Apostila

COBIT 5

Framework de Governança e Gestão Corporativa de TI

Luzia Dourado

Maio, 2014

Caros concurseiros!

Eis que disponibilizo mais uma versão da apostila de COBIT 5 para auxiliar nos estudos! Devido a grande procura por este material (mais de 2900 downloads☺), resolvi revisá-lo e incrementá-lo com informações que possam facilitar o entendimento desse assunto.

Vale lembrar que este material pode auxiliar também aqueles que buscam obter a certificação. Espero que seja útil!!!

Bons estudos a todos! Deus os abençoe!

Força, Foco e FÉ!

Luzia Dourado.

lmdourado@hotmail.com

Sumário

INTRODUÇÃO

Antes de introduzirmos os conceitos e detalhes do framework COBIT 5, é necessária a definição de conceito de governança e gestão corporativa de TI.

Mas o que é Governança Corporativa de TI?

A norma ISO/IEC 38500, que estabelece um modelo para a Governança Corporativa de TI no qual o COBIT 5 se baseia, define **Governança Corporativa de TI** como:

"O sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. A governança corporativa de TI envolve a avaliação e a direção do uso da TI para dar suporte à organização no alcance de seus objetivos estratégicos e monitorar seu uso para realizar os planos. A governança inclui a estratégia e as políticas para o uso de TI dentro de uma organização."[1].

A norma orienta que os diretores da organização governem a TI por meio de três tarefas principais:

- Avaliar o uso atual e futuro da TI;
- Orientar a preparação e a implementação de planos e políticas para garantir que o uso da TI atenda aos objetivos do negócio;
- Monitorar o cumprimento das políticas e o desempenho em relação aos planos.

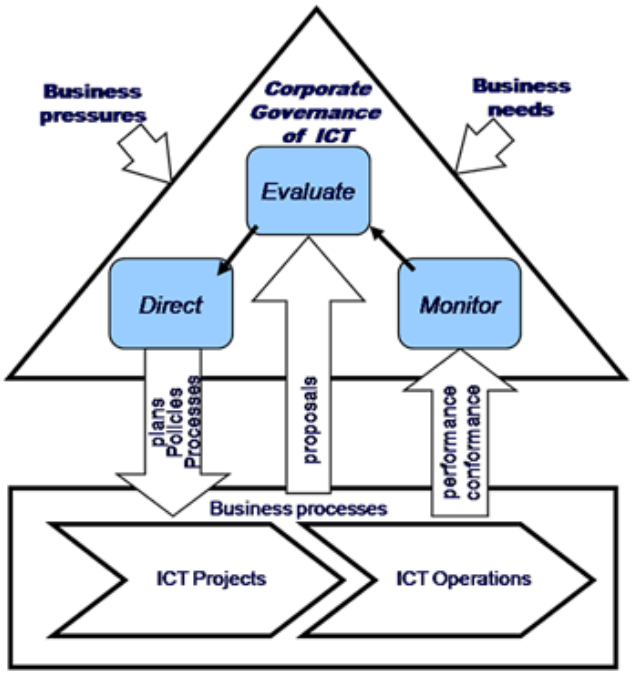

Figura 1 - Modelo de governança corporativa de TI. Fonte: ISO/IEC 38500, pág. 13

Segundo a norma, Avaliar (***Evaluate***) significa que os diretores devem avaliar o uso atual e futuro da TI, incluindo as estratégias, propostas e arranjos de fornecimento (interno, externo ou ambos).

Dirigir (***Direct***) significa que os diretores devem atribuir responsabilidades para a preparação e implementação dos planos e políticas que estabelecem o direcionamento dos investimentos nos projetos e operações de TI.

Monitorar (***Monitor***) significa que os diretores devem monitorar o desempenho da TI por meio de sistemas de mensuração apropriados, garantindo que esse desempenho esteja de acordo com os planos e objetivos de negócio e que a TI esteja em conformidade com as obrigações externas e práticas internas de trabalho.

