

# TOGAF®

---

*Version 9.1 Enterprise Edition*

## Módulo 31 Adaptando o ADM: Segurança

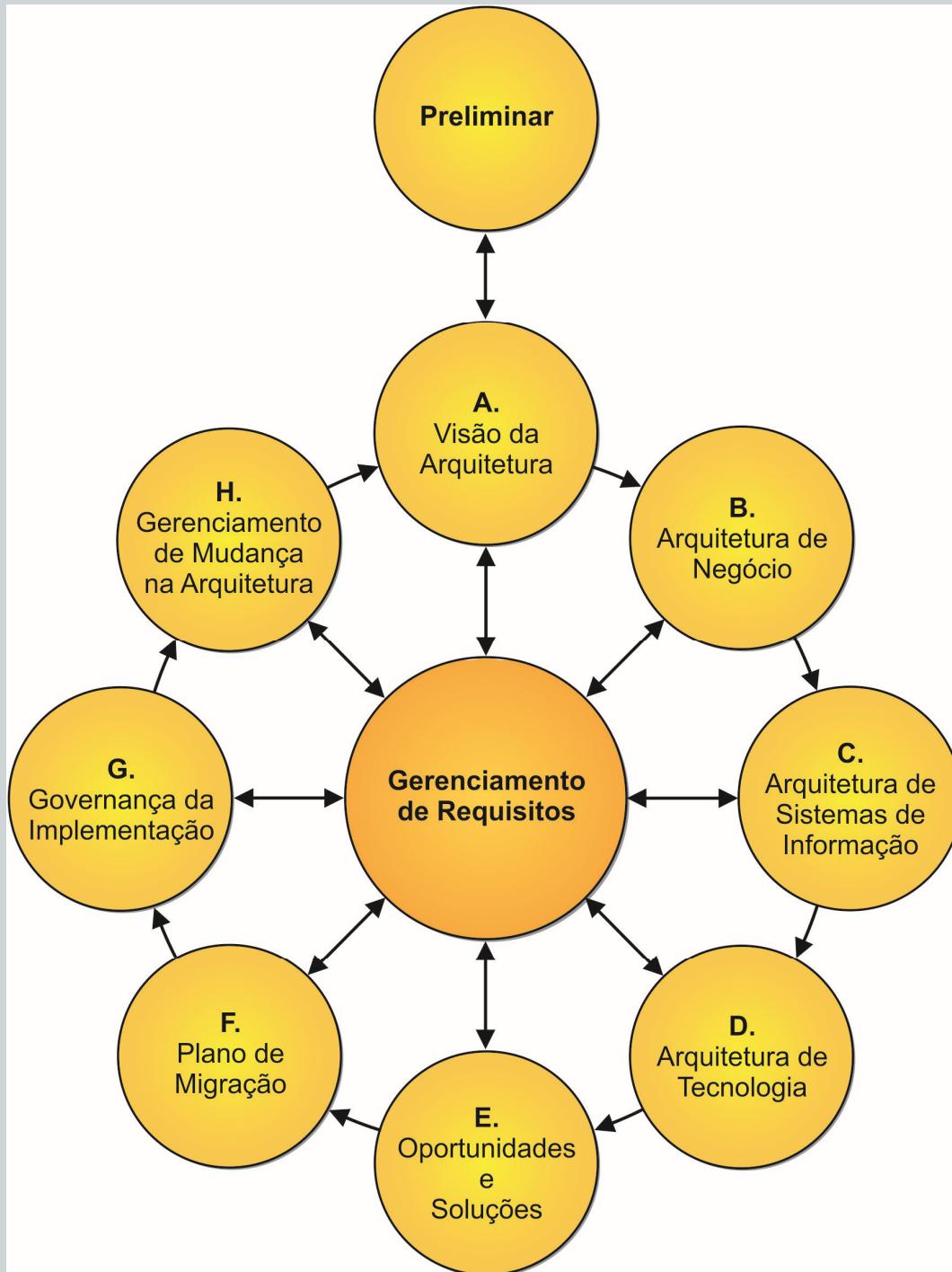
V9.1 Edition Copyright © January 2009

THE **Open** GROUP  
All rights reserved  
Published by The Open Group, January 2009



**SETTI**  
Tecnologia & Inovação

# Adaptando o ADM: Segurança



TOGAF é uma marca registrada do The Open Group nos Estados Unidos e em outros países

**TOGAF®**

# Roadmap

<b>Parte I - Introdução</b>
Prefácio, Visão global executiva, Principais Conceitos, Definições e Notas da Versão
<b>Parte II – Método de Desenvolvimento da Arquitetura</b>
Introdução ao ADM
Narrativas das Fases do ADM
<b>Parte III – Orientações e Técnicas do ADM</b>
Orientações para Adaptação do Processo do ADM
Técnicas para o Desenvolvimento da Arquitetura
<b>Parte IV – Framework de Conteúdo da Arquitetura</b>
Metamodelo de Conteúdo
Artefatos Arquiteturais
Entregáveis da Arquitetura
Blocos de Construção
<b>Parte V – Continuum da Corporação e Ferramentas</b>
Continuum da Corporação
Particionamento da Arquitetura
Repositório da Arquitetura
Ferramentas para o Desenvolvimento da Arquitetura
<b>Parte VI – Modelos de Referência do TOGAF</b>
Arquitetura de Fundação: Modelo de Referência Técnico
Modelo de Referência da Infraestrutura Integrada da Informação
<b>Parte VII – Framework de Capacidade da Arquitetura</b>
Staff da Arquitetura
Aderência da Arquitetura
Contratos da Arquitetura
Governança da Arquitetura
Modelos de Maturidade da Arquitetura
Frameworks de Competências da Arquitetura

- Parte III, Diretrizes para o ADM e Técnicas, Capítulo 21



# Objetivos do Módulo

Os objetivos deste módulo são:

- Obter um conhecimento das considerações de segurança que precisam ser atendidas durante a aplicação do ADM

