THE DEVELOPER'S CONFERENCE

# Trilha – DevOps

**Alessandra Monteiro Martins**

Especialista em Governança de TI pela Universidade Católica de Brasília,
Licenciada em Informática pela Universidade do Estado do Amazonas,
Certificações ITIL, COBIT, ISO27002,CTFL, KMPI, Scrum Master, CLF

THE DEVELOPER'S CONFERENCE

# Uma Jornada DevSecOps Desafios e Recompensas

Femme it
O JEITO FEMININO DE FALAR DE TI

THE DEVELOPER'S CONFERENCE

Cyber Security Girls

# Head GPS | DPO  D1
# Alessandra Monteiro Martins

**Formada em Licenciatura em Informática pela Universidade do Estado do Amazonas, Especialista em Governança de TI pela Universidade Católica de Brasília, Certificações ISO 27002, ITIL v3, COBIT5, Scrum Master, KMP I, CTFL, PDPFe outras.**

**Atuando no Mercado de Tecnologia da Informação desde 2004, trabalhando há mais de 5 anos, voltada para Qualidade de Software, Projetos, DevSecOPs, Segurança da Informação, Governança de TI, SI e Corporativa.**

# Agenda


- Conceitos: Engenharia de Software, Metodologias, DevSecOps, Ciclos de Vida , SI, Desenvolvimento Seguro
- Contexto:Security by Design
  - Papéis e Responsabilidades
    - Desafios
      - Recompensas
        - *Referências*

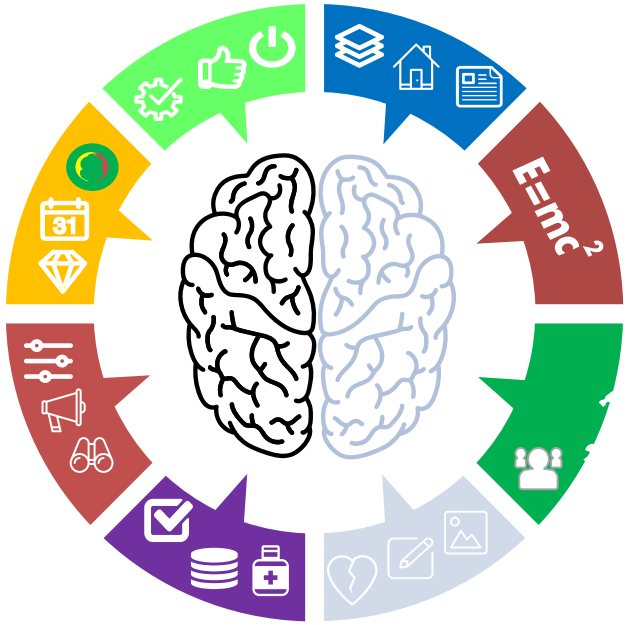
# Conceitos: Engenharia de Software

## Knowledge Area (KA) SWEBOK

THE DEVELOPER'S CONFERENCE

### Áreas de Conhecimento da Engenharia de Software

- REQUISITOS DE SOFTWARE
- DESIGN DE SOFTWARE
- CONSTRUÇÃO DE SOFTWARE
- TESTE DE SOFTWARE
- MANUTENÇÃO DE SOFTWARE
- MODELOS E MÉTODOS DE ENGENHARIA DE SOFTWARE
- QUALIDADE DE SOFTWARE

