



Security by Design com AWS



Paulo Costa
Engenheiro de Software de Plataforma - Syngenta Digital



Agenda

- Conceito e pilares de SbD
- Modelagem de ameaças
 - Etapas da modelagem
 - Exemplo
- Padrões de ambientes e boas práticas - AWS



Minimizar riscos

Conjunto de recomendações

~~Metodologia~~

Arquiteturas padronizadas

Boa prática

Security by Design

~~Segurança reativa~~

~~Softwares novos~~

Processo de desenvolvimento



Conceito e pilares



Segurança da informação

2. Integridade

Preservação, precisão, consistência dos dados durante todo o seu ciclo de vida.

4. Autenticidade

Valida a autorização do usuário para acessar, receber e transmitir informações.



1. Confidencialidade

Dados acessíveis a determinados usuários e protegidos contra pessoas não autorizadas.

3. Disponibilidade

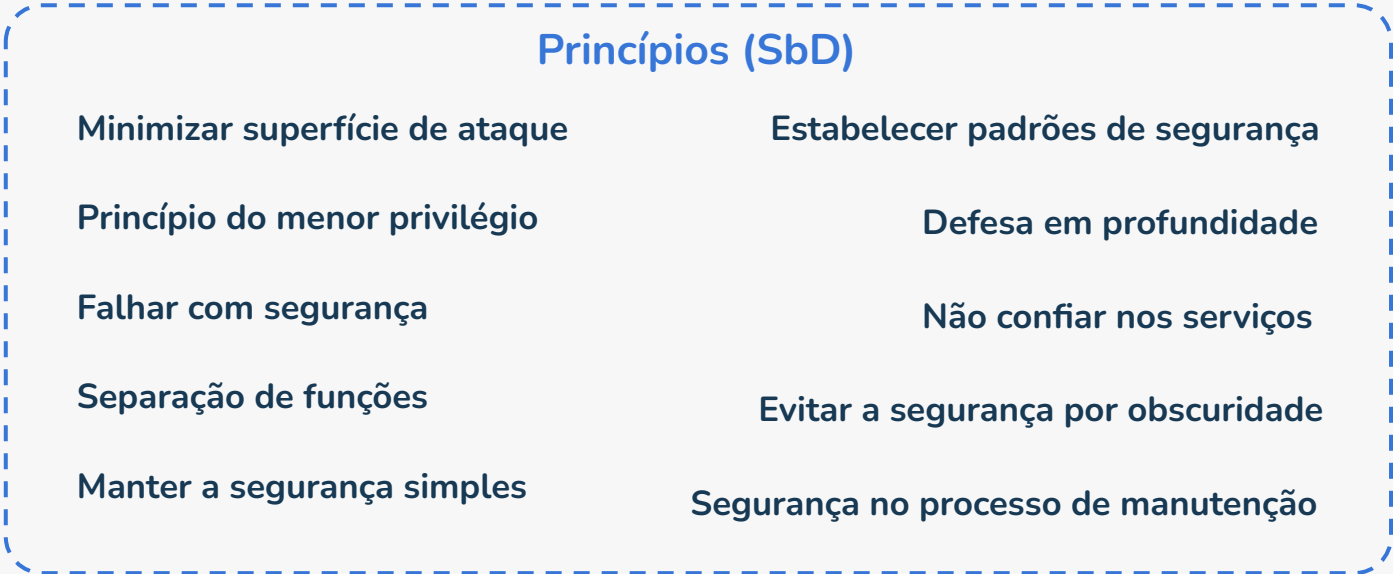
Garantia de acesso aos dados em tempo integral (24/7).

5. Legalidade

Define o valor legal da comunicação em relação à legislação.



Conceito e pilares



Modelagem de ameaças

Faz parte do conjunto de recomendações para se iniciar uma implementação do SbD.