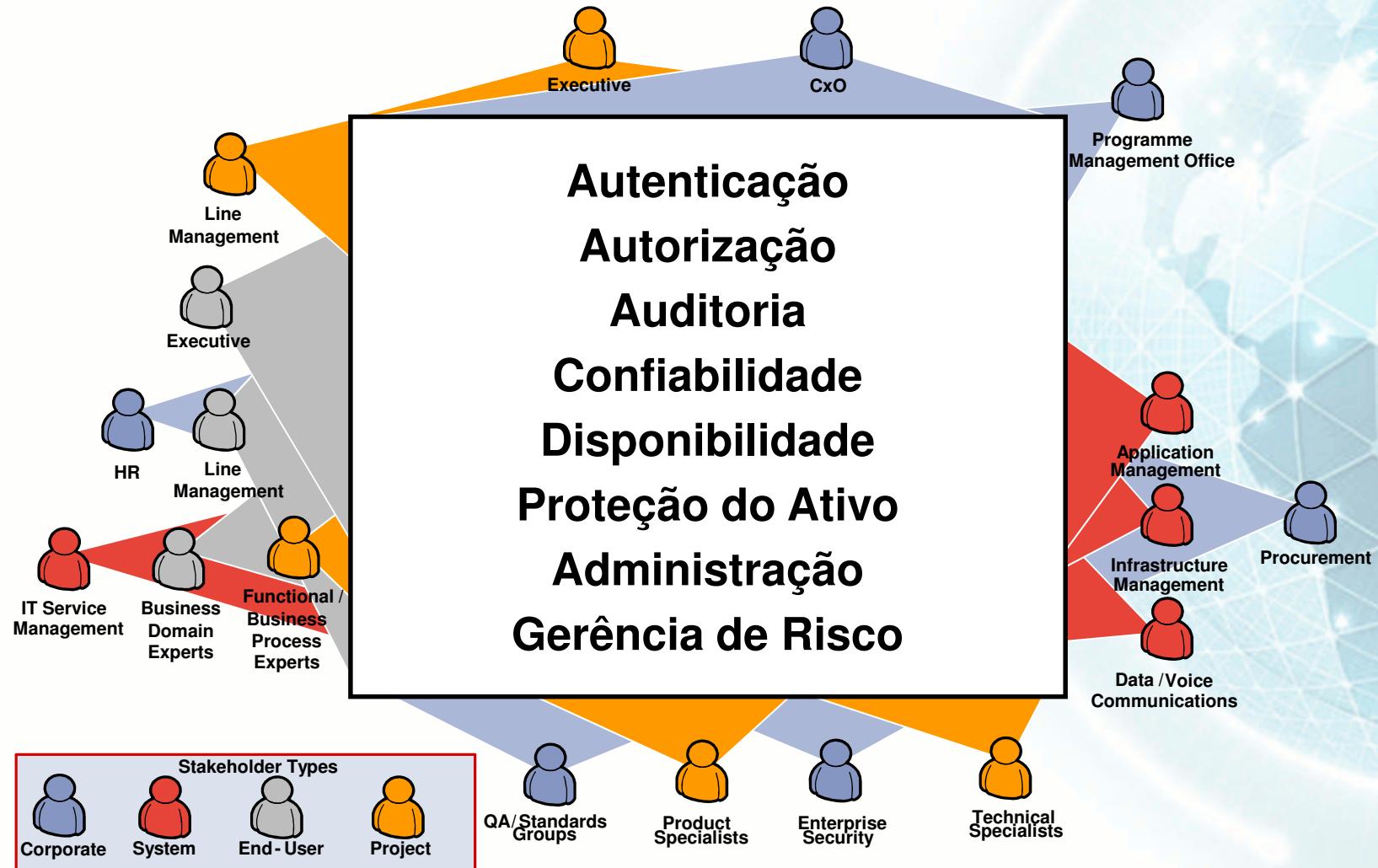
# Segurança e o ADM

- O TOGAF introduz diretrizes para ajudar os profissionais a evitar o esquecimento de preocupações críticas de segurança
- As diretrizes não tem a intenção de ser uma metodologia de desenvolvimento de arquitetura de segurança
- Elas se propõem a informar ao Arquiteto Corporativo sobre as tarefas e papéis da arquitetura de segurança
- Foram desenvolvidos objetivos de segurança para cada fase do ADM

# Características da Arquitetura de Segurança

- Ela tem sua própria metodologia de segurança
- Ela compõe seus próprios pontos de vista e visões distintas
- Ela atende a fluxos não normativos
- Ela introduz seu próprio fluxo normativo único
- Introduz componentes únicos, de propósito único no projeto
- Ela exige um conjunto único de habilidades do arquiteto corporativo.

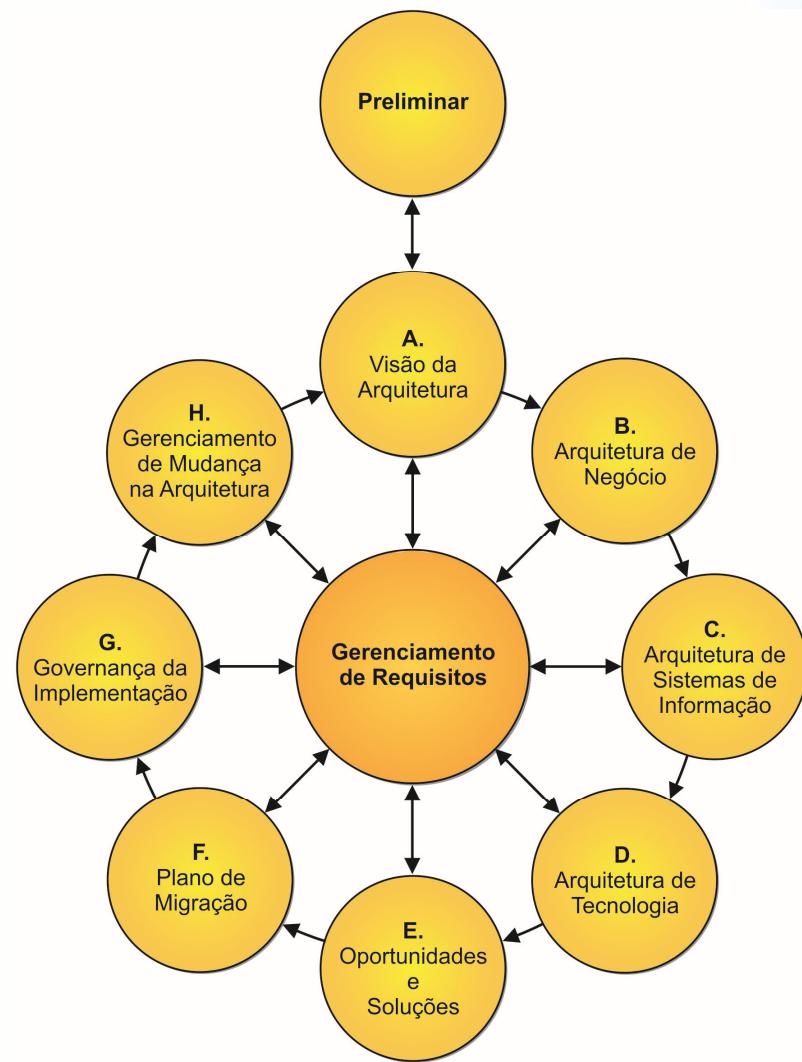
# Preocupações das Partes Interessadas



# Artefatos de Segurança Típicos

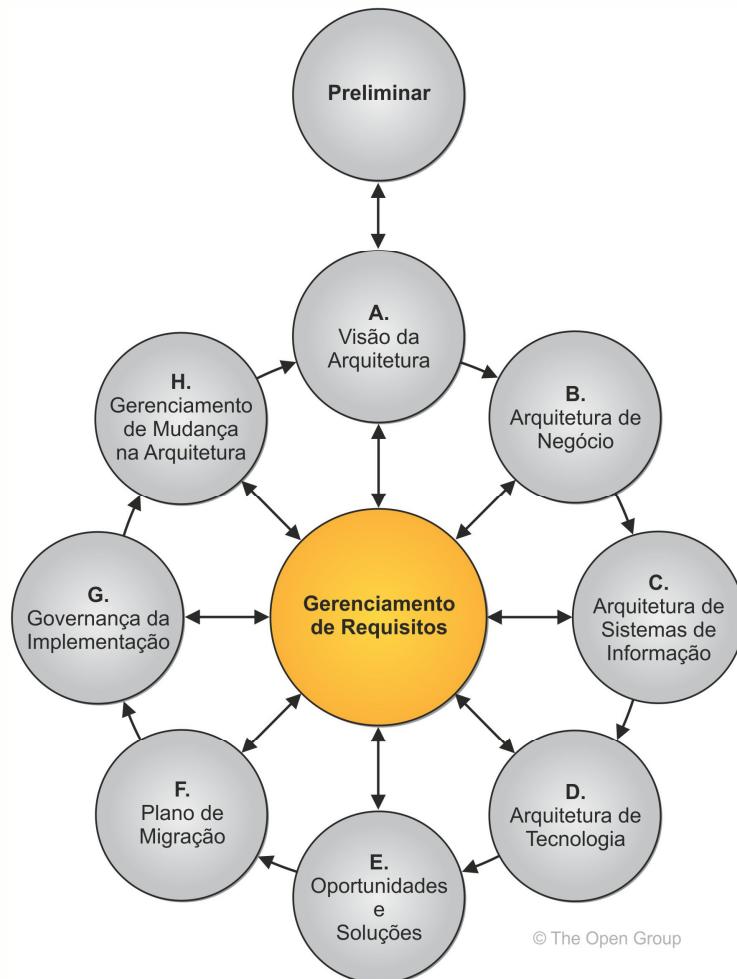
- Regras de negócios em relação ao manuseio dos dados / informação dos ativos
- Políticas de segurança escritas e publicadas
- Dados codificados / informações dos ativos, propriedade e custódia
- Documentação de análise de risco
- Documentação de política para classificação de dados