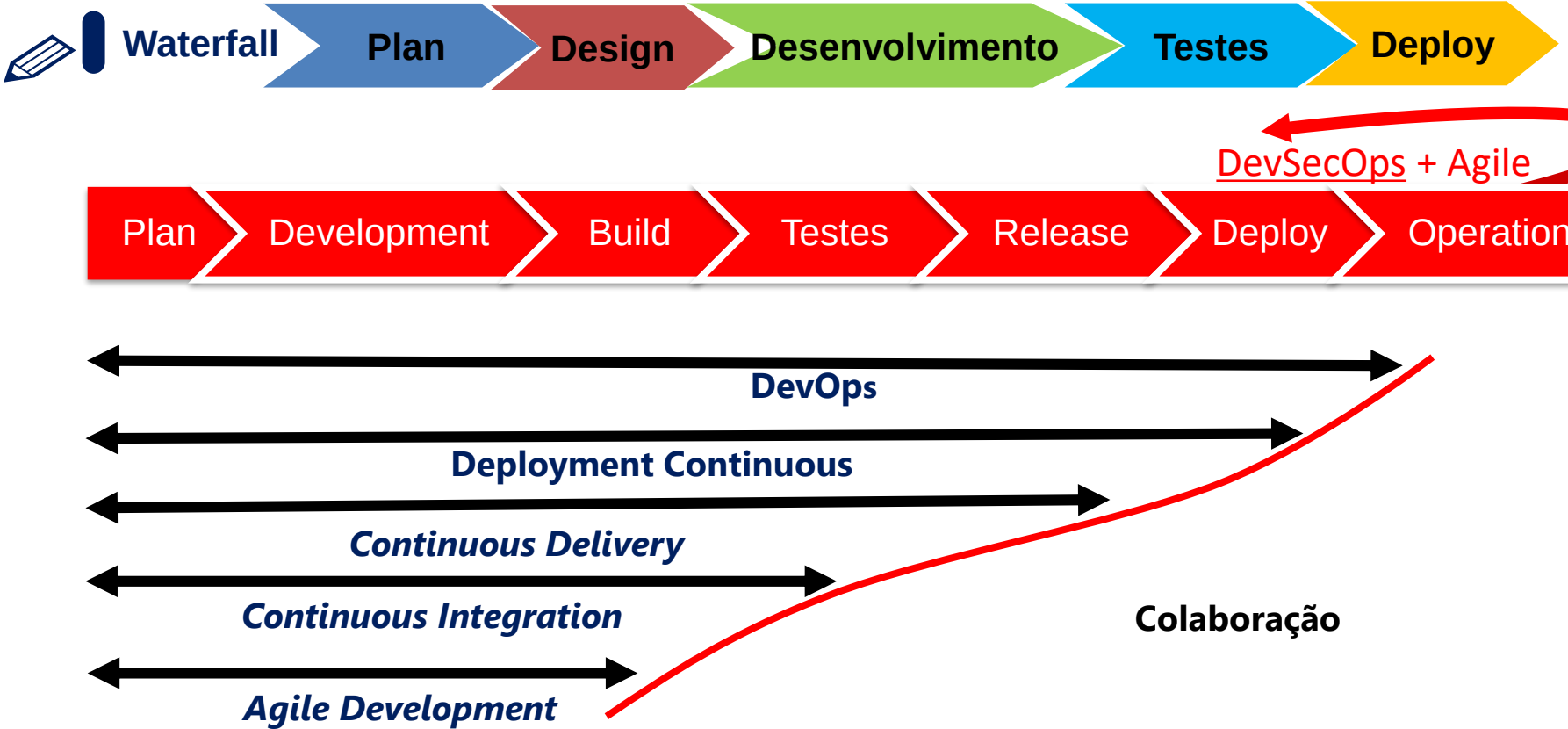



- ENGENHARIA DE SOFWARE ECONÔMICA

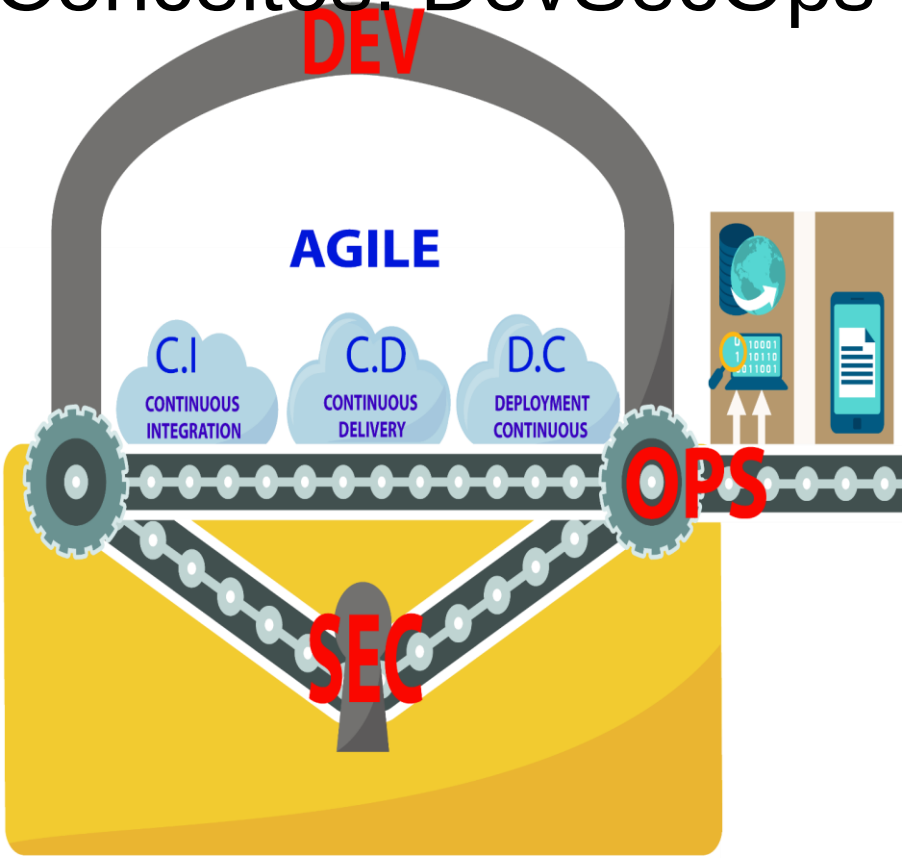
- GERENCIAMENTO DE CONFIGURAÇÃO DE SOFTWARE
- GERENCIAMENTO DE EENGENHARIA DE SOFTWARE
- PROCESSO DE ENGENHARIA DE SOFTWARE
- PRÁTICA PROFISSIONAL DE ENGENHARIA DE SOFTWARE
- FUNDAMENTOS DE COMPUTAÇÃO
- FUNDAMENTOS MATEMÁTICOS
- FUNDAMENTOS DE ENGENHARIA

# Conceitos: Metodologias

THE DEVELOPER'S CONFERENCE



# Conceitos: DevSecOps




THE DEVELOPER'S CONFERENCE

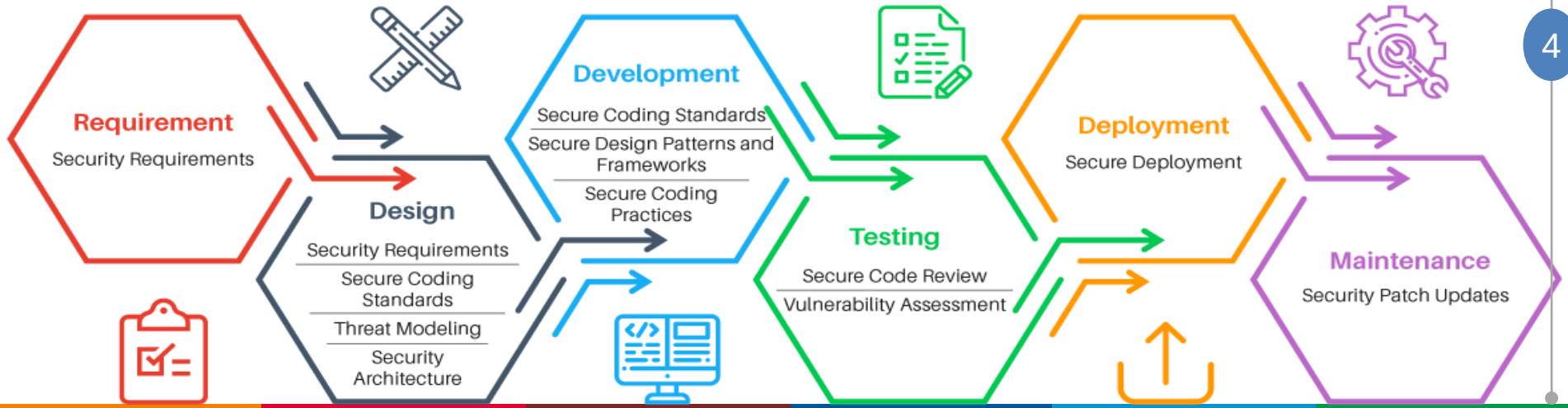
## O que é DevSecOps ?