Estruturas/modelos de ameaças:

- STRIDE
- PASTA
- CVSS
- Attack Trees
- Security Cards
- Trike
- hTMM
- VAST

STRIDE

Spoofing <> Falsificação

Tampering <> Adulteração

Repudiation <> Repúdio

Information disclosure <> Divulgação de informações

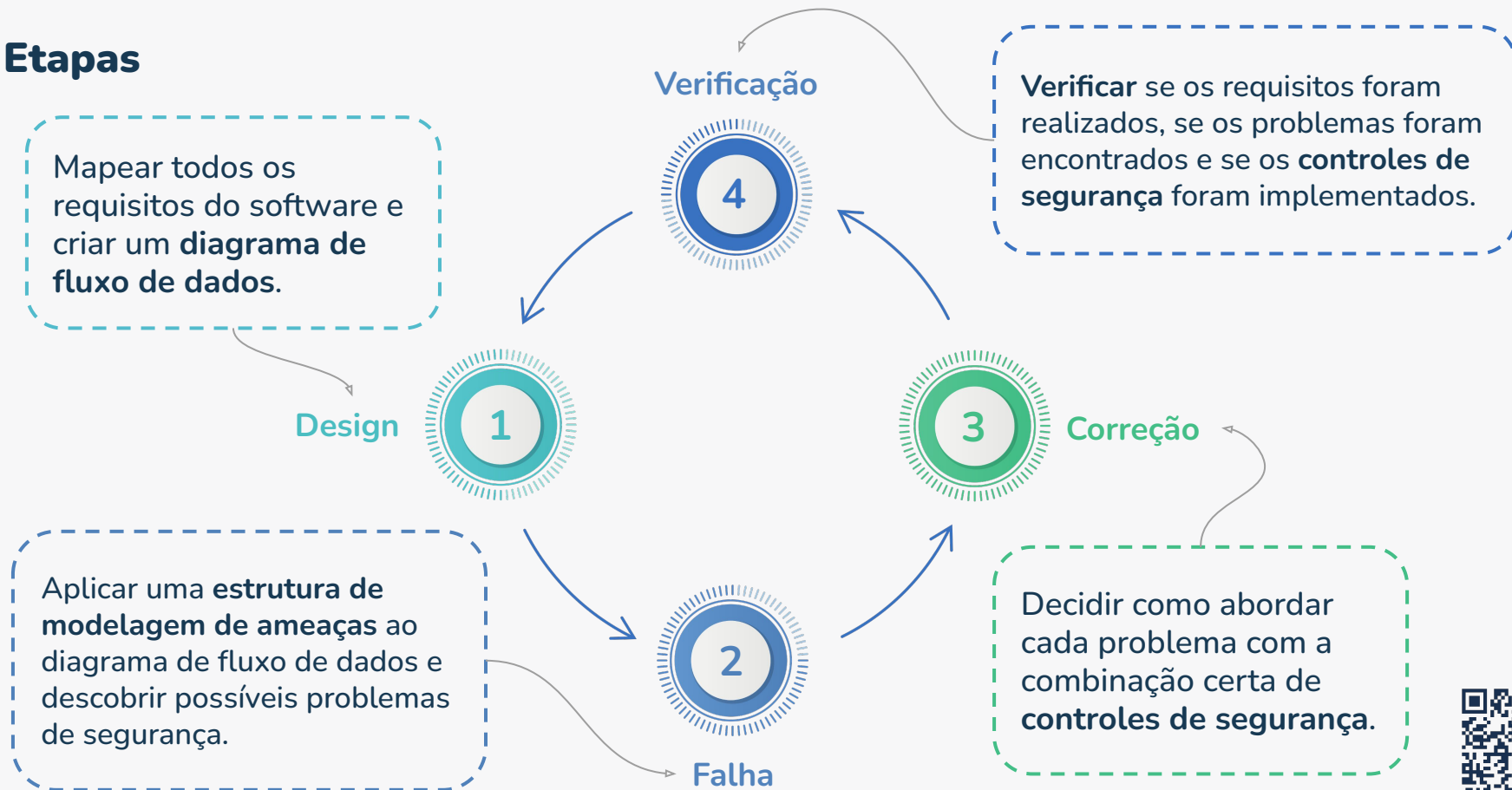
Denial of service <> Negação de serviço

Elevation of privilege <> Elevação de privilégio



