

4SEG – SEGURANÇA DE REDES

AULA SOBRE GOVERNANÇA, GESTÃO DE TI, FRAMEWORK COBIT 5

Profa. Maria Cláudia Roenick Guimarães
E-mail: maria.roenick@faeterj-rio.edu.br

Governança de TI

- Com o crescimento da importância da área de TI para o sistema corporativo, surgiu o conceito de Governança de TI, que tem por objetivo:
 - Melhorar os processos de TI;
 - Alinhar a gestão da TI com estratégias da organização;
 - Melhor gerir os recursos de TI (aplicativos, informações, infraestrutura e pessoas).
- A Governança de TI habilita a organização a:
 - Obter todas as vantagens de sua informação;
 - Maximizar os benefícios;
 - Capitalizar as oportunidades;
 - Ganhar em poder competitivo.



- Existe uma diferença entre Governança e Gestão de TI:
 - “A gestão e a governança de TI possuem diferentes atribuições dentro do negócio. A governança de TI é responsável por definir como funcionam as coisas na TI e verificar se as normas e políticas estão sendo seguidas corretamente.
 - Já a gestão de TI é responsável por manter o desempenho de serviços, promover a transformação digital na empresa, manter a satisfação dos usuários e clientes dos serviços, além de fazer a gestão da equipe de TI.”
(<https://www.euax.com.br/2018/08/governanca-de-ti/>)
- Isso implica essencialmente em garantir que a TI faça certo as coisas certas, ou seja, padronizar os processos, definir como os serviços serão solicitados e atendidos, desenvolver projetos que deem um gás no desempenho da TI, mitigar os riscos possíveis e medir os resultados que a TI está entregando para o negócio.

- Para auxiliar nesse acompanhamento, existem padrões e frameworks que permitem a medição de desempenho de soluções e a adoção de boas práticas;
- Os mais adotados no mercado são:
 - ISO/IEC 27001 – gestão da segurança da informação;
 - ISO/IEC 20000 – gerenciamento de qualidade de serviços;
 - CMMI (Capability Maturity Model Integration) – melhores práticas para desenvolvimento de softwares;
 - TOGAF (The Open Group Architecture Framework) – abordagem para projeto;
 - PMBOK (Project Management Body of Knowledge) – melhores práticas de gerenciamento de projetos da PMI;
 - ITIL (Information Technology Infrastructure Library) – conjunto de boas práticas para gerenciamento de serviços de TI;
 - COBIT (Control Objectives for Information and Related Technology) – guia de boas práticas para gestão de TI.

- Dos padrões e frameworks listados estudaremos com mais detalhes a ISO/IEC 27000, ITIL e COBIT;
- Mais detalhes sobre os demais:
 - ISO/IEC 20000 (<https://www.kalendae.com.br/blog/iso-20000/>):

A ISO/IEC 20000 é uma norma técnica reconhecida em todo o mundo. Ela define uma série de requisitos obrigatórios baseados em um conjunto de boas práticas para que as empresas executem uma gestão dos serviços de TI de qualidade. Pode ser aplicada a empresas e profissionais. E ambos se beneficiam de ter a certificação, por ser uma forma de garantir a clientes e parceiros comerciais que o negócio mantém um bom conjunto de práticas para gerir os serviços de TI.

- Mais detalhes sobre os demais:
 - CMMI (Capability Maturity Model Integration):

É um modelo de referência que contém práticas (Genéricas ou Específicas) necessárias à maturidade no desenvolvimento de software. Desenvolvido pelo SEI (Software Engineering Institute), o CMMI é uma evolução do CMM e procura estabelecer um modelo único para o processo de melhoria corporativo, integrando diferentes modelos e disciplinas.

(<http://www.linhadecodigo.com.br/artigo/1401/cmmi-para-iniciantes.aspx>)
 - TOGAF (The Open Group Architecture Framework):

É um framework que ajuda a construir uma arquitetura de TI corporativa que oferece uma estrutura de alto nível para o desenvolvimento de software, permitindo organizar o processo de desenvolvimento por meio de uma abordagem sistemática que visa reduzir erros, manter cronogramas, manter o orçamento e alinhar a TI com as unidades de negócios para produzir resultados de qualidade.

(<https://cio.com.br/voce-sabe-o-que-e-o-togaf-e-como-ele-vem-sendo-atualizado/>)

- Mais detalhes sobre os demais:

- PMBOK (Project Management Body of Knowledge):

Consiste, na verdade, em uma padronização que identifica e conceitua processos, áreas de conhecimento, ferramentas e técnicas da gestão de projetos. As orientações desse guia não devem ser seguidas à risca, já que cada projeto possui características e especificidades que os diferenciam dos demais.