# O ADM do TOGAF



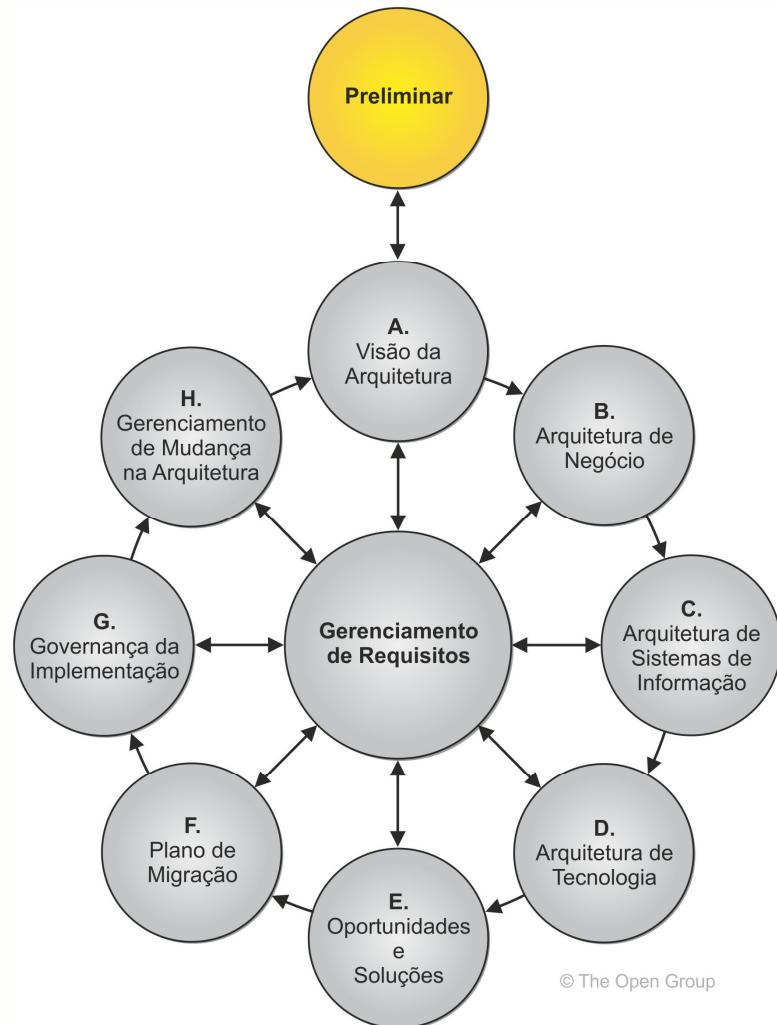
TOGAF®

# Gerenciamento de Requisitos do ADM



- Políticas de Segurança e Normas de Segurança se tornam parte do processo de gerenciamento de requisitos
- Novos requisitos de Segurança surgem de várias origens:
  - Uma nova obrigação estatutária ou regulatória
  - Uma nova ameaça percebida ou experienciada
  - Uma nova iniciativa de arquitetura descobre novas partes interessadas como novos requisitos

# Fase Preliminar



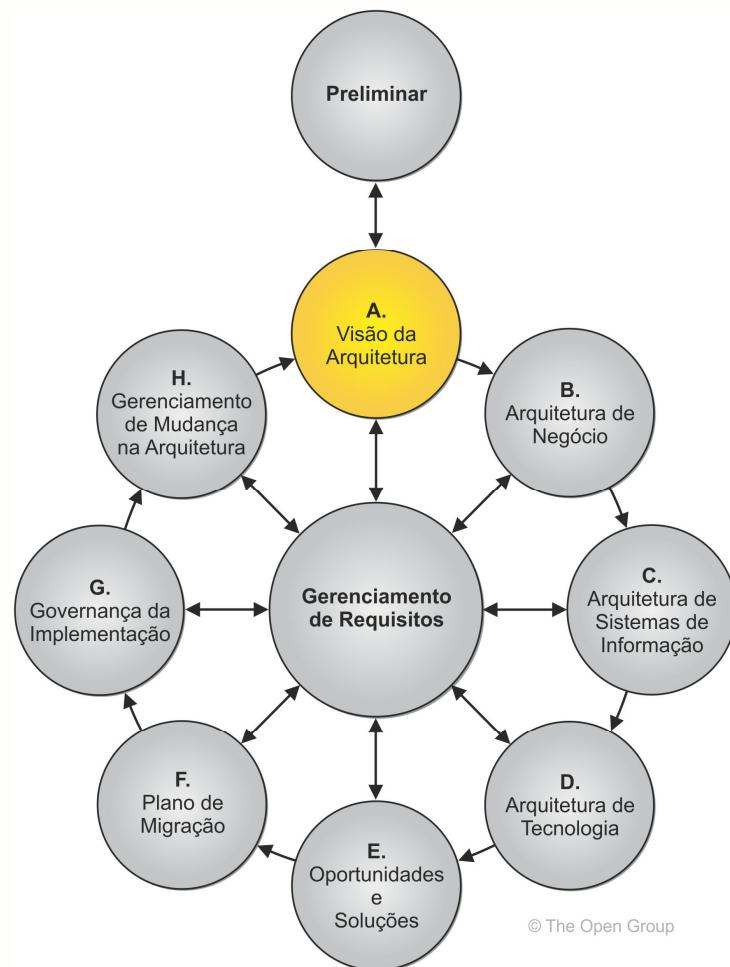
- Demarca as unidades organizacionais da corporação que serão impactadas pela arquitetura de segurança
- Define e documenta requisitos para políticas regulatórias e de segurança aplicáveis.
- Define as capacidades de segurança requeridas como parte da Arquitetura de Capacidade
- Implementa ferramentas de arquitetura de segurança

# Fase Preliminar – Entradas/Saídas

- Entradas:
  - Política de Segurança
  - Estatutos relevantes
  - Lista de jurisdições aplicáveis
- Saídas:
  - Lista de Regulações aplicáveis
  - Lista de políticas de segurança aplicáveis
  - Lista da equipe de segurança
  - Lista de pressupostos de segurança e condições de contorno

# Fase A

## Visão da Arquitetura



- Obter apoio gerencial para medidas de segurança
- Definir os marcos gerenciais necessários de aprovação de assuntos relacionados a segurança
- Determinar os requisitos de recuperação de desastres ou planos de continuidade de negócios aplicáveis
- Identificar antecipadamente o(s) ambiente(s) que o(s) sistema(s) será(ão) implantado(s)
- Determinar a criticidade do sistema: de Segurança Crítica/de Missão Crítica/Não Crítica

