DevSecOps.

QUESITO 2.3 Benefícios da integração contínua e entrega contínua no DevSecOps
Conceito 0 – Não abordou nenhum benefício da integração contínua e entrega contínua no DevSecOps.
Conceito 1 – Abordou, corretamente, somente um benefício da integração contínua e entrega contínua no DevSecOps.
Conceito 2 – Abordou, corretamente, dois benefícios da integração contínua e entrega contínua no DevSecOps.

QUESITO 2.4 Benefícios da colaboração entre diferentes equipes promovida pelo SAMM
Conceito 0 – Não abordou nenhum benefício da colaboração entre diferentes equipes promovida pelo SAMM.
Conceito 1 – Abordou, corretamente, somente um benefício da colaboração entre diferentes equipes promovida pelo SAMM.
Conceito 2 – Abordou, corretamente, dois benefícios da colaboração entre diferentes equipes promovida pelo SAMM.