Governança de TI e Gestão de TI não é a mesma coisa?

A governança corporativa de TI não pode ser confundida com o conceito de gestão de TI. A governança corporativa de TI está inserida na governança corporativa da organização e é dirigida por esta, e busca o direcionamento da TI para atender ao negócio e o monitoramento para verificar a conformidade com o direcionamento tomado pela administração da organização [2]. **A governança corporativa de TI não é de responsabilidade exclusiva dos gestores de TI e, sim, da alta administração (*board*).**

A **Gestão de TI**, conforme definido pela ISO/IEC 38500 é o **sistema de controles e processos necessários para alcançar os objetivos estratégicos estabelecidos pela direção da organização** [1]. A gestão de TI implica a utilização sensata de meios (recursos, pessoas, processos, práticas) pra alcançar um objetivo. Atua no planejamento, construção, organização e controle das atividades operacionais e se alinha com a direção definida pela organização.

Portanto, a gestão controla tarefas operacionais, enquanto a governança controla a gestão.

Finalmente, o que é o COBIT 5?

O **COBIT 5**, desenvolvido e difundido pelo ISACA (Information System Audit and Control) e lançado no final de 2012, **é um framework de governança e gestão corporativa de TI**.

O framework faz a **integração do conteúdo dos principais frameworks** publicados pelo ISACA: COBIT 4.1; Val IT; Risk IT; Business Model for Information Security (BMIS); IT Assurance Framework (ITAF); Taking Governance Forward (TGF); e Board Briefing on IT Governance 2nd Edition.

Além disso, ele se alinha a outros padrões de mercado como Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO), Body Project Management of Knowledge (PMBOK), PRINCE2 e The Open Group Architecture Framework (TOGAF).

O COBIT 5 ajuda as organizações a **criar valor para TI**, **mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos.** Tem como objetivos:

- oferecer um framework abrangente que auxilia as organizações a otimizar o valor gerado pela TI;
- permitir que a TI seja governada e gerenciada de forma holística para toda a organização.
- criar uma linguagem comum entre TI e negócios para a governança e gestão de TI corporativa.

Mas quais são os benefícios do COBIT 5 para as organizações?

COBIT 5 ajuda as organizações de todos os tamanhos a:

- ✓ Manter informações de alta qualidade para suportar as decisões de negócios;
- ✓ Gerar "valor" dos investimentos em TI, ou seja, atingir metas estratégicas e entregar benefícios de negócio por meio do efetivo uso da TI;
- ✓ Atingir a excelência operacional por meio da aplicação confiável e eficiente da tecnologia;
- ✓ Manter riscos relacionados com a TI em um nível aceitável;
- ✓ Otimizar o custo de serviços de TI;
- ✓ Manter a conformidade com leis, regulamentos, acordos contratuais e políticas.

Como esses benefícios podem ser obtidos a fim de criar valor para os stakeholders (partes interessadas) das organizações?

A **entrega de valor** para os stakeholders **requer uma boa governança e gestão** dos ativos de informação e de tecnologia. **Para se obter essa governança, os Conselhos de administração, executivos e gestores devem tratar a TI como qualquer outra parte significante do negócio.**

Além disso, os requisitos legais, regulatórios e contratuais relacionados ao uso da TI pelas organizações têm aumentado, de modo que a TI também poderá ser uma ameaça caso não funcione propriamente.

Portanto, COBIT 5 provê um framework que auxilia as organizações a atingirem suas metas e entregar valor por meio de uma efetiva governança e gestão da TI corporativa [3].