Ele é uma espécie de enciclopédia sobre gerenciamento de projetos publicada. Sua publicação é regularmente revisada pelo PMI (Project Management Institute - é uma instituição internacional sem fins lucrativos que associa profissionais de gestão de projetos).

Sua função é padronizar e difundir as práticas mais eficientes, testadas e comprovadas por gerentes de projetos do mundo inteiro em um só guia.

(<https://robsoncamargo.com.br/blog/PMBOK>)

- COBIT (Control Objectives for Information and Related Technology):
 - Atualmente está na versão 5 – COBIT 5;
 - Fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI, ou seja, auxilia as organizações a criar valor por meio da TI mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos;
 - Permite que a TI seja governada e gerida de forma holística para toda a organização, abrangendo o negócio de ponta a ponta bem como todas as áreas responsáveis pelas funções de TI, levando em consideração os interesses internos e externos relacionados com TI;
 - O COBIT 5 é genérico e útil para organizações de todos os portes, sejam comerciais, sem fins lucrativos ou públicas.

COBIT 5

Figura - 2: Princípios do COBIT 5



Fonte: COBIT 5 -
Modelo
Corporativo para
Governança e
Gestão de TI
da Organização

COBIT 5 – Governança e Gestão

- A visão do COBIT 5 sobre esta importante distinção entre governança e gestão é:
 - Governança: garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos.
 - Gestão: é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos.
- Juntos, esses cinco princípios permitem que a organização crie um modelo eficiente de governança e gestão otimizando os investimentos em tecnologia da informação e seu uso para o benefício das partes interessadas;