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

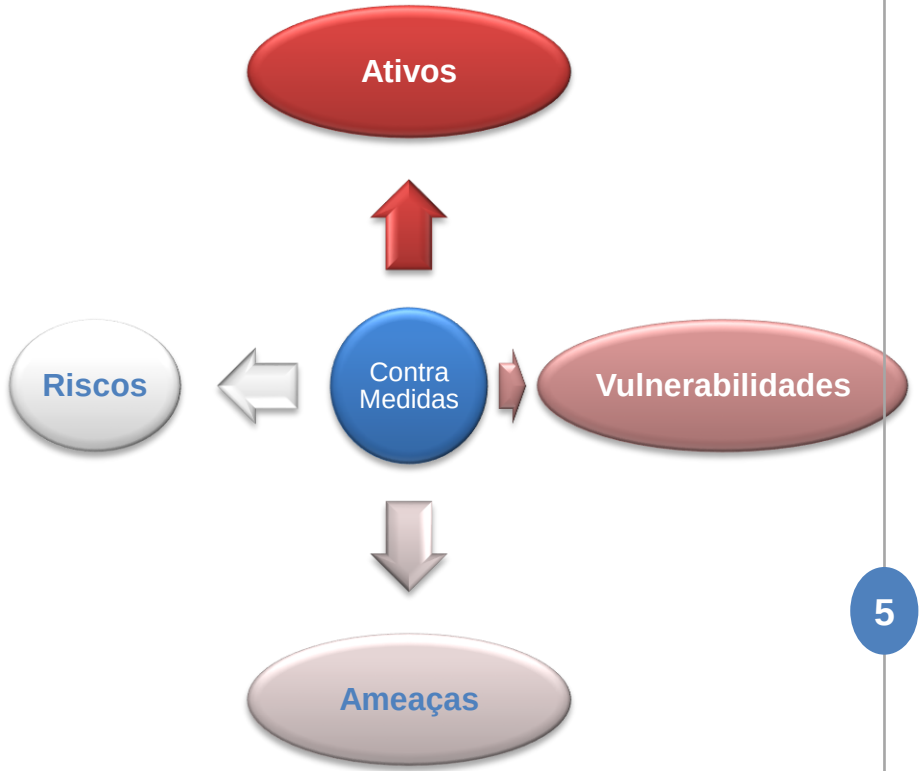
# Conceitos: Ciclos de Vida

THE DEVELOPER'S CONFERENCE

| | | | | | |
|---|---|---|---|---|---|
| SLDC | Requisitos | Desenho | Desenvolvimento | Testes | Implantação |
| Secure SDLC | Avaliação de Riscos | Modelagem de Ameaças e Revisão de Desenho | Análise Estática | Testes de Segurança e Revisão de Código | Configuração de Segurança e Avaliação de Segurança |



# Conceitos: Segurança da Informação

# Conceitos: Desenvolvimento Seguro

THE DEVELOPER'S CONFERENCE

| | | | | | | |
|---|---|---|---|---|---|---|
| Conceitos Core de Segurança | Reunindo Requisitos de Segurança | Princípios de Design de Segurança | Práticas de Codificação Segura | Técnicas e Ferramentas de Teste de Segurança | Plano de Revisão Final de Segurança | Gestão de Patch de Segurança |
| Metodologias de Garantia | Checklist de Construção e Definição de "Portões" de Segurança | Controles de Segurança em Nível de Design | Análise de Segurança do Código | Lidando com Defeitos de Segurança | Revisão de Segurança e Processos de Resposta | Lindando c Atualizaçã 3º Partes |
| Padrões e Frameworks | Baseline de Segurança do Produto | Modelagem de Ameaças | Revisão de Segurança de Código | Desenvolvimento de Métricas de Segurança | Gestão de Riscos da Cadeia de Suprimentos | Política d Eliminaçã |



Treinamento e Conscientização → Requisitos de Segurança do Negócio → Design da Segurança → Codificação Segura → Testes de Segurança → Revisão de Segurança e Resposta → Manutenção

# Contexto: Security By Design

THE DEVELOPER'S CONFERENCE

**1 - Minimizar a superfície de área de ataque**

Através da utilização de patterns de desenvolvimento de código e boas práticas de desenvolvimento seguro.

**2 - Estabelecimento de Padrões**

Através da utilização de senhas fortes, ciclo de vida de senhas, autenticação multifator e tokens.

**3 - Princípio do Menor Privilégio**

Através da criação de contas com a menor quantidade de privilégios necessários para executar seus processos de negócios. Isso engloba direitos de usuário, permissões de recursos, como limites de CPU, memória, rede e permissões do sistema de arquivos.

**4 – Princípio da Defesa em Profundidade**

Utilizando um controle que seria razoável, mais controles que abordam riscos de diferentes maneiras são melhores. Os controles, quando usados em profundidade, podem tornar vulnerabilidades extremamente difíceis de explorar e, portanto, improváveis de ocorrer.

**5 – Falhar com Segurança**

Os aplicativos geralmente não processam transações por vários motivos. A forma como eles falham podem determinar se um aplicativo é seguro ou não, por exemplo se expõe, endpoints, paths, strings de conexão etc.

# Contexto: Security By Design

THE DEVELOPER'S CONFERENCE

### 6 - Não Confie nos Serviços

Todos os sistemas externos com parceiros, integradores, brokers, devem ser tratados de maneira semelhante, os dados devem ser sempre verificados para garantir a segurança de exibição ou compartilhamento com o usuário final.

### 7 - Separação de deveres

Através da determinação de papéis que têm diferentes níveis de confiança do que usuários normais. Em particular, os administradores são diferentes dos usuários normais, utilizando RBAC para atribuição de permissionamento.

### 8 - Evitar a segurança por obscuridade

A segurança de um aplicativo não deve depender do conhecimento do código-fonte mantido em segredo. A segurança deve se basear em muitos outros fatores, incluindo políticas razoáveis de senha, defesa em profundidade, limites de transação de negócios, arquitetura de rede sólida e controles de fraude e auditoria.

### 9 - Mantenha a Segurança simples

Onde os desenvolvedores devem evitar o uso de negativos duplos e arquiteturas complexas quando uma abordagem mais simples seria mais rápida e simples.

### 10 - Correção de Problemas de Segurança da maneira correta

Quando um problema de segurança for identificado, é importante desenvolver um teste para ele e entender a causa raiz do problema. Quando padrões de design são usados, é provável que o problema de segurança seja difundido entre todas as bases de código, portanto é essencial desenvolver a correção correta sem introduzir regressões.