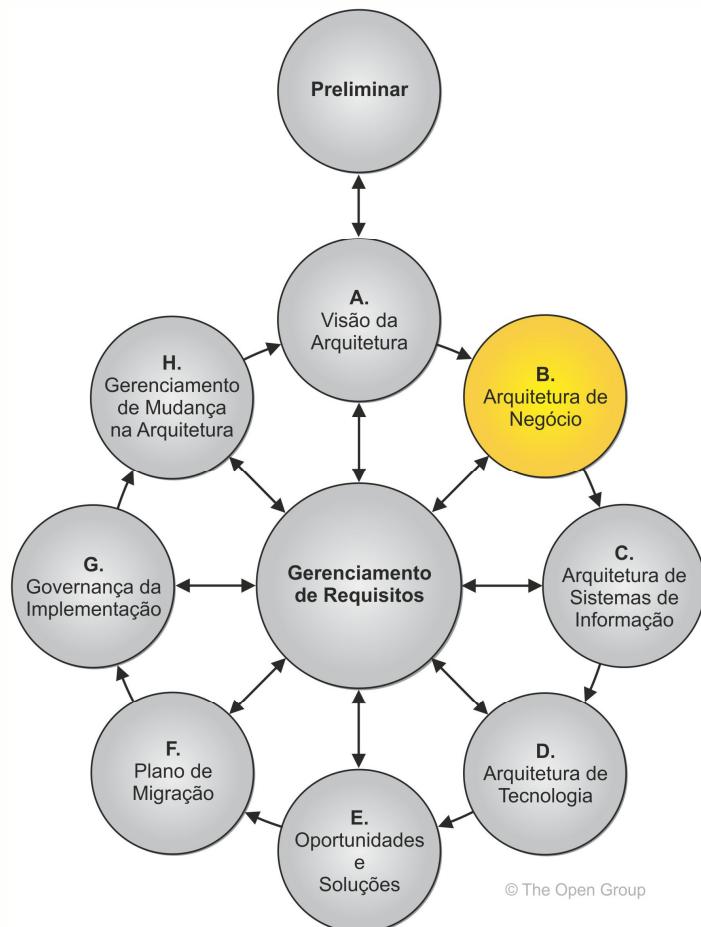
# Fase A

## Visão da Arquitetura – Entradas/Saídas

- Entradas
  - Lista de políticas de segurança aplicáveis
  - Lista de jurisdições aplicáveis
  - Planos completos de planos de desastre e recuperação e continuidade
- Saídas
  - Declaração de segurança física
  - Declaração de Segurança de Negócios
  - Declaração de Segurança regulatória
  - Carta com política de segurança assinada pelo CEO ou representante
  - Lista de checkpoints de desenvolvimento de arquitetura
  - Lista de planos de desastre e recuperação e de continuidade de negócios
  - Homologação dos sistemas críticos

# Fase B

## Arquitetura de Negócio

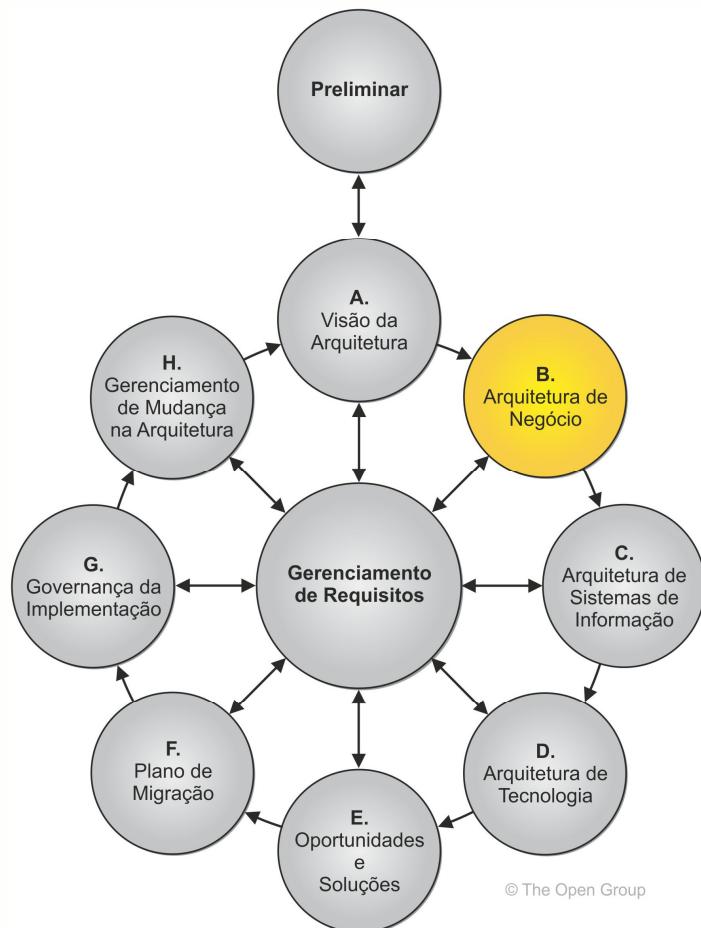


- Determinar quem são os atores legítimos que irão interagir com o sistema
- Avaliar e criar uma linha de base de específica de segurança de processos de negócio
- Determinar quem / o quanto é aceitável transtornos em utilizar medidas de segurança:
- Identificar e documentar sistemas de interconexão além do controle do projeto
- Determinar os ativos em risco, se algo der errado
- Determinar o custo da perda de ativos
- Identificar e documentar a propriedade dos ativos

Continued

# Fase B

## Arquitetura de Negócio



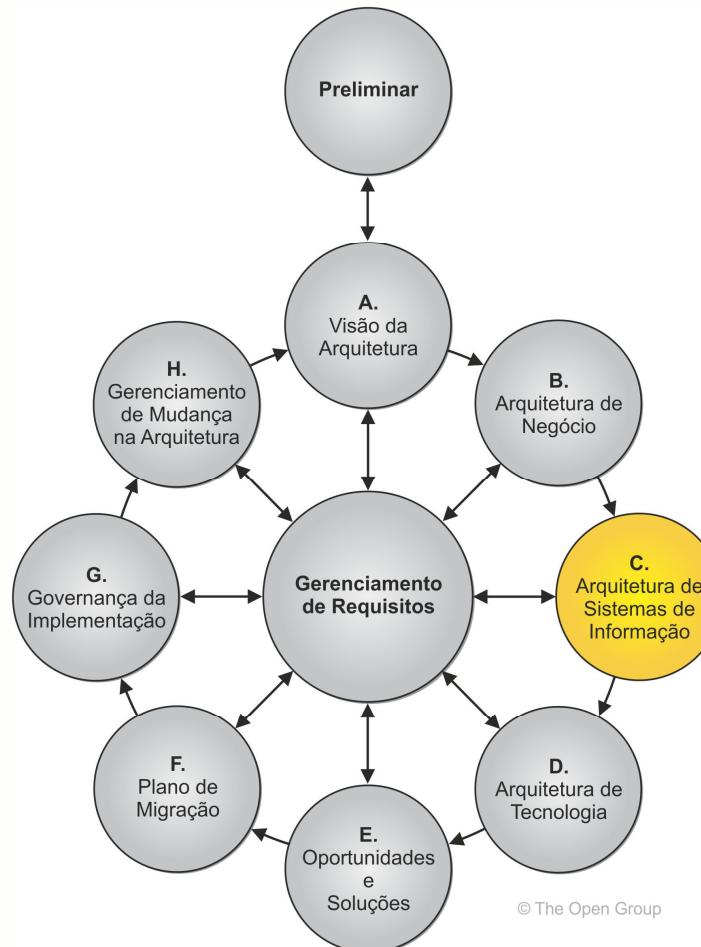
- Determinar e documentar os processos de segurança forenses apropriados
- Identificar a criticidade da disponibilidade e da correta operação do serviço em geral
- Determinar e documentar o quanto de segurança (custo) é justificado pelas ameaças e valor dos ativos
- Reavaliar e confirmar as decisões da visão de arquitetura
- Avaliar o alinhamento ou conflito de políticas de segurança identificadas com os objetivos de negócio
- Determinar "o que pode dar errado?"