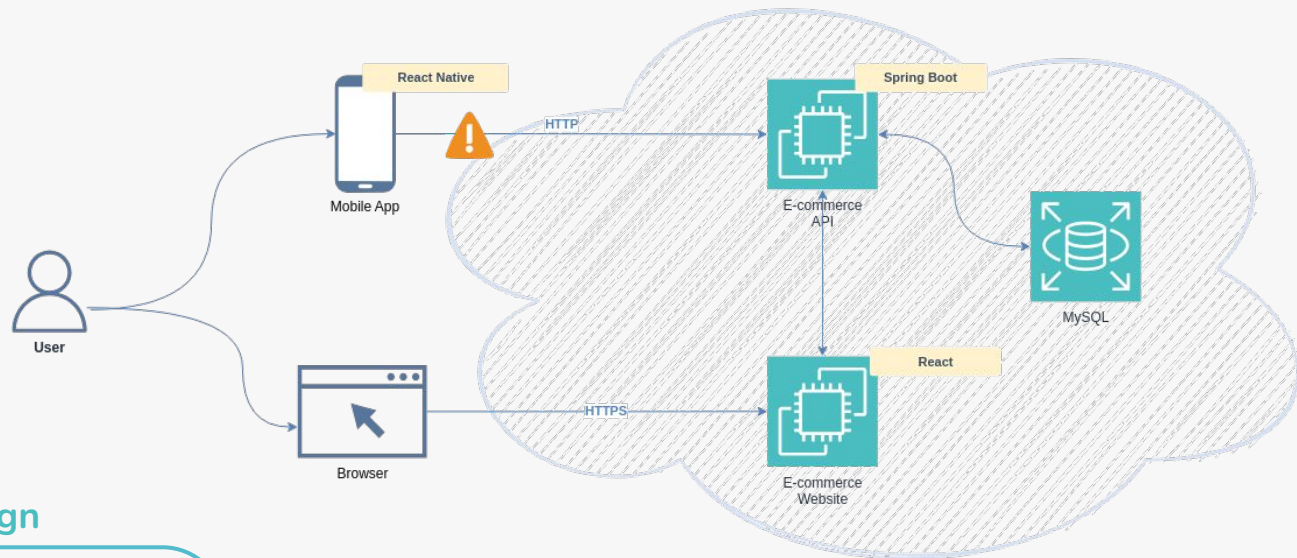
Modelagem de ameaças

Etapas



Modelagem de ameaças

Exemplo



Design

Tecnologias:

Typescript - React e React native
Java - Spring Boot

Serviços AWS:

Servidores EC2
RDS (Banco MySQL)

Comunicação/Protocolos:

HTTP e HTTPS

Falha

STRIDE

Information disclosure
Elevation of privilege
-
Falta de criptografia
no protocolo HTTP