PRINCIPAIS NOVIDADES DO COBIT 5

A principal novidade do COBIT 5 é que ele está **focado** em **governança corporativa de TI**, **deixando claro a distinção entre governança e gestão**, a fim de se aumentar a utilização corporativa deste framework, **ressaltando o papel da alta administração nas tomadas de decisões de TI.**

O novo framework é fundamentado em **5 princípios** de governança corporativa de TI **que permitem que a organização construa um framework efetivo de governança e gestão de**

TI baseado em um conjunto holístico de **7 enablers**[1] **(ou viabilizadores) que otimizam investimentos em tecnologia e informação utilizados para o benefício dos stakeholders**.

COBIT 5 se tornou uma família de produtos, ou seja, as informações referentes ao framework (COBIT 5) está em uma publicação separada da que contém as informações relativas aos processos (***COBIT 5: Enabling Process***), além de conter outras publicações relativas à implementação, segurança da informação, riscos, qualidade, dentre outros. A publicação referente ao framework é disponibilizada de forma gratuita mediante cadastro prévio no site da ISACA, porém a publicação *COBIT 5: Enabling Process* é paga para quem não é membro da ISACA.

A publicação COBIT 5 (framework) é o principal produto da família, contendo:

- ✓ Sumário Executivo
- ✓ Componentes e estruturas
- ✓ 5 princípios, em que cada princípio é descrito em um capítulo
- ✓ Visão dos 7 viabilizadores e suas dimensões
- ✓ Cascata de objetivos (*COBIT 5 Goals Cascade*)
- ✓ Modelo de Referência de Processos
- ✓ Introdução ao Guia de Implementação
- ✓ Modelo de Capacidade de Processos

A publicação ***COBIT 5: Enabling Process*** **descreve os processos, objetivos e métricas, matriz RACI, práticas de gestão com suas entradas, saídas e atividades de forma mais organizada em formato de tabela, facilitando a leitura**. Ao final de cada processo, há uma seção denominada *Related Guidance* que associa cada processo do COBIT com outros frameworks que podem ser utilizados para implementar o processo.

A distinção ente governança e gestão pode ser percebida no Modelo de Referência de Processos, que **subdivide os 37 processos de TI em** duas principais áreas de atividade – **governança e gestão** – que são divididas em domínios de processos. Os **5 processos de governança** compõem o domínio **Avaliar, dirigir e monitorar (EDM)** e os **32 processos de gestão** compõem os 4 domínios:

- **Alinhar, Planejar e Organizar (APO);**
- **Construir, Adquirir e Implementar (BAI);**
- **Entregar, Servir e Suportar (DSS) e**
- **Monitorar, Avaliar e Medir (MEA).**

[1] Enabler = viabilizador, facilitador, habilitador

EVOLUÇÃO DO COBIT 5

O COBIT começou, em 1996, como um framework para auditoria e controles de TI, com foco nos objetivos de controle. Depois, em 2000, foi lançada a terceira versão com a inclusão de orientações para a gestão de TI. Em 2005, com o COBIT 4.0, se tornou o framework de governança de TI, com a inclusão de processos de governança e *compliance* (conformidade). E atualmente, na quinta versão, é o framework integrador de governança e gestão de TI corporativa.