# Fase B: Arquitetura de Negócio – Entradas/Saídas

- Entradas
  - Declarações de segurança iniciais de negócio e regulatória
  - Lista dos planos aplicáveis de recuperação de desastres e continuidade de negócio
  - Lista das políticas de segurança e regulamentações aplicáveis
- Saídas
  - Lista de processos forenses
  - Lista de novos requisitos para recuperação de desastres e continuidade de negócio
  - Declarações sobre ambientes de negócio e regulatório validadas
  - Lista de políticas e regulamentações de segurança validada
  - Lista de processos de segurança alvos
  - Lista de processos de segurança de linha de base
  - Lista de atores da segurança
  - Lista de sistemas de interconexão
  - Declaração de tolerância de segurança para cada classe de atores da segurança
  - Lista de ativos com valores e propriedade
  - Lista de caminhos confiáveis
  - Declaração(ões) de impacto na disponibilidade
  - Matriz de análise de ameaça

# Fase C

## Arquiteturas de Sistemas de Informação

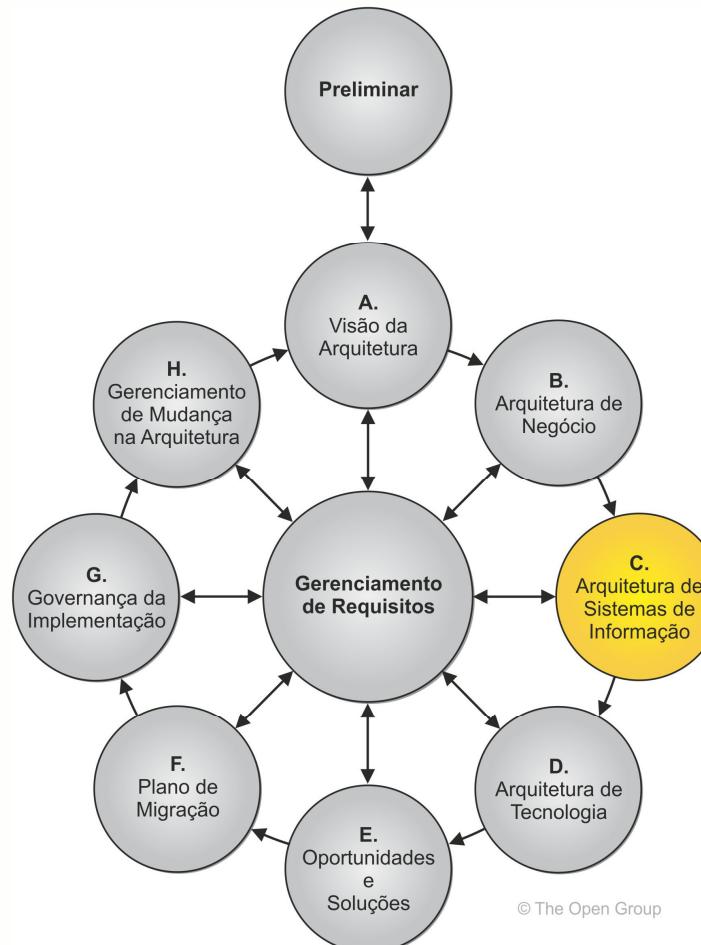


- Avaliar e criar uma linha de base dos elementos específicos de segurança atuais
- Identificar ações padrão de segurança e estados de falha
- Identificar e avaliar diretrizes e padrões reconhecidamente aplicáveis
- Revisitar suposições relacionadas a interconectar sistemas além do controle do projeto
- Determinar e documentar o nível de sensibilidade ou classificação da informação armazenada / criada / usada
- Identificar e documentar a custódia dos ativos

Continued

# Fase C

## Arquiteturas de Sistemas de Informação

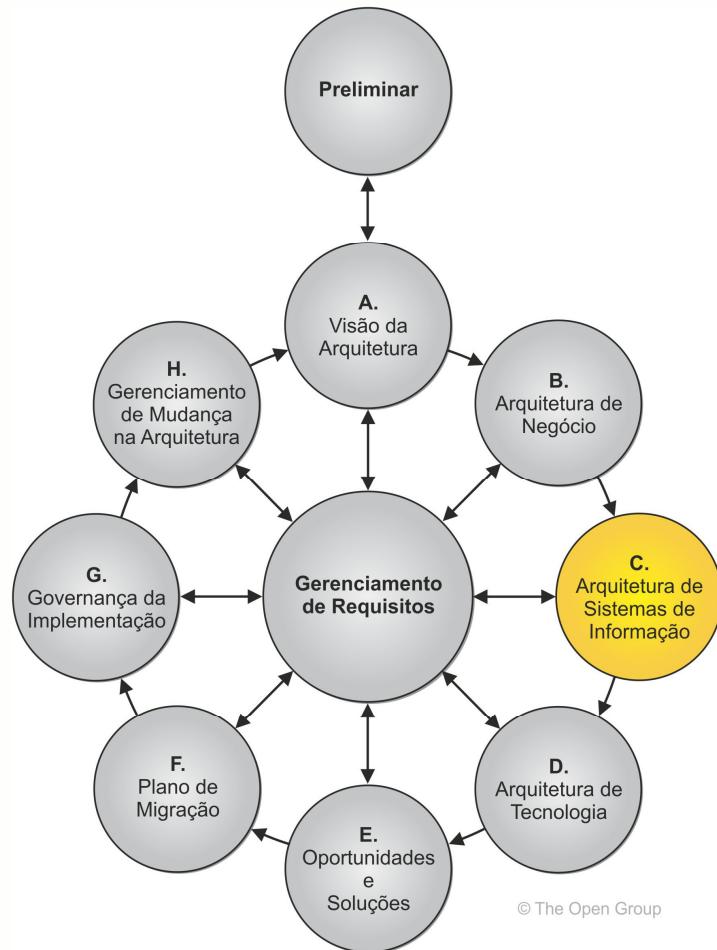


- Identificar a criticidade da disponibilidade e a operação correta de cada função
- Determinar o relacionamento do sistema projetado com os planos de continuidade/desastre de negócio
- Identificar quais aspectos do sistema precisam ser configuráveis para refletir alterações nas políticas/ambiente de negócio/controle de acesso
- Identificar o tempo de vida das informações utilizadas, tal como definido pelas necessidades do negócio e requisitos regulamentares

