Saiba Mais

Itaú

DevSecOps

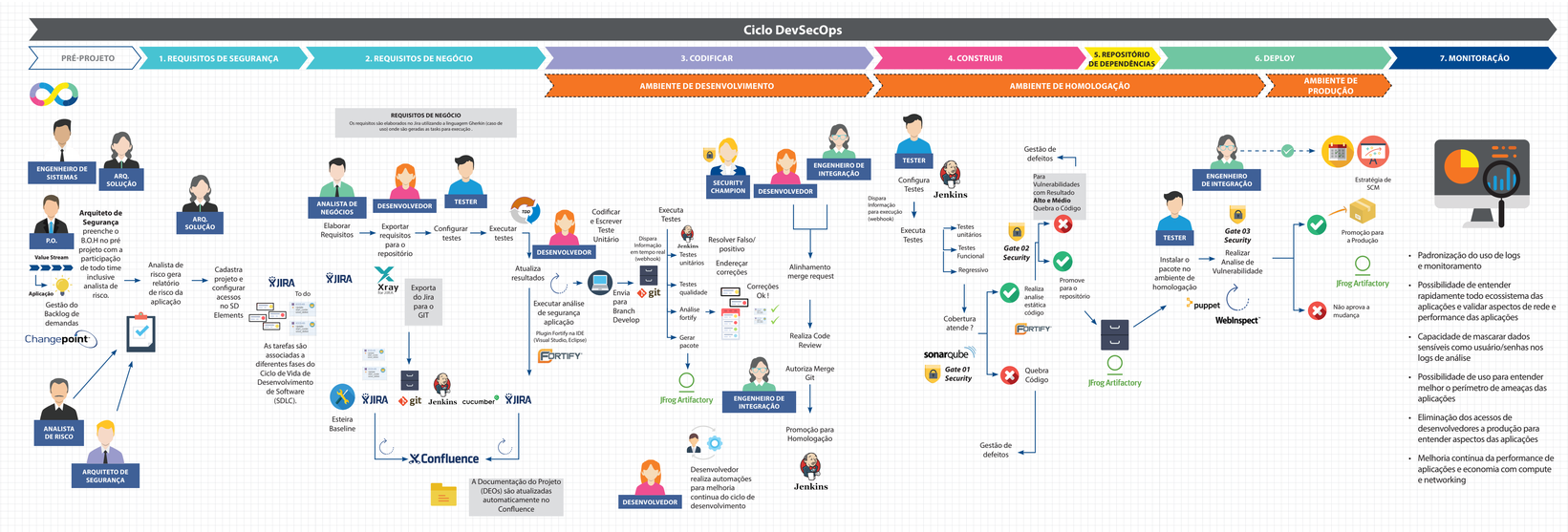
MAIO/2017

Estamos alinhados com a **Cloud Security Alliance** e **NIST (National Institute of Standards and Technology)**

Referência Interna

https://confluence.ctsp.prod.cloud.ihf/display/CLOUD/Welcome+Kit

moover
www.mooverconsulting.com.br



Juntos construiremos um banco ainda mais digital.

Tecnologia é vital e cada vez mais continuará sendo um dos diferenciais competitivos do banco.

Muitos esforços e investimentos tem sido realizados, gerando grandes mudanças no nosso ambiente técnico, na forma como trabalhamos e nos relacionamos.

O engajamento de todos é fundamental para viabilizar essa transformação.

Guia Itaú

Sec Dev Ops

Série Itaú Aprendendo

+ Agilidade, eficiência, colaboração, time-to-market

- Padronização do uso de logs e monitoramento
- Possibilidade de entender rapidamente todo ecossistema das aplicações e validar aspectos de rede e performance das aplicações
- Capacidade de mascarar dados sensíveis como usuário/senhas nos logs de análise
- Possibilidade de uso para entender melhor o perímetro de ameaças das aplicações
- Eliminação dos acessos de desenvolvedores a produção para entender aspectos das aplicações
- Melhoria continua da performance de aplicações e economia com compute e networking

Aprenda:

- O que isso significa
- Como é o novo ciclo de entrega
- Quais ferramentas estamos disponibilizando
- O que é importante saber
- Onde buscar informações complementares

MOOVEN

Itaú DevSecOps

O que é?

Termo criado para descrever um conjunto de práticas para integração entre os times de Desenvolvimento de Software, Operações e Segurança e a adoção de processos automatizados para produção rápida e segura de aplicações e serviços.

Pilares:

Ideação e Planejamento Contínuo: Capacidade de promover a relevância nas decisões de portfólio de Software alinhadas às necessidades de negócio, com foco na identificação, priorização, planejamento e rastreabilidade contínua do backlog de entrega.

Integração Contínua: Capacidade de disponibilização, integração frequente (merging) de código em repositório compartilhado, ter frequentemente uma versão confiável de software pronta para ser entregue em produção (build + test).

Teste contínuo: Capacidade de aferir de forma frequente, integral e automatizada a qualidade de uma versão disponível de produto de software.

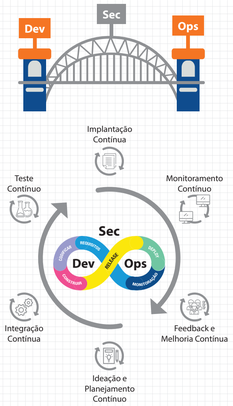
Implantação Contínua: Capacidade de liberar frequentemente as versões prontas de produto de software nos ambientes

Monitoramento Contínuo: Capacidade de padronizar e organizar os logs e recursos gerenciados, monitorar e tomar ações rápidas e antecipadas de forma frequente, que garantam o máximo a disponibilidade do ambiente e aplicações.