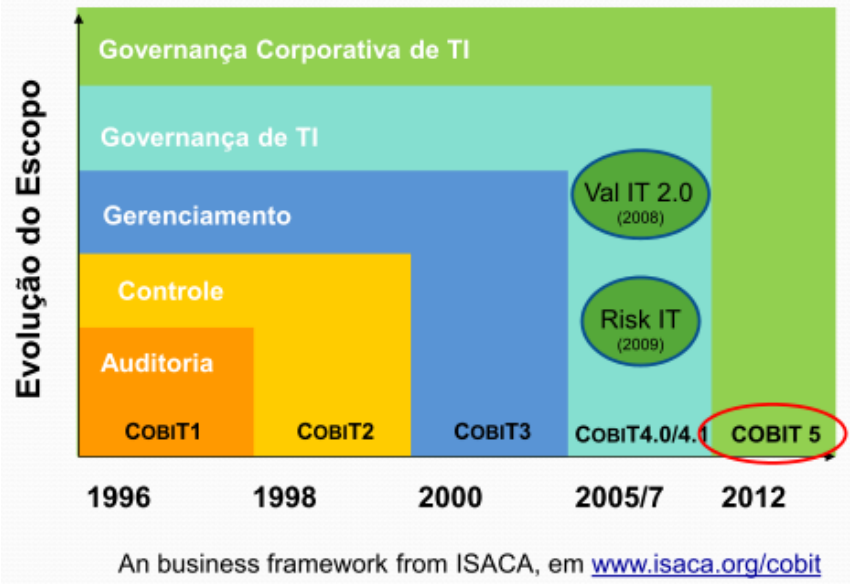

Figura 2 - Evolução do COBIT

PRINCÍPIOS DO COBIT 5

O framework baseia-se em 5 princípios:

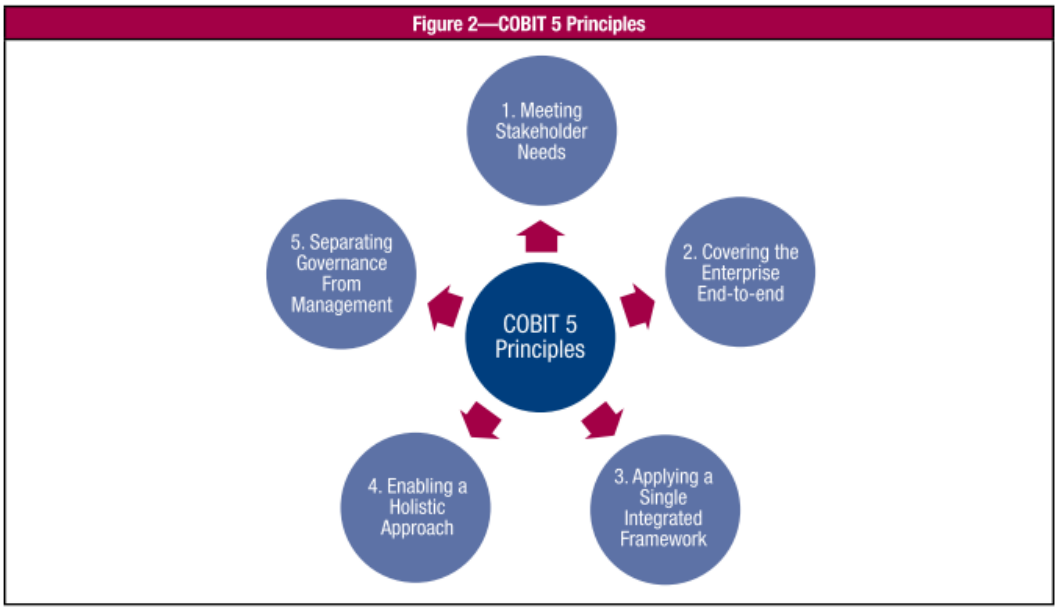

Figura 3 – Princípios do COBIT 5 Fonte: COBIT ® 5, Figura 2, ©2012 ISACA®

1. Atender as necessidades dos stakeholders
2. Cobrir a organização de ponta a ponta
3. Aplicar um framework único e integrado
4. Possibilitar uma abordagem holística
5. Separar a governança da gestão

A seguir segue a descrição de cada princípio:

Princípio 1. Atender as necessidades dos stakeholders

As organizações existem para criar valor para os stakeholders, ou seja, para todas as partes interessadas (acionistas, auditores, fornecedores, consultores, alta administração, etc).

O que é criação de valor?

A **criação de valor** significa **obter benefícios por meio da otimização do uso de recursos e dos riscos a um nível aceitável**. Esse é o objetivo da governança! Para cada stakeholder, a criação de valor pode representar interesses diferentes e algumas vezes conflitantes.