# Papéis e Responsabilidades

PSBD 2,6 ,7

THE DEVELOPER'S CONFERENCE

## Blue Team

Identificar

Gestão de Ativos

Gestão de Riscos

Controle de Danos

Resposta a Incidentes -SOC

MDM - DA

Segurança Defensiva

01

## Orange Team

Proteger

Conscientização e Treinamento

Segurança de Dados

Procedimentos de Proteção

Codificação Segura

QA

02

## Purple Team

Detectar

Identificar anomalias

Facilitar as Melhorias em defesa e detecção

Aprimorar as habilidades dos membros do time azul e vermelho – Heurísticas

ES, NOC

03

## Red Team

Responder

Segurança Ofensiva

Ethical Hacker

Pentest

Exploração de Vulnerabilidades

ANS

04

## Green Team

Recuperar

Melhorar a capacidade dos logs trabalhando com padrões e priorização de eventos importantes – AIOPS

Melhorar dados para forense digital e casos de resposta a incidentes

05

## Yellow Team

Construir

Arquitetos e Engenheiros de Software e Sistemas

Desenvolvedores de Aplicação

DBA , AN,

06

# Papéis e Responsabilidades

THE DEVELOPER'S CONFERENCE

1

**Analistas JR, PL, SR**

Negócios, Requisitos, Qualidade, Testes, Segurança, Infraestrutura, Desenvolvimento

2

**Arquiteto de Dados**

Deve se ocupar do projeto das bases de dados e sua estrutura lógica, não se envolvendo diretamente nos aspectos físicos

3

**Arquiteto de Software**

Deve se ocupar de quebrar a complexidade do desenvolvimento de aplicações e pedaços menores e melhores gerenciáveis.

4

**Arquiteto de Infraestrutura**

Deve se ocupar **infraestrutura**, , do "esqueleto" de sistemas e projetos de tecnologia que inclui o funcionamento de software e hardware de redes, servidores e bancos de dados

5

**Arquiteto de Soluções**

Define as soluções tecnológicas de acordo com os objetivos da empresa, sua responsabilidade é entender os problemas que o negócio pretende resolver e encaminhar

# Papéis e Responsabilidades

THE DEVELOPER'S CONFERENCE

6

## Arquiteto Corporativo

Deve se ocupar de alinhar pessoas, processos, metas, áreas de negócios, tecnologias e ferramentas,, pensando estrategicamente no uso atual e futuro.

7

## Arquiteto de Segurança

Deve se ocupar com as especificaçãoes de segurança para as arquiteturas de redes, infraestrutura, sistemas, desde o Projeto a implementação de forma segura

## DBA

Deve se ocupar da Administração e manutenção dos Bancos de Dados no dia a dia.

9

## UX

Especificações, prototipagem e Desenvolvimento do Design, layout, mapeando a jornada do usuario pelas interfaces e facilitando-a

10

## Engenheiro de Software

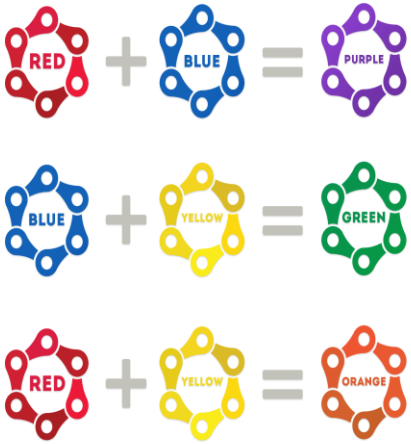
Deve se ocupar de transformar um conjunto de processos de negócio em software; modelar o domínio do negócio de modo que um software possa ser produzido

# Papéis e Responsabilidades

PSBD 2,6 ,7

THE DEVELOPER'S CONFERENCE

## Papéis:



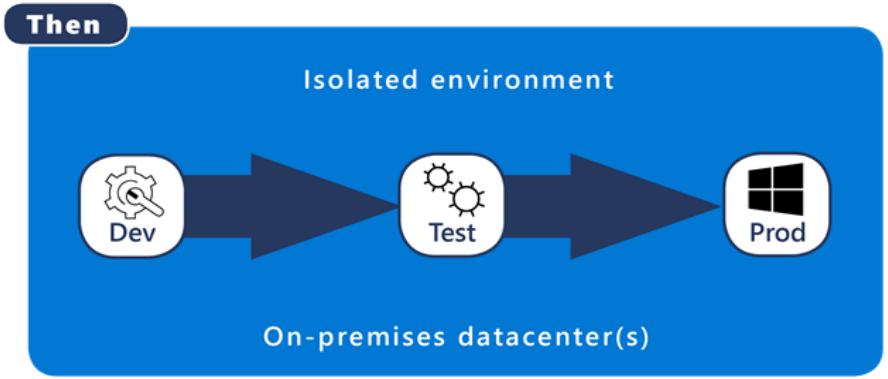

1. Process Master (Scrum Master)
2. Service Master (Product Owner)
3. DevOps Engineer
4. Gatekeeper – Release Coordinator
5. Reliability Engineer (opcional)
6. Time Desenvolvimento ( Dev, QA,DBA)
7. Time de Operação

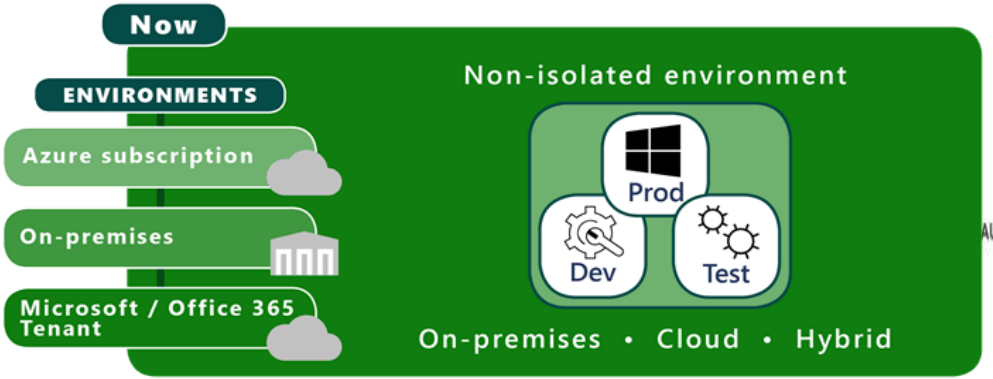
- Arquiteto de Soluções
- Arquiteto Corporativo
- Arquiteto de Infraestrutura
- Engenheiro de Software
- Engenheiro/ Arquiteto de Software
- Arquiteto de Dados, Analista de Negócios, Desenvolvedores, Analista de Testes, Designers, Analista de Segurança
- DBA, Analista de Segurança, Analista de Monitoramento, Analista de Infraestrutura e Suporte, Arquiteto / Enhgenheirode Segurança