Feedback e Melhoria Contínua: Capacidade de identificar e tratar de forma frequente os feedbacks e necessidades das equipes envolvidas em todas as fases do ciclo de vida do software ou serviço.

É isso que estamos entregando agora.

Criamos a nossa esteira DevSecOps e progressivamente iremos migrar as siglas e incrementar o ambiente com novas práticas, recursos e ferramentas.



Por que DevSecOps é importante para nós?

Agilidade: acelera a nossa capacidade e frequência de entrega de software.

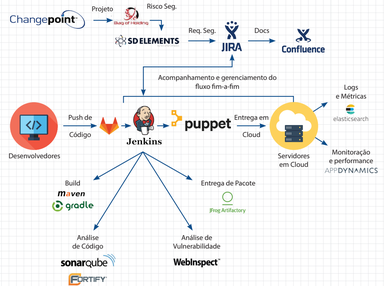
Qualidade: permite entregarmos melhores softwares em produção e reduzir o esforço de sustentação.

Colaboração: promove a orquestração e integração entre os diversos atores.

Eficiência: reduz desperdícios e o esforço na execução das atividades através da automatização.

Segurança: promove e garante a aplicação das nossas políticas de segurança.

Landscape de ferramentas:



- **Gitlab:** Controle de versão de fonte
- **Maven/Gradle:** Ferramentas de build
- **Fortify:** Análise estática de segurança
- **SonarQube:** Teste de cobertura e qualidade de código
- **Jenkins:** Orquestra o fluxo de continuous integration e continuous delivery
- **Jfrog ArtFactory:** Controle de versão de binário e dependências
- **Puppet:** Gerenciador de configuração de máquina (garante as versões de SW que estão no ambiente)
- **Jira:** Planejamento e gestão do backlog, acompanhamento de entregas
- **Confluence:** Repositório de documentação
- **SD Elements:** Gestão de requisitos de segurança de SW
- **Changepoint:** Gestão do portfólio de projetos
- **Bag of Holding:** Organização e priorização de atividades de segurança de software, gestão e classificação de risco da aplicação
- **WebInspect:** ferramenta de análise dinâmica de segurança
- **AppDynamics:** ferramenta para melhoria de performance das aplicações
- **ElasticSearch:** ferramenta para indexação de logs da aplicação

DevSecOps + Cloud

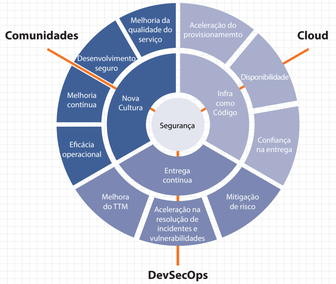
Como as coisas se complementam?

DevSecOps e Cloud são ambos catalizadores entre si. A flexibilidade, resiliência, agilidade e serviços proporcionada é intensificada quando a esteira DevSecOps está hospedada na Cloud.

Ambientes de desenvolvimento, teste até a produção podem ser provisionados e configurados quando e conforme necessários.

Este processo minimiza gargalos típicos no ciclo de entrega, acelerando e reduzindo custos, além de oferecer o que há de mais avançado em termos de experiência para os times.

É esse estágio que queremos e vamos atingir.



- Entregas mais frequentes
- Antecipação do valor ao cliente
- Infraestrutura mais flexível e resiliente
- Sistemas mais robutos e seguros

Papéis

Qual o meu papel nesse novo ambiente?

ENGENHEIRO DE INTEGRAÇÃO

Responsável pelo gerenciamento da Release e estratégia de gestão de versionamento e código fonte.

SECURITY CHAMPION

Responsável por avaliar critérios das ferramentas de segurança e garantir mitigação de vulnerabilidades.

DESENVOLVEDOR

Responsável por aplicar no desenvolvimento as definições de segurança, qualidade, boas práticas de engenharia de Software e automação do processo.

TESTER

Responsável por configurar o plano de testes, garantir a validação necessária do código desenvolvido e identificar defeitos.

ENGENHEIRO DE SISTEMAS

Responsável pela definição da solução e aderência do código aos padrões estabelecidos no Itaú.

ANALISTA DE RISCO

Responsável por orientar o desenvolvedor no preenchimento do B.O.H e endereçar novas aplicações para engenharia de segurança.

ANALISTA DE SUPORTE

Responsável pelas configurações das ferramentas para as novas aplicações.

ARQUITETO DE SEGURANÇA

Verificar o estado atual das arquiteturas de sistema e projetá-las de forma segura, seguindo as recomendações e boas práticas do mercado. Preencher o B.O.H e SD. Elements.

12 factors

O que é?

É um conjunto de práticas para construir Softwares-como-Serviço (SaaS). Pode ser aplicada para o desenvolvimento de aplicações em qualquer linguagem de programação e com qualquer combinação de serviços de suporte (banco de dados, filas, cache de memória, etc).

Classificação Itaú para os 12 factors

Obrigatórias

- **Base de código**
- **Dependências**
- **Configurações**
- **Build, release, run**
- **Dev/prod semelhantes**
- **Logs**

Importantes

- **Processos**
- **Concorrência**
- **Descartabilidade**

Desejáveis

- **Serviços de apoio**
- **Vínculo de porta**
- **Processos de Admin**

OWASP Top 10

O que é?

O OWASP Top 10 é uma lista de vulnerabilidades mais críticas encontradas em projetos de aplicações web. A lista mais recente é de 2017 e deve ser conhecida e considerada por todos os engenheiros e desenvolvedores que trabalham com aplicações. São elas:

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Broken Access Control
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Insufficient Attack Protection
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Underprotected APIs