Correção

Criptografar todos os
dados em trânsito com
protocolo HTTPS

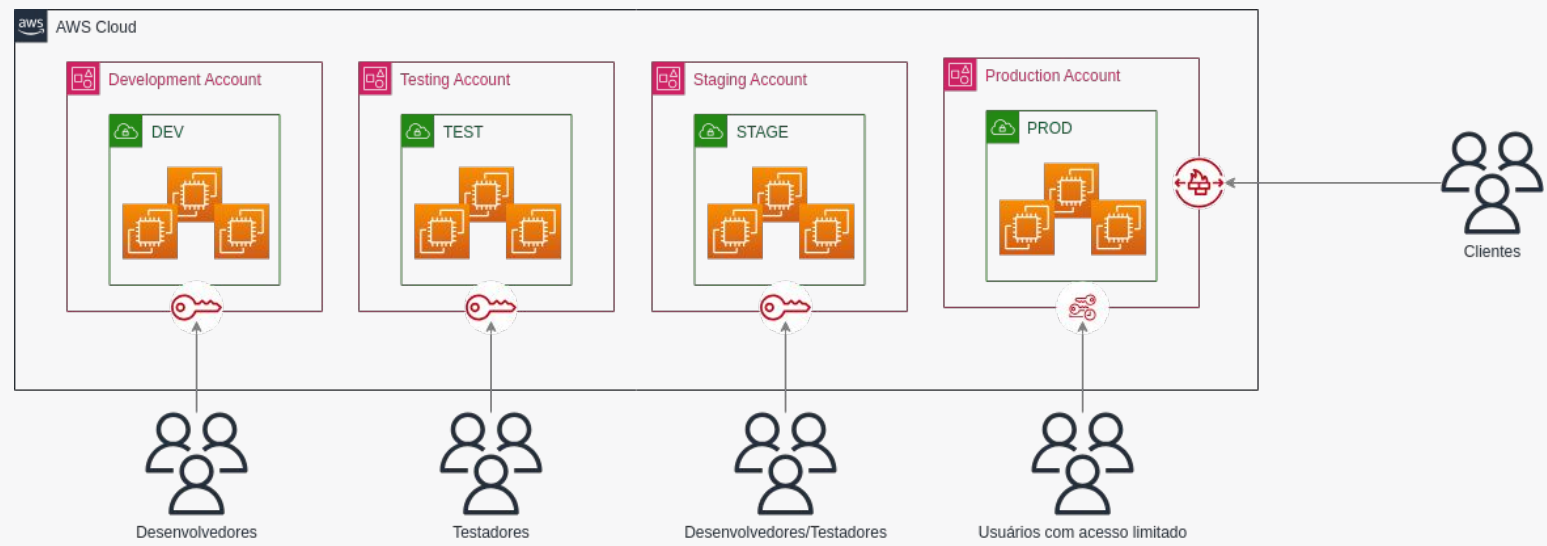
Verificação

Aplicar e validar a
correção

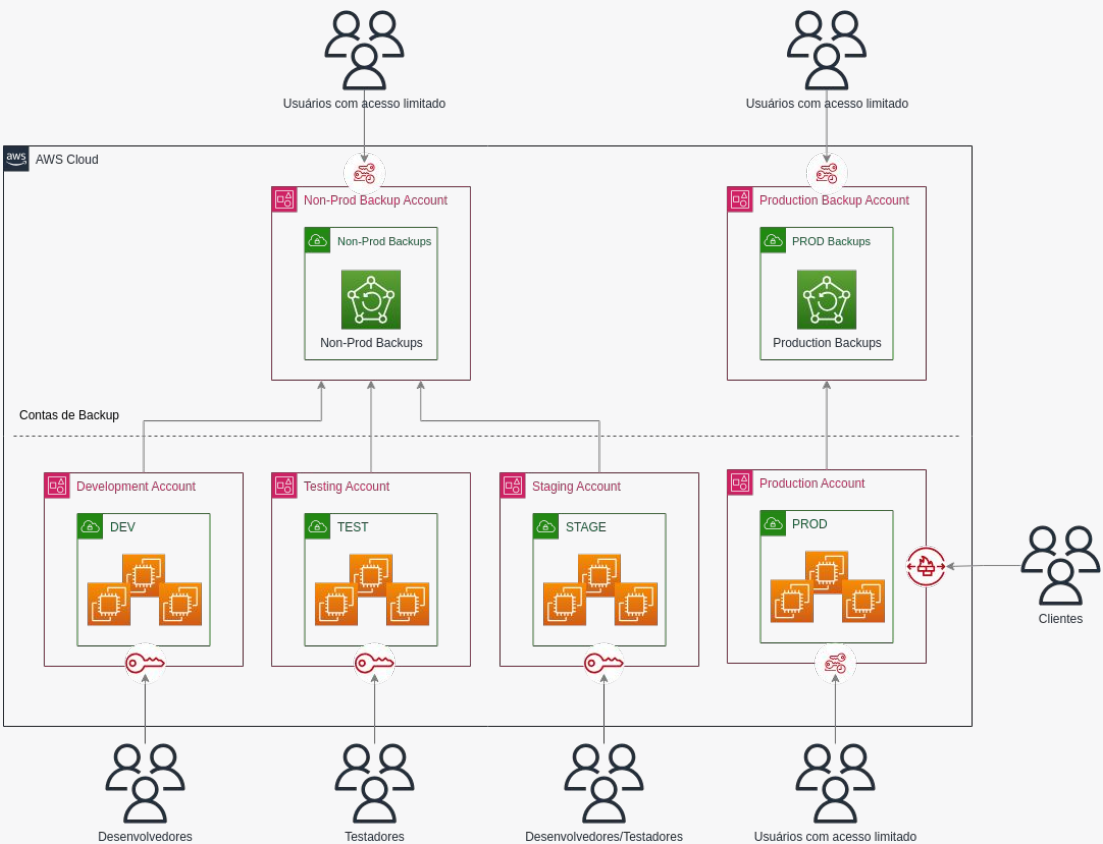


Padrões de ambientes - AWS