Continuação

# Fase C

## Arquiteturas de Sistemas de Informação



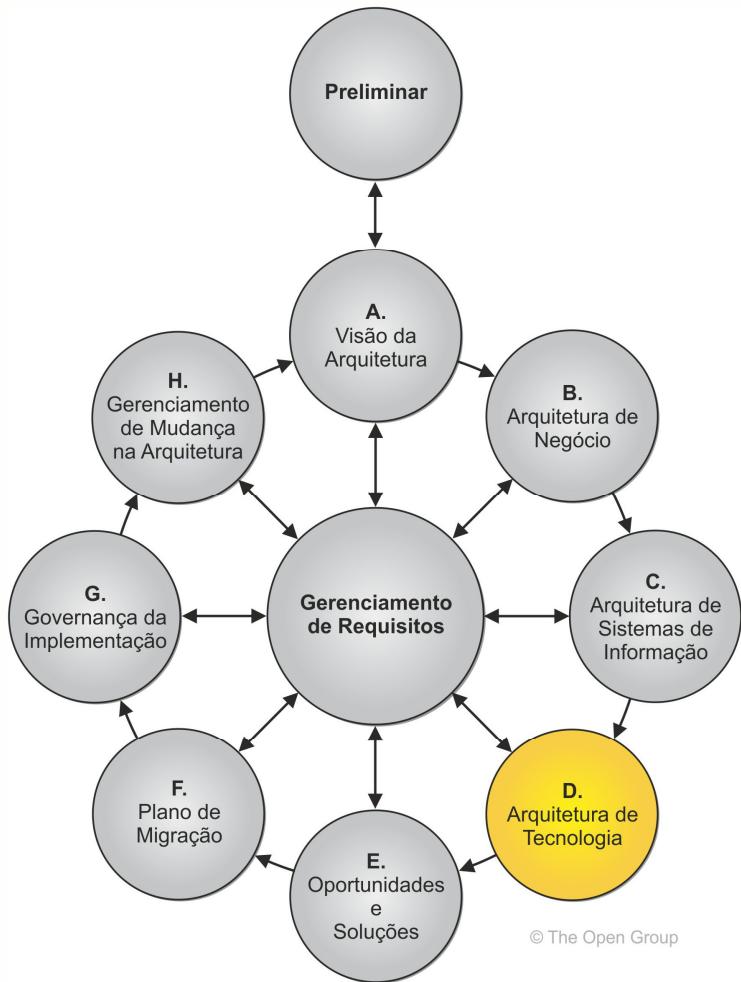
- Determinar formas de endereçar riscos identificados
- Identificar ações / eventos que justifiquem registro para posterior análise ou desencadear processos forenses
- Identificar e documentar requerimentos rigorosos visando prover a precisão dos eventos registrados (não repúdio)
- Identificar possíveis / prováveis caminhos de ataque
- Determinar “O que pode dar errado?”

# Fase C: Arquiteturas de sistemas de Informação – Entradas / Saídas

- Entradas
  - Matriz de análise de ameaças
  - Análise de risco
  - Processos forenses documentados
  - Políticas de negócios e regulamentos validados
  - Lista dos sistemas interconectados
  - Recuperação de desastres e requisitos de continuidade de negócios
- Saídas
  - Matriz em nível de log de eventos e requisitos
  - Estratégia de gestão de risco
  - Definições de dados de ciclo de vida
  - Lista de elementos configuráveis do sistema
  - Lista de linha de base de elementos relacionados a segurança do sistema
  - Elementos novos ou agregados de elementos relacionados a segurança do sistema
  - Modelos de casos de uso de segurança
  - Lista de normas de segurança aplicáveis:
  - Lista validada de sistemas interligados
  - Relatório de classificação de informações
  - Lista de guardiões de ativos
  - Declaração de criticidade da função
  - Planos revistos de desastre e recuperação e continuidade de negócio
  - Matriz refinada de análise de ameaça

# Fase D

## Arquitetura Tecnológica

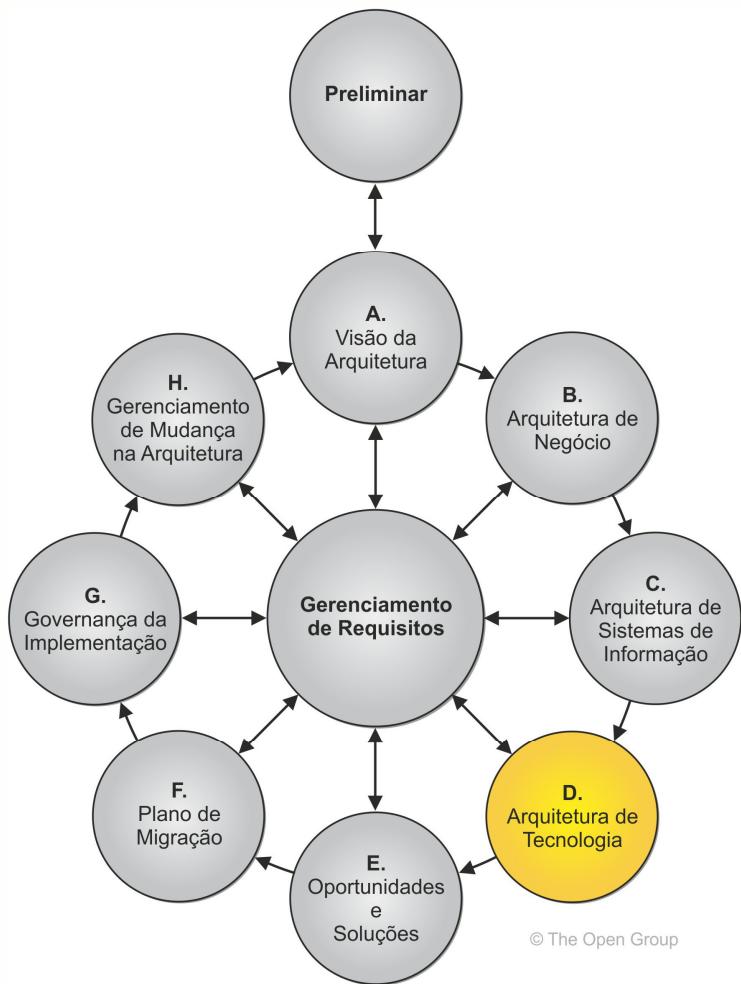


- Avaliar e criar linha de base das tecnologias específicas de segurança atuais
- Revisitar pressupostos relacionados a interconexão de sistemas além do controle do projeto
- Identificar e avaliar padrões e diretrizes reconhecidamente aplicáveis
- Identificar métodos para regular o consumo de recursos
- Engendar um método pelo qual a eficácia de medidas de segurança seja medida e comunicada de forma contínua