O sistema de governança abrange negociar e decidir entre os diferentes interesses dos stakeholders e deve considerar a opinião de todos quando são tomadas decisões sobre os benefícios, recursos e avaliação dos riscos.

Para cada decisão de governança, as seguintes questões podem e devem ser feitas:

- Quem recebe os benefícios?
- Quem assume os riscos?
- Quais são os recursos necessários?

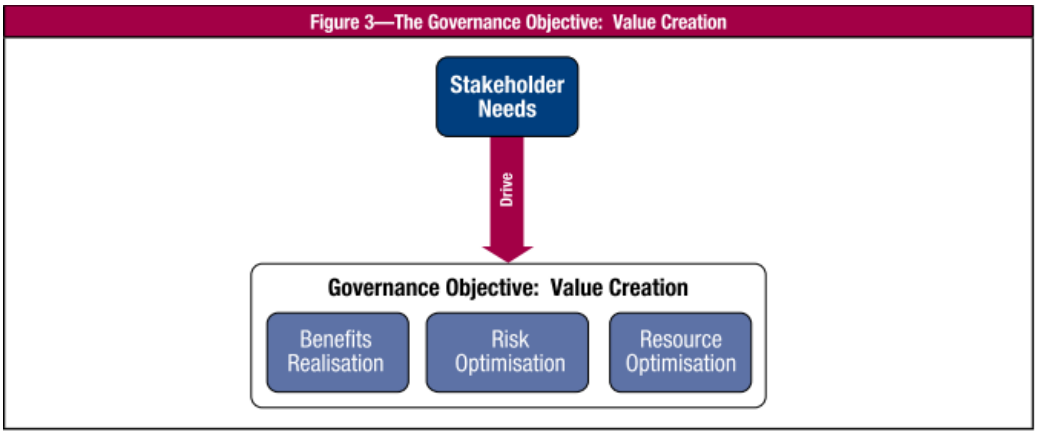

Figura 4 - Objetivo da Governança
Fonte: COBIT ® 5, Figura 3, ©2012 ISACA®

As necessidades dos stakeholders precisam ser transformadas em estratégias corporativas. **Por isso, este princípio está intimamente alinhado com o conceito de alinhamento estratégico entre TI e negócio**.

Para isso, há um mecanismo denominado ***COBIT 5 Goals Cascade*** (cascata de objetivos) com a finalidade de desdobrar:

- os drivers (direcionadores ou motivadores) e as necessidades dos stakeholders em objetivos de negócio;

- os objetivos de negócio em objetivos de TI;

- os objetivos de TI em objetivos para os viabilizadores.

Vale ressaltar que a cascata de objetivos não é algo novo no COBIT 5, pois já existia no COBIT 4.1.