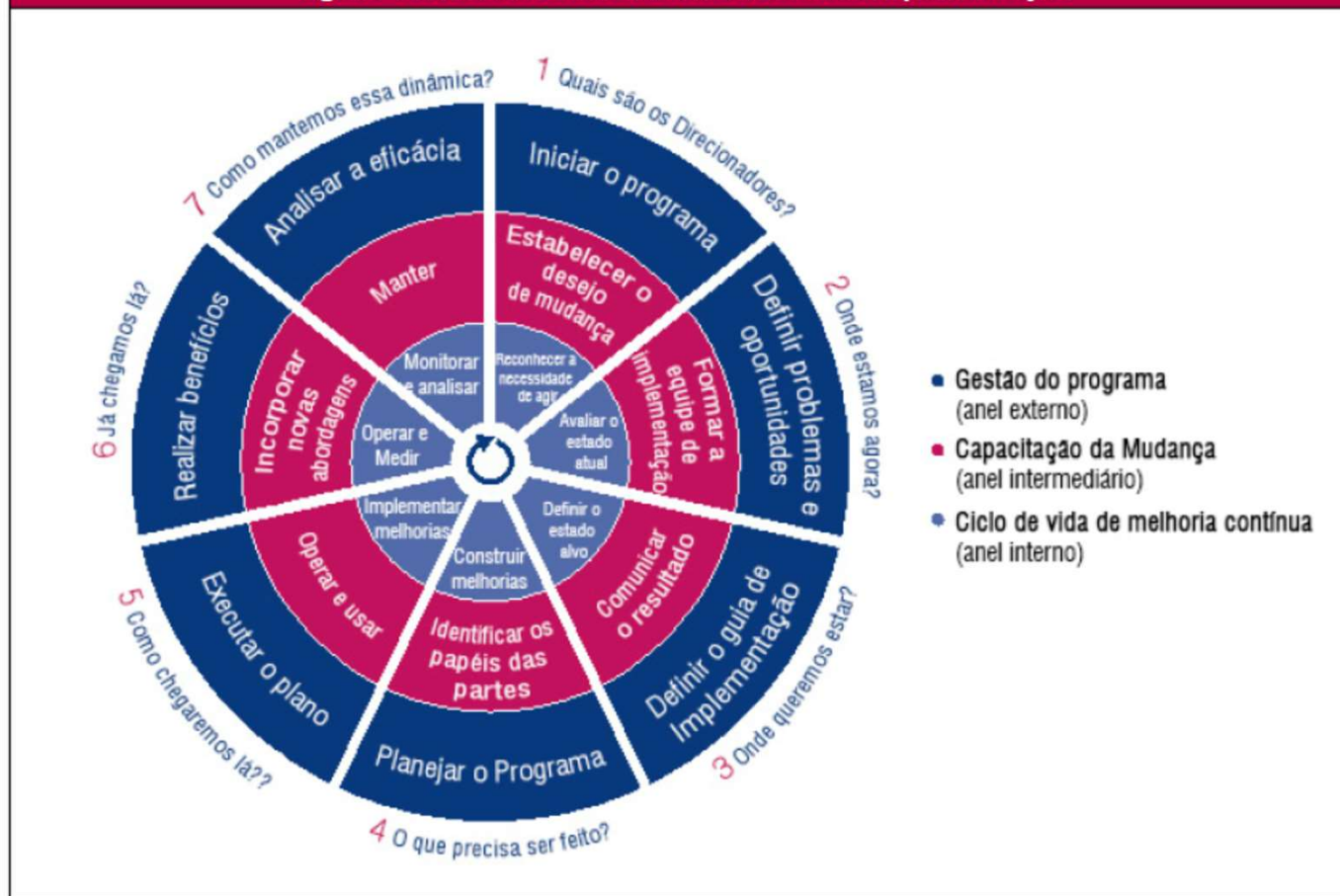
COBIT 5 - Implementação

- A visão do COBIT 5 sobre esta importante distinção entre governança e gestão é:
 - Governança: garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos.
 - Gestão: é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos.
- Juntos, esses cinco princípios permitem que a organização crie um modelo eficiente de governança e gestão otimizando os investimentos em tecnologia da informação e seu uso para o benefício das partes interessadas;

COBIT 5 - Implementação

Fonte: COBIT 5 -
Modelo
Corporativo para
Governança e
Gestão de TI
da Organização –
Capítulo 7

Figura - 17: As Sete Fases do Ciclo de Vida da Implementação



COBIT 5 - Implementação

- “A **1ª Fase** começa com o reconhecimento e aceitação da necessidade de uma implementação ou iniciativa de implementação: identificar os atuais pontos fracos e desencadeadores e cria um desejo de mudança nos níveis de gestão executiva;
- A **2ª Fase** concentra-se na definição do escopo da implementação ou da iniciativa de implementação usando o mapeamento dos objetivos corporativos do COBIT em objetivos de TI e nos respectivos processos de TI, e considerando também como os cenários de risco poderiam destacar quais os principais processos que se deve concentrar.
 - Diagnósticos de alto nível também podem ser úteis para definir o escopo e compreender as áreas com alta prioridade que se deve concentrar. Uma avaliação do estado atual é então realizada, e os problemas ou deficiências são identificados realizando-se uma avaliação da capacidade do processo.
 - Iniciativas em larga escala devem ser estruturadas como múltiplas interações do ciclo de vida - para qualquer iniciativa de implementação superior a seis meses há um risco de perda da dinâmica, foco e adesão das partes interessadas.”

Fonte: COBIT 5 - Modelo Corporativo para Governança e Gestão de TI da Organização – Capítulo 7

COBIT 5 - Implementação

- “Durante a **3ª Fase**, uma meta de melhoria é definida, seguida por uma análise mais detalhada, que alavanca a orientação do COBIT, a fim de identificar falhas e possíveis soluções. Algumas soluções podem apresentar resultados rápidos enquanto outras poderão exigir atividades mais desafiadoras em um prazo maior. Prioridade deve ser dada às iniciativas mais fáceis de alcançar e que provavelmente produzirão os melhores benefícios;
- A **4ª Fase** planeja soluções práticas através da definição de projetos apoiados por estudos de casos justificáveis. Um plano de mudança para a implementação também é desenvolvido nesta fase;
- As soluções propostas são implementadas na forma de práticas diárias na **5ª Fase**. Medições podem ser definidas e o monitoramento estabelecido com o uso das metas e indicadores do COBIT para garantir que o alinhamento da organização seja atingido e mantido e o desempenho possa ser medido. O sucesso exige demonstração de envolvimento e empenho pela alta administração, bem como a responsabilidade dos envolvidos das áreas de TI e de administração;”

Fonte: COBIT 5 - Modelo Corporativo para Governança e Gestão de TI da Organização – Capítulo 7

COBIT 5 - Implementação

- “A **6ª Fase** concentra-se na operação sustentável dos habilitadores novos ou aperfeiçoados e no monitoramento do atingimento dos benefícios esperados;
- Durante a **7ª Fase**, o sucesso da iniciativa como um todo é analisado, novos requisitos para a governança ou gestão de TI da organização são identificados e a necessidade de melhoria contínua é reforçada.
- Com o tempo, o ciclo de vida deve ser seguido de forma interativa paralelamente à criação de uma abordagem sustentável para a governança e gestão de TI da organização.”