Continuação

# Fase D

## Arquitetura Tecnológica



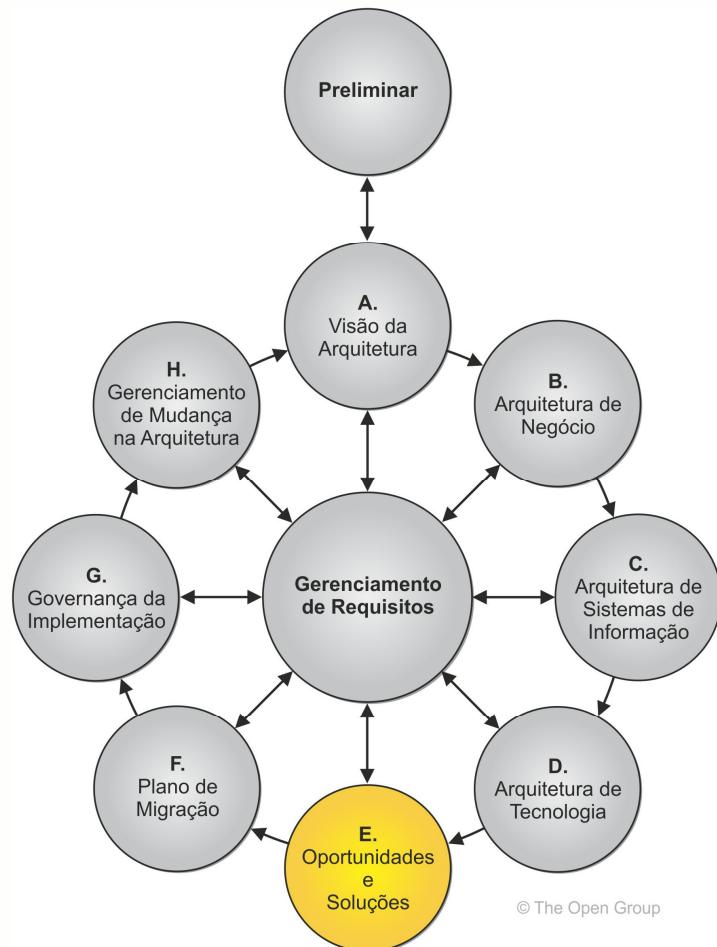
- Identificar o nível de confiança (depuração) aceitável para o sistema
- Identificar os privilégios mínimos requeridos para qualquer entidade alcançar um objetivo técnico ou de negócio
- Identificar medidas de mitigação de segurança, onde forem justificadas por uma avaliação de risco
- Determinar "o que pode dar errado?"

# Fase D: Arquitetura Tecnológica – Entradas/Saídas

- Entradas
  - Lista dos elementos do sistema relacionados com segurança
  - Lista dos sistemas interconectados
  - Lista de normas de segurança aplicáveis
  - Lista de agentes de segurança
  - Estratégia de gestão de risco
  - Políticas de segurança validadas
  - Requisitos regulamentares validados
  - Políticas de negócios validadas relacionados com requisitos de confiança
- Saídas
  - Lista básica de tecnologias de segurança
  - lista de sistemas interconectados validadas
  - lista de padrões de segurança selecionados
  - Plano de conservação de recursos
  - Métricas de segurança e plano de monitoração
  - Políticas de autorização de usuários
  - Plano de gerenciamento de risco
  - Requisitos de confiança de usuários (depuração)

# Fase E

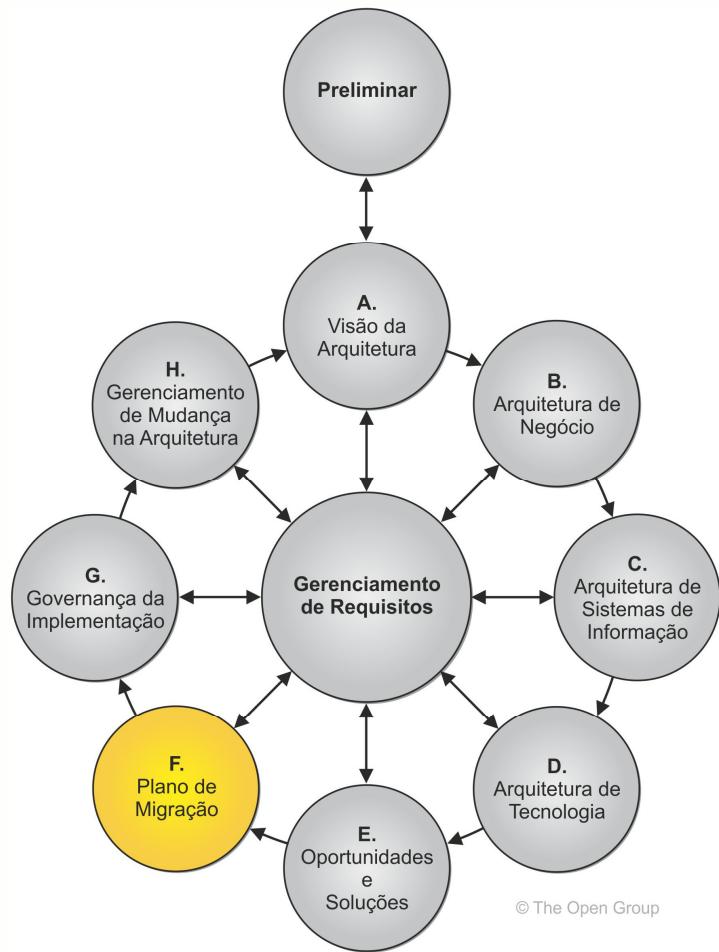
## Oportunidades e Soluções



- Identificar os serviços de segurança existentes disponíveis para reutilização
- Engendrar medidas de mitigação endereçando os riscos identificados
- Avaliar software de segurança e recursos de segurança do sistema para que sejam testados e reutilizáveis
- Identificar novos códigos/recursos/ativos que são apropriados para o reuso
- Determinar “o que pode dar errado?”

# Fase F

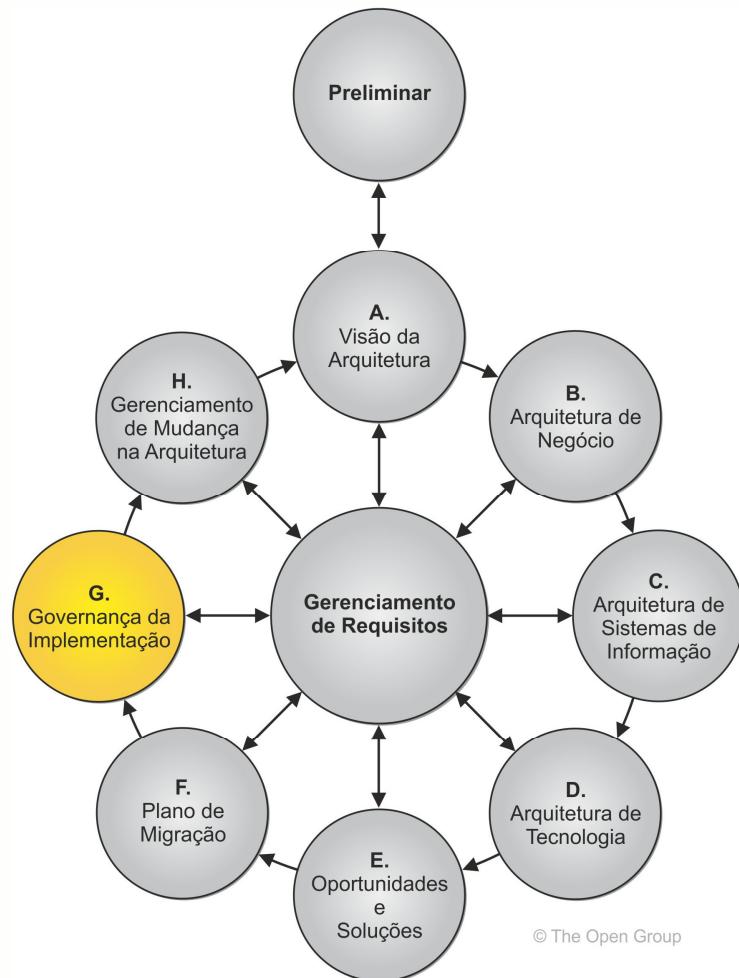
## Plano de Migração



- Avaliar o impacto de novas medidas de segurança em novos componentes ou sistemas existentes
- Implementar métodos de garantia de que a eficácia das medidas de segurança será medida e comunicada de forma contínua
- Identificar os parâmetros corretos de instalação seguras, condições iniciais e configurações
- Implementar planos de desastre e recuperação e continuidade de negócio
- Determinar “O que pode dar errado?”