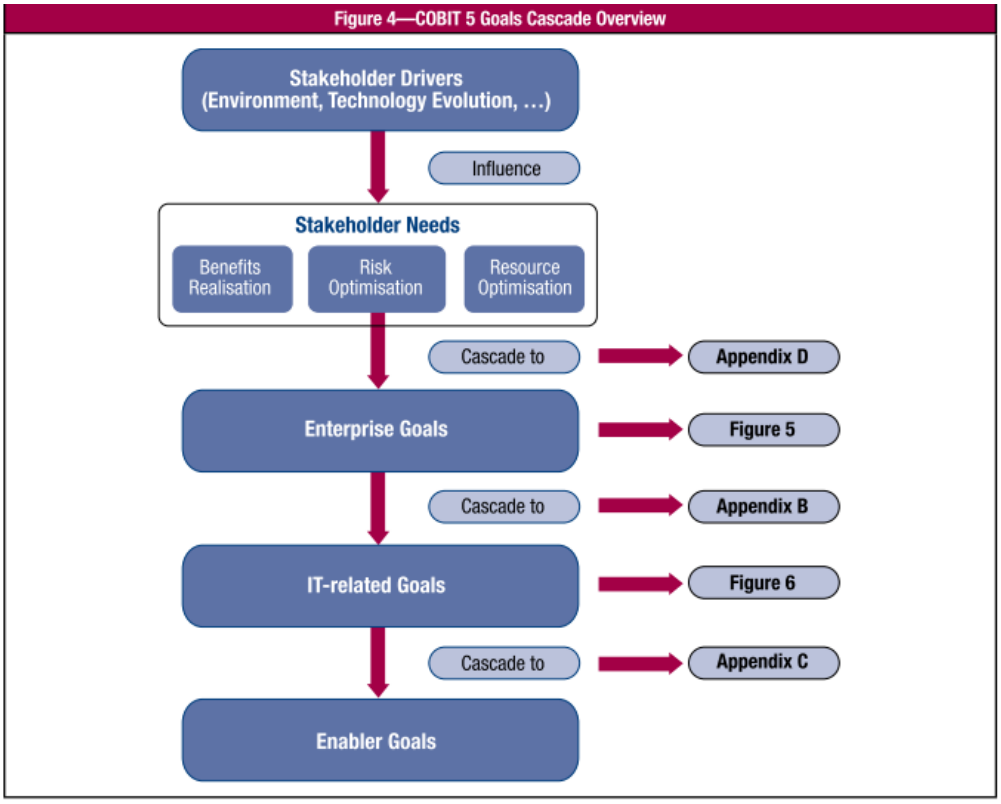

Figura 5 - Cascata de Objetivos
Fonte: COBIT ® 5, Figura 4, ©2012 ISACA®

Em uma visão *bottom-up*, a cascata de objetivos auxilia a organização em como empregar os viabilizadores para alcançar os objetivos de negócio de forma mais concreta.

Que benefícios são obtidos por meio dessa cascata de objetivos?

A cascata de objetivos permite a definição de prioridades para implementação, aprimoramento e garantia de governança corporativa de TI, com base em objetivos estratégicos e riscos relacionados. Na prática, a cascata de objetivos:

- Define objetivos tangíveis e relevantes em vários níveis;
- Filtra a base de conhecimento do COBIT com base nos objetivos de negócio relevantes para implementação;
- Identifica e comunica claramente como os viabilizadores do COBIT (às vezes muito operacionais) são importantes para o alcance dos objetivos de negócio.

Mais detalhes sobre o ***COBIT 5 Goals Cascade*** pode ser visto no Anexo I.

Princípio 2. Cobrir a organização de ponta a ponta

O COBIT 5 trata a governança e gestão de TI cobrindo a organização de ponta a ponta. Isso significa que o COBIT 5 [3]:

- ✓ Integra a governança corporativa de TI dentro da governança corporativa;
- ✓ **Cobre todas as funções e processos requeridos dentro da organização;**
- ✓ **Não foca apenas nas funções de TI**, mas trata a informação e tecnologia relacionadas como ativos que precisam ser tratados como qualquer outro ativo por todos na organização.

Por meio desse princípio, **os gestores de negócio têm a responsabilidade de tratar a TI como um ativo estratégico**, gerenciando a TI da mesma forma como gerenciam os outros ativos da organização.

Sistema de Governança

Para que a governança cubra a organização de ponta a ponta, o sistema de governança possui os seguintes componentes:

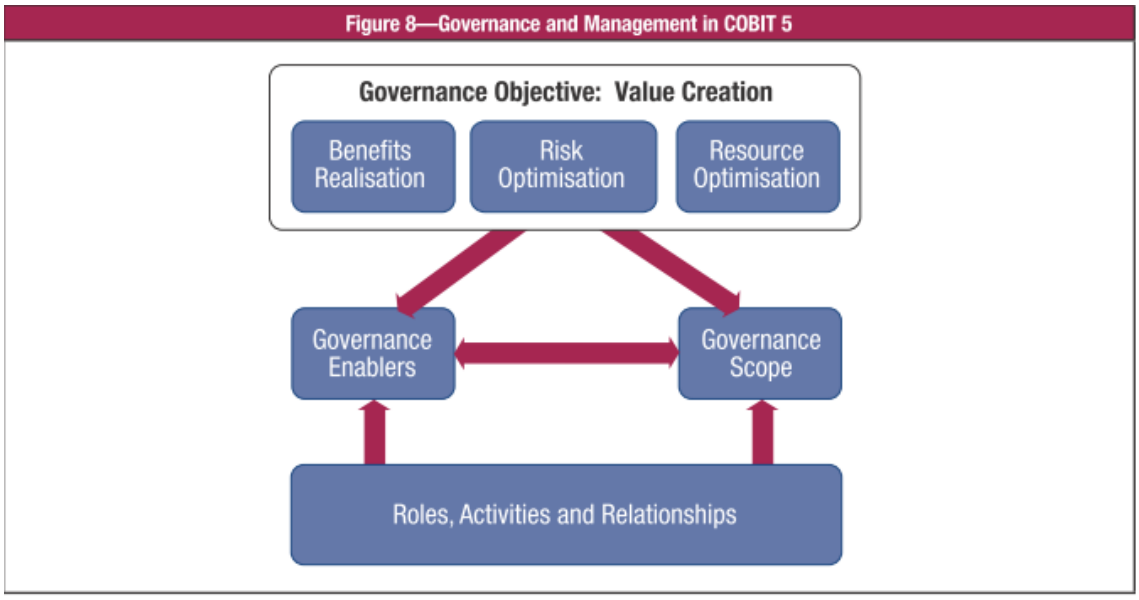

Figura 6 - Governança de Gestão Fonte: COBIT ® 5, Figura 8, ©2012 ISACA®

- ➢ **Viabilizadores da governança**: são os recursos organizacionais usados na governança como princípios, estruturas, processos e práticas.
- ➢ **Escopo da governança**: área em que será aplicada a governança (toda a organização ou só uma parte).
- ➢ **Papéis, Atividades e Relacionamentos**: define quem está envolvido com governança, como são envolvidos, o que fazem e como interagem dentro do escopo da governança.

A figura abaixo mostra os papéis, atividades e relacionamentos que ocorrem na governança. Os stakeholders (partes interessadas) delegam para o corpo de governança estabelecer uma direção para as atividades de gestão que, por sua vez, instrui e alinha as operações de TI da organização. Os executores (parte operacional da organização) reportam o resultado de suas atividades para a gestão que é monitorada pelo corpo de governança que presta contas do desempenho para os stakeholders.

Vale ressaltar que o COBIT 5 fornece, para cada processo, matrizes RACI de responsabilidade, em que estão incluídos papeis relacionados a TI e ao negócio.

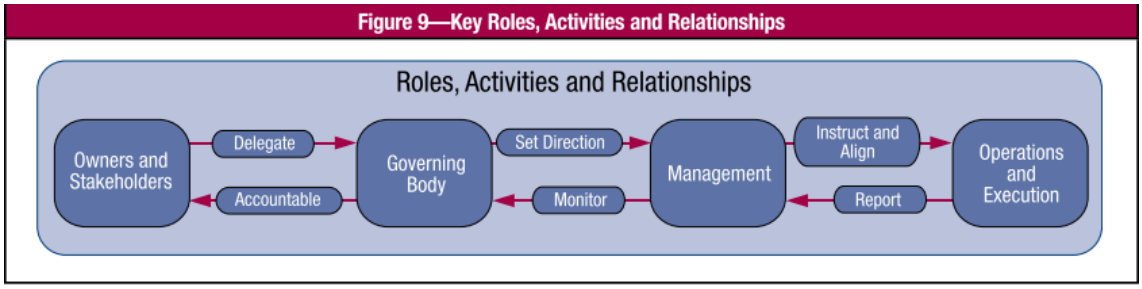

Figura 7 - Papéis, Atividades e Relacionamentos. Fonte: COBIT ® 5, Figura 8, ©2012 ISACA®