Fonte: COBIT 5 - Modelo Corporativo para Governança e Gestão de TI da Organização – Capítulo 7

COBIT 5 – Questões de Concurso

- Concurso: 2019 - FCC - Tribunal Regional Federal da 3ª Região (TRF 3) - Técnico Judiciário

Entre as ferramentas ordinariamente utilizadas na gestão de projetos pelas organizações, pode-se citar o COBIT, que:

- (a) mapeia todas as etapas envolvidas nos projetos prioritários da organização e aponta aquelas que podem ser suprimidas com vistas à redução do tempo de execução.
- (b) é uma metodologia para elaboração do planejamento estratégico da companhia e alocação dos projetos de acordo com sua aderência às metas estabelecidas.
- (c) corresponde a um diagrama de causa e efeito (inputs e outputs) presentes nos principais projetos da organização.
- (d) consiste em um guia de melhores práticas utilizado na gestão de tecnologia da informação, que permite identificar quais projetos possuem maiores chances de sucesso.
- (e) avalia os diferentes cenários probabilísticos dos riscos envolvidos na execução de projetos e apresenta ações de mitigação.

COBIT 5 – Questões de Concurso

- Concurso: 2019 – CESPE – CGE/CE - Auditor de Controle Interno - TI

Com base no COBIT 5, julgue os itens a seguir e assinale a opção correta:

I. Existe, no domínio Avaliar, Dirigir e Monitorar, processo destinado a garantir que desempenho, medição e relatórios de conformidade da TI corporativa sejam transparentes às partes interessadas.

II. Para cada habilitador no COBIT, é possível definir um conjunto específico de metas relevantes para apoiar os objetivos de TI.

III. A gestão, diferentemente da governança, visa garantir que as necessidades das partes interessadas sejam avaliadas a fim de determinar objetivos corporativos.

- (a) Apenas o item I está certo.
- (b) Apenas o item III está certo.
- (c) Apenas os itens I e II estão certos.
- (d) Apenas os itens II e III estão certos.
- (e) Todos os itens estão certos.

COBIT 5 – Questões de Concurso

- Concurso: 2019 - CESPE - TCE RO - Analista de TI - Desenvolvimento de Sistemas

O COBIT possui um amplo conjunto de conceitos e elementos utilizados na boa governança de tecnologia da informação. Entre eles, destacam-se os princípios, os processos, as estruturas, a cultura, a informação, os serviços e as pessoas. Estes compõem o conceito de:

- (a) objetivos da governança de TI.
- (b) cascata de objetivos do COBIT.
- (c) dimensões dos habilitadores do COBIT.
- (d) habilitadores corporativos do COBIT.
- (e) papéis, atividade e relacionamentos do COBIT.

COBIT 5 – Questões de Concurso

- Concurso: 2019 - FCC - Tribunal Regional Federal da 3ª Região (TRF 3) - Técnico Judiciário

Entre as ferramentas ordinariamente utilizadas na gestão de projetos pelas organizações, pode-se citar o COBIT, que:

- (a) mapeia todas as etapas envolvidas nos projetos prioritários da organização e aponta aquelas que podem ser suprimidas com vistas à redução do tempo de execução.
- (b) é uma metodologia para elaboração do planejamento estratégico da companhia e alocação dos projetos de acordo com sua aderência às metas estabelecidas.
- (c) corresponde a um diagrama de causa e efeito (inputs e outputs) presentes nos principais projetos da organização.
- (d) consiste em um guia de melhores práticas utilizado na gestão de tecnologia da informação, que permite identificar quais projetos possuem maiores chances de sucesso.
- (e) avalia os diferentes cenários probabilísticos dos riscos envolvidos na execução de projetos e apresenta ações de mitigação.

COBIT 5 – Questões de Concurso

- Concurso: 2019 – CESPE – CGE/CE - Auditor de Controle Interno - TI

Com base no COBIT 5, julgue os itens a seguir e assinale a opção correta:

I. Existe, no domínio Avaliar, Dirigir e Monitorar, processo destinado a garantir que desempenho, medição e relatórios de conformidade da TI corporativa sejam transparentes às partes interessadas.

II. Para cada habilitador no COBIT, é possível definir um conjunto específico de metas relevantes para apoiar os objetivos de TI.

2019

III. A gestão, diferentemente da governança, visa garantir que as necessidades das partes interessadas sejam avaliadas a fim de determinar objetivos corporativos.

- (a) Apenas o item I está certo.
- (b) Apenas o item III está certo.
- (c) Apenas os itens I e II estão certos.**
- (d) Apenas os itens II e III estão certos.
- (e) Todos os itens estão certos.

COBIT 5 – Questões de Concurso

- Concurso: 2019 - CESPE - TCE RO - Analista de TI - Desenvolvimento de Sistemas

O COBIT possui um amplo conjunto de conceitos e elementos utilizados na boa governança de tecnologia da informação. Entre eles, destacam-se os princípios, os processos, as estruturas, a cultura, a informação, os serviços e as pessoas. Estes compõem o conceito de:

- (a) objetivos da governança de TI.
- (b) cascata de objetivos do COBIT.
- (c) dimensões dos habilitadores do COBIT.
- (d) habilitadores corporativos do COBIT.**
- (e) papéis, atividade e relacionamentos do COBIT.