# Fase G

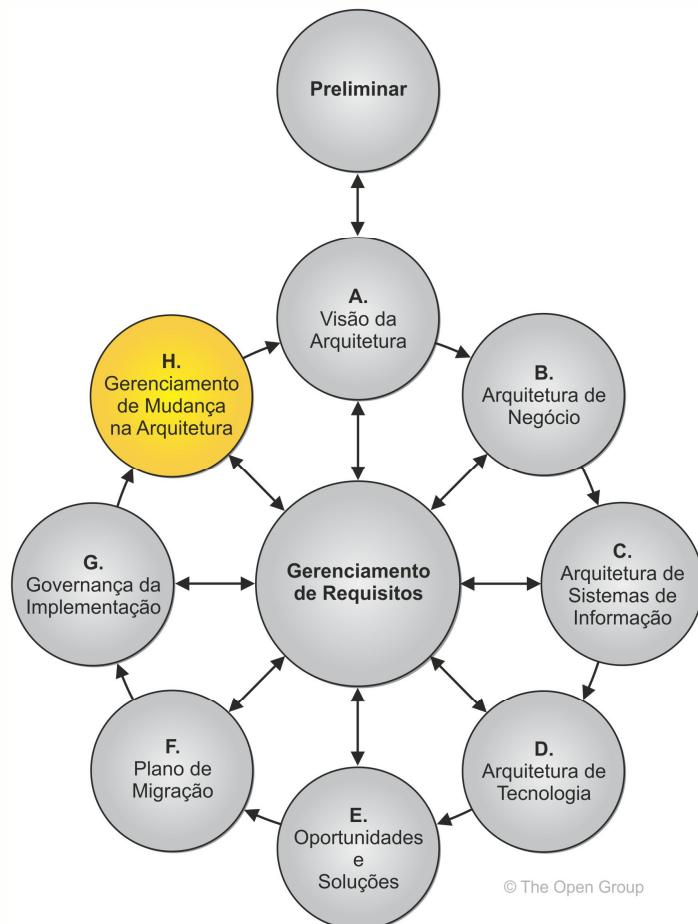
## Governança da Implementação



- Estabelecer revisões de projeto e de código
- Implementar métodos e procedimentos para rever evidências reflitam a estabilidade operacional e aderência às políticas de segurança
- Implementar treinamento necessário para garantir a correta implantação, configuração e operação
- Determinar "o que deu errado?"

# Fase H

## Gerenciamento de Mudança na Arquitetura



- Determinar “o que deu errado?”
- Incorporar as mudanças relevantes de segurança do ambiente nos requisitos para o aprimoramento futuro

# Sumário

- O TOGAF introduz diretrizes sobre Segurança e para o ADM para que profissionais evitem negligenciar uma preocupação crítica de segurança.
- As diretrizes não tem a intenção de ser uma metodologia de desenvolvimento de segurança
- A intenção é informar ao arquiteto corporativo sobre tarefas e papéis da arquitetura de segurança

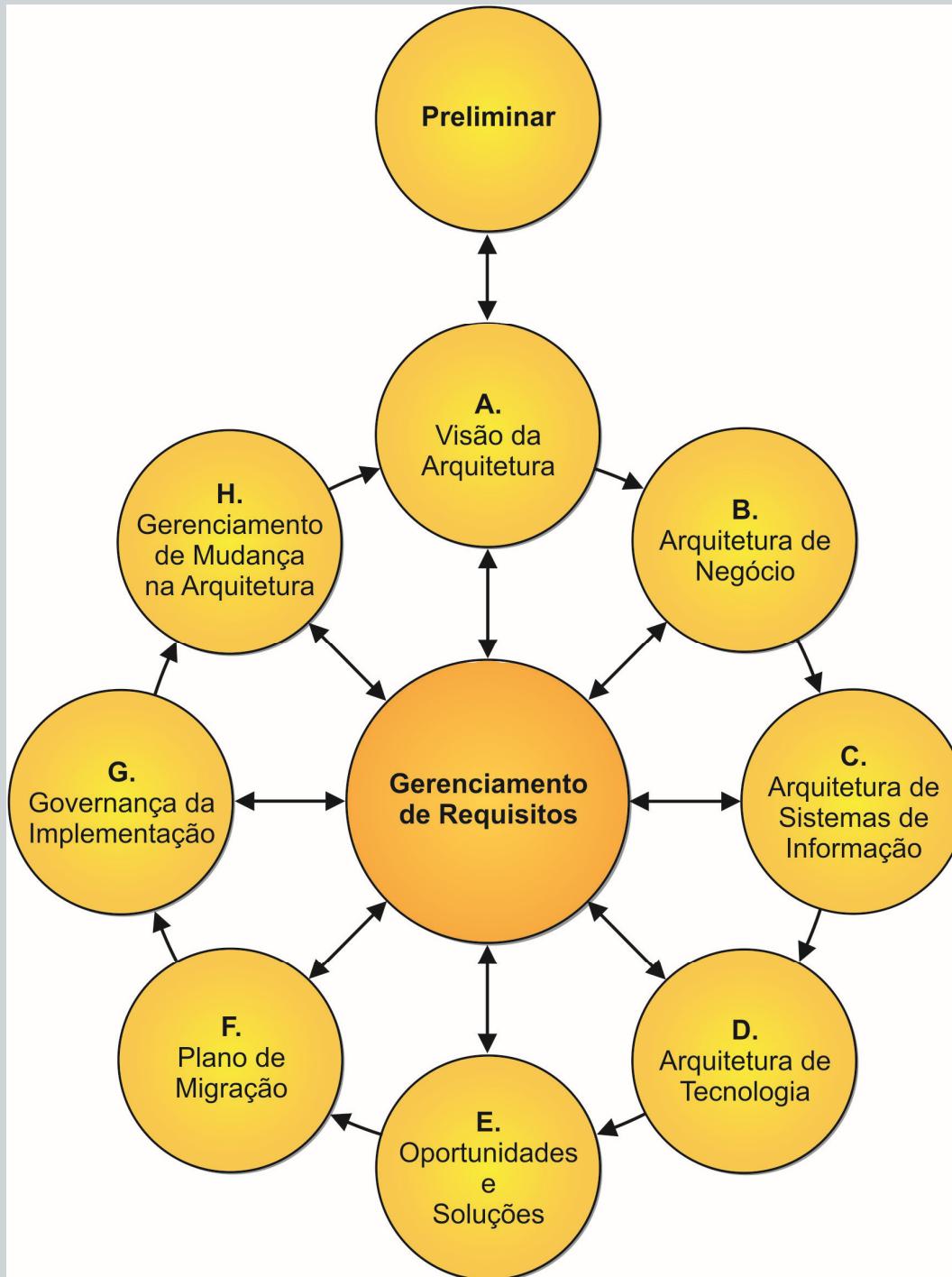
# Exercício

Novos requisitos de segurança surgiram de várias fontes:

1. Uma nova obrigação estatutária ou regulatória
2. Uma nova ameaça percebida ou experienciada
3. Uma nova iniciativa de arquitetura de TI descobre novas partes interessadas e/ou novos requisitos

Para cada um destas situações, discuta seu impacto no ADM

# Adaptando o ADM: Segurança



TOGAF é uma marca registrada do The Open Group nos Estados Unidos e em outros países

**TOGAF®**