Princípio 3. Aplicar um framework único e integrado

COBIT 5 é uma estrutura única e integrada, porque integra todos os conhecimentos anteriormente dispersos em diferentes frameworks da ISACA, tais como o COBIT 4.1, Val IT (valor de TI para o negócio), Risk IT (risco relacionado ao uso de TI), BMIS (segurança). Está alinhado com os mais atuais e relevantes padrões e frameworks utilizados [3]:

- de gestão corporativa: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000;
- Relacionados a TI: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOK/PRINCE2, CMMI etc.

Isso permite à organização utilizar o COBIT 5 como um integrador dos frameworks de governança e de gestão.

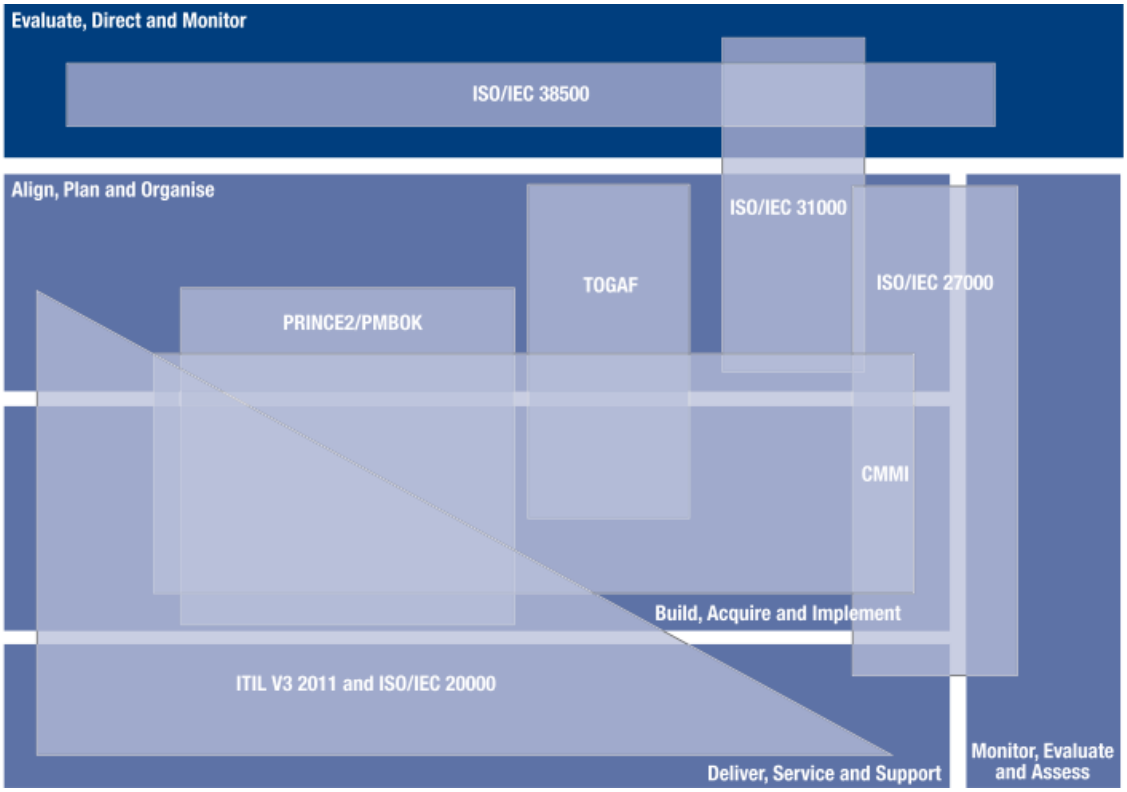

Figura 8 - Padrões cobertos