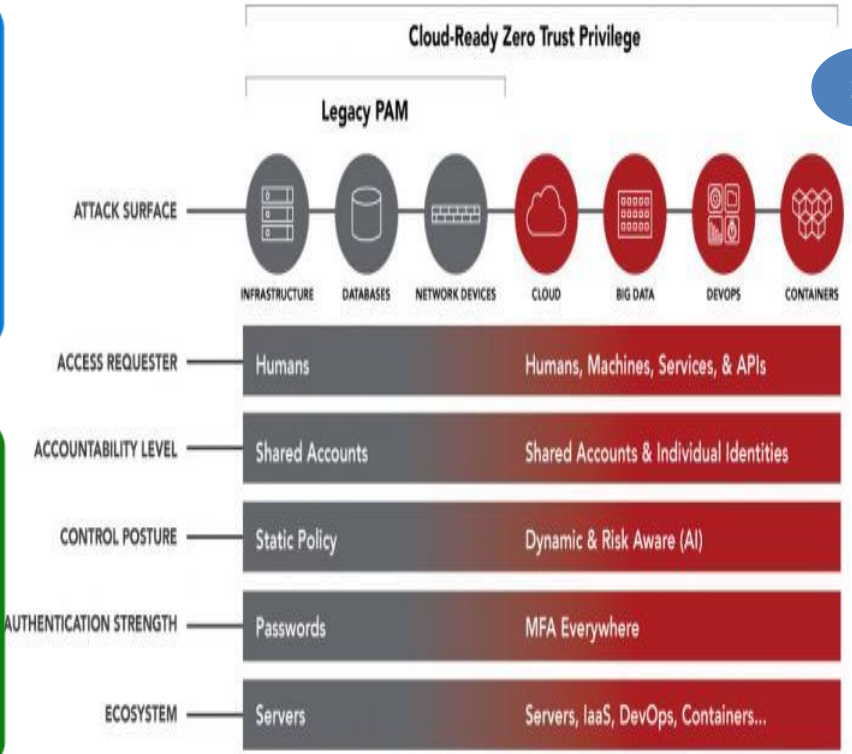
# Desafios:

THE DEVELOPER'S CONFERENCE





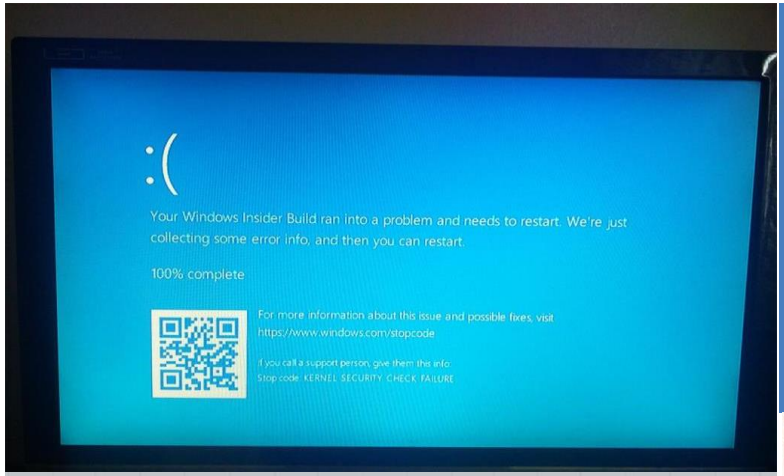



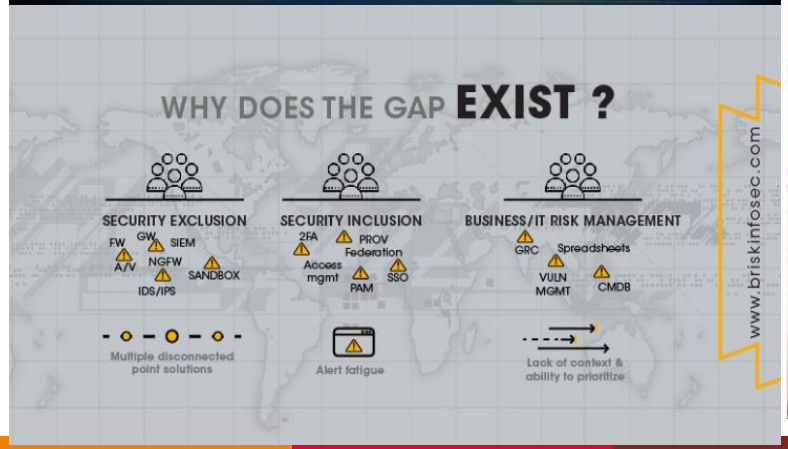



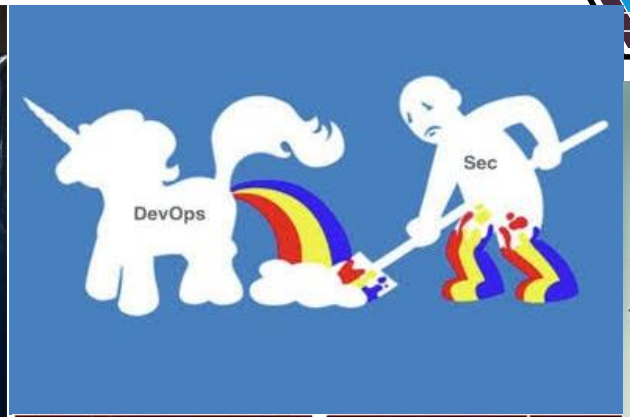
# Desafios:

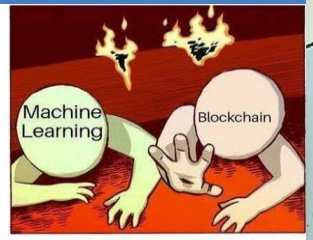
THE DEVELOPER'S CONFERENCE





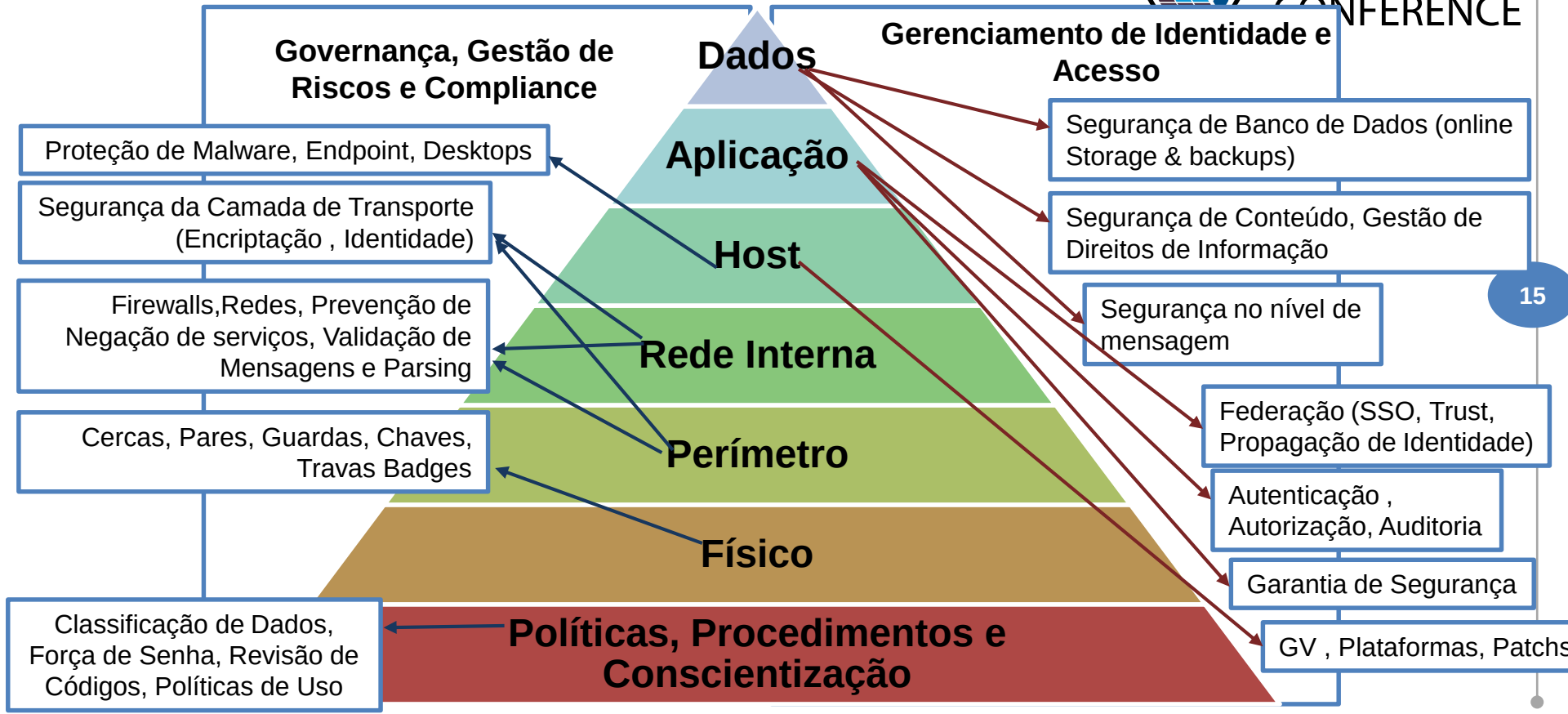



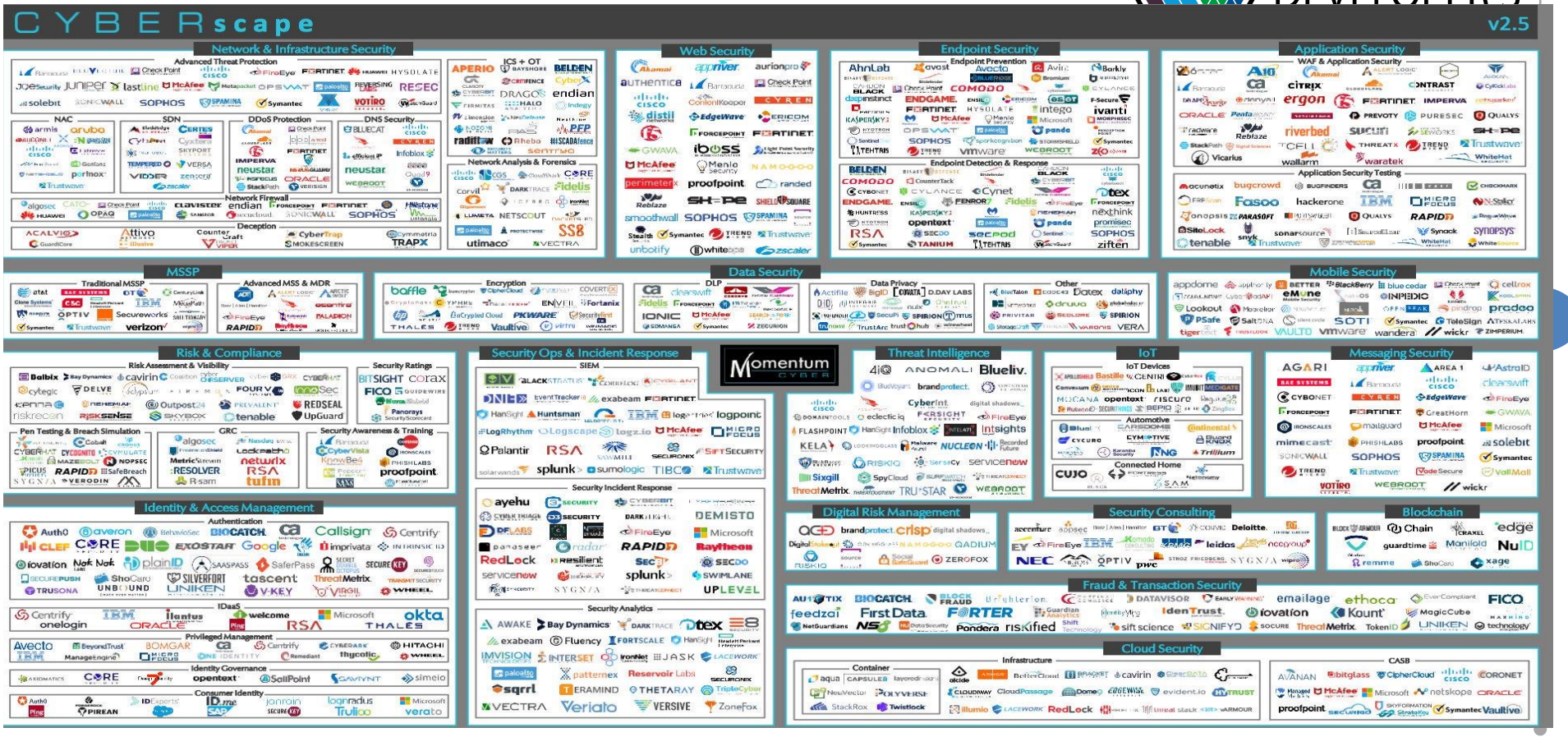


# Desafios:

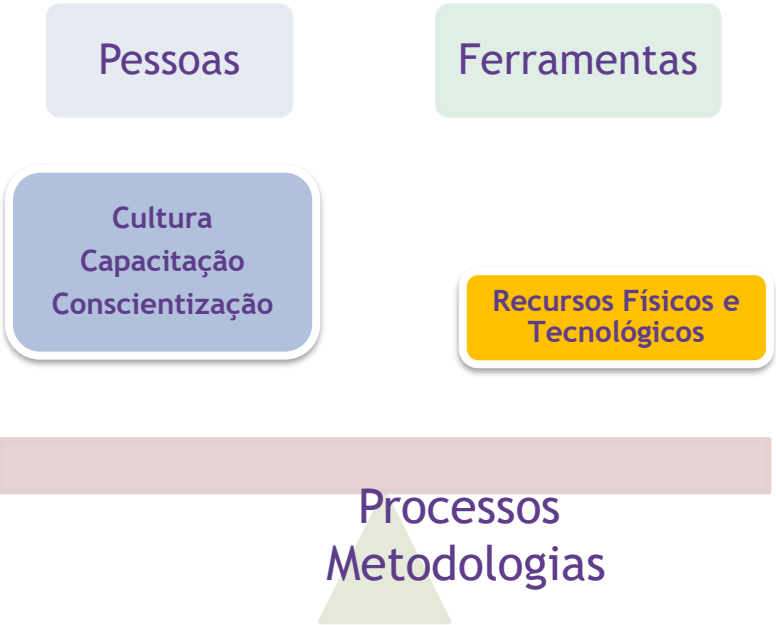

Governança, Gestão de Riscos e Compliance
Gerenciamento de Identidade e Acesso
Dados
Aplicação
Host
Rede Interna
Perímetro
Físico
Políticas, Procedimentos e Conscientização
Proteção de Malware, Endpoint, Desktops
Segurança da Camada de Transporte (Encriptação , Identidade)
Firewalls,Redes, Prevenção de Negação de serviços, Validação de Mensagens e Parsing
Cercas, Pares, Guardas, Chaves, Travas Badges
Classificação de Dados, Força de Senha, Revisão de Códigos, Políticas de Uso
Segurança de Banco de Dados (online Storage & backups)
Segurança de Conteúdo, Gestão de Direitos de Informação
Segurança no nível de mensagem
Federação (SSO, Trust, Propagação de Identidade)
Autenticação , Autorização, Auditoria
Garantia de Segurança
GV , Plataformas, Patchs

# Desafios:

THE DEVELOPER'S

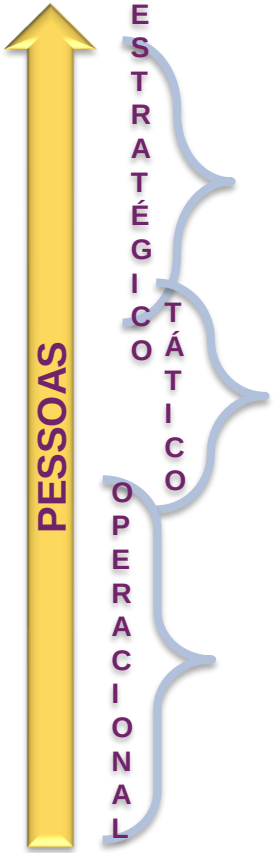


# Recompensas:




- Controle de defeitos documentados (Gestão de problemas e defeitos)
- Controle de Código da infraestrutura (SCM)
- Testes de aceitação automatizados (BDD)
- Geração de Massa de testes automatizada
- Fluxo de verificação automática de defeitos corrigidos
- Ambiente de testes apartado e versionado
- Servidor de Deployment (Gestão de dependências)
- Criação de ambientes versionados e de forma automática (conteinerização de ambientes produtivos) – Gestão de Configuração
- Processo automatizado de solicitações de Mudanças
- Criação de Logs
- Monitoração Contínua
- Supervisão da Implementação automatizada com ferramentas

# Recompensas:


THE DEVELOPER'S ERENCE

**Gestão**
- Pessoas
- Responsabilidades
- Educação e

**Engenharia de Requisitos**
- Funcionais
- Não Funcionais

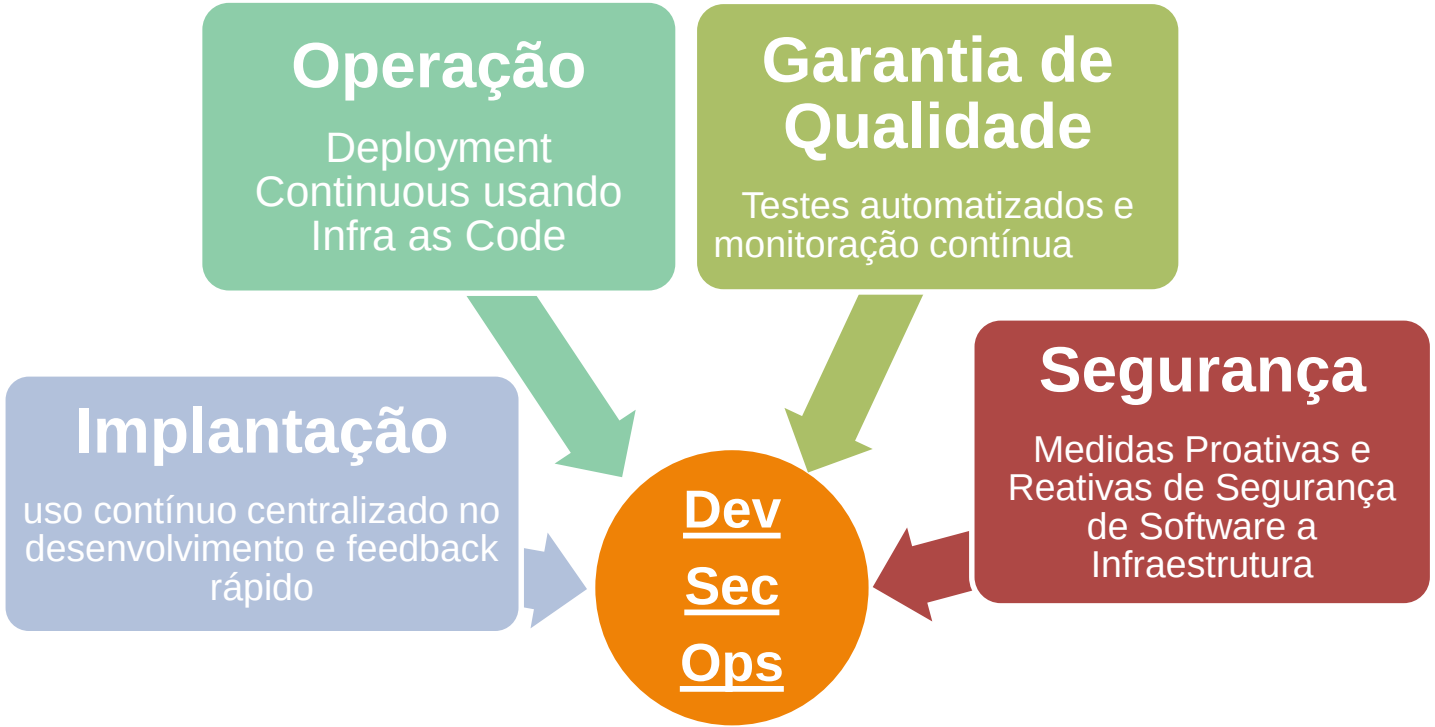
**Gestão Configuração**
- Mudanças
- Dados
- Infraestrutura

**Padronização de Processos:**
Qualidade | Testes
- Defeitos
- Liberação e Implantação

**Segurança**
- Gestão de Acesso e Identidade
- Monitoração e Auditoria

# Recompensas:

THE DEVELOPER'S CONFERENCE



# Referências:


- FILHO, Wilson de Pádua – “Engenharia de Software: Fundamentos Métodos e Padrões – LTC -3º Edição , 2009, Rio de Janeiro
- COSTA, I; NETO, M; COSTA NETO, P; JUNIOR, J. et al. Qualidade em Tecnologia da Informação. São Paulo: Editora Atlas, 2013.
- CORREIA, M. Segurança no Software. Lisboa: Editora, 2010.
- LYRA, M. et al. Segurança e Auditoria em Sistemas de Informação. Rio de Janeiro: Editora Ciência Moderna, 2008.
- MIGUEL, A. Gestão de Projectos de Software. Lisboa: Editora QFCA, 2010.RIOS, E;
- MOREIRA, T. et al. Teste de Software. Rio de Janeiro: Alta Books, 2013. C. 2010.
- SOLOMON, M.G; KIM, D.et at. Fundamentos de Segurança de Sistemas de Informação. Rio de Janeiro: Editora LTC, 2014.
- MORAIS, Gleicon - “CAIXA DE FERRAMENTAS DEVOPS – Casa do Código, 2017 São Paulo, SP.
- AGNER, Luiz. **Ergodesign e arquitetura de informação: trabalhando com o usuário**. Rio de Janeiro: Editora Quartet, 2º Edição, 20109
- Data Management Body of Knowledge (DAMA DMBoK®) – LLC Editora, 1º Edição,2012. Data & Information – DAMA Brasil, 1º Edição, 2015.
- Guidelines and Strategies for Secure Interaction Design – Capítulo 13, KA-PING YEE
- OWASP – Code Review versão 2.0
- http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- https://www.checkmarx.com/glossary/a-secure-sdlc-with-static-source-code-analysis-tools/
- https://www.hack2secure.com/images/Pdf/Hack2Secure_Secure_SDLC_Services.pdf
- https://www.eccouncil.org/programs/certified-application-security-engineer-case/
- https://www.us-cert.gov/bsi/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes
- https://br.pinterest.com/pin/797207571509409038/visual-search/?x=6&y=8&w=530&h=298
- https://twitter.com/dockercon/status/666188361
- https://slideplayer.com/slide/15950081/456091136
- https://mikecardus.com/leaders-responsibility/
- https://www.eenewsembedded.com/news/static-analysis-secure-software-development-lifecycle
- https://www.owasp.org/index.php/OWASP_Testing_Guide_Appendix_C:_Fuzz_Vectors
- https://www.owasp.org/images/1/19/OTGv4.pdf
- https://docs.zephyrproject.org/latest/security/security-overview.html
- Exin White Paper

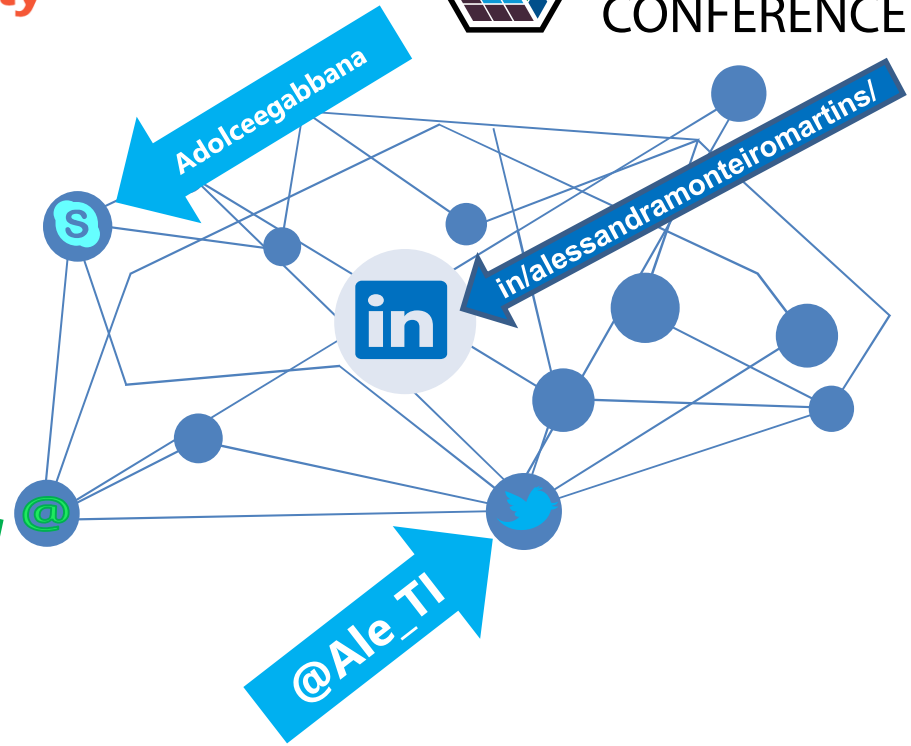
# Referências:


- https://www.centrify.com/education/what-is-zero-trust-privilege/
- https://www.youtube.com/watch?v=RmCffGgcF6E
- https://slideplayer.com/slide/12989551/
- https://www.briskinfosec.com/blogs/blogsdetail/From-tech-to-business-driven-security
- https://www.darknet.org.uk/2016/03/defence-depth-web-applications/
- https://twitter.com/brysonbort/status/1071481534060920835
- https://www.cbinsights.com/research/periodic-table-cybersecurity-startups/
- https://ifsecglobal.com/wp-content/uploads/2018/12/8793-IFSEC-Global-Periodic-Table-1.pdf
- https://thisismyclassnotes
- https://dzone.com/articles/effective-devsecops

Femme it
O JEITO FEMININO DE FALAR DE TI

Cyber Security Girls

THE DEVELOPER'S CONFERENCE

# THE DEVELOPER'S CONFERENCE