Ambientes SDLC (Software Development Life Cycle)

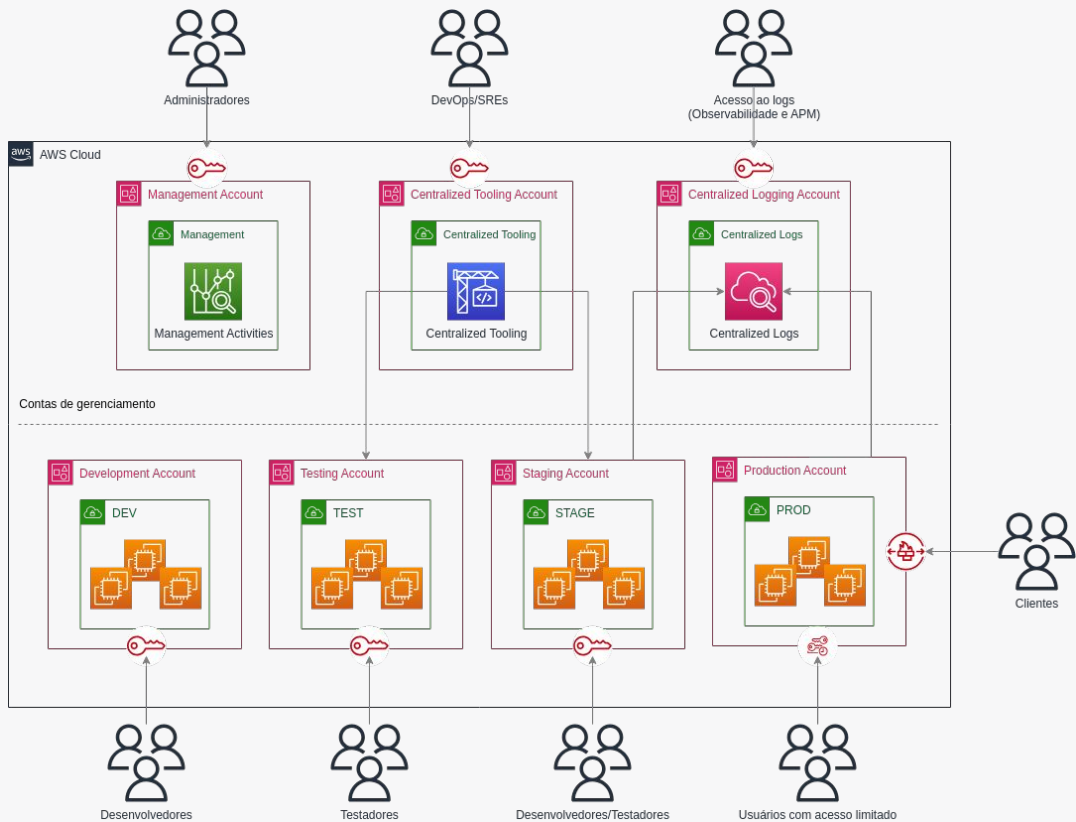


Ambientes de backup



Padrões de ambientes - AWS

Ambientes com gestão centralizada e governança



Obrigado!



linktr.ee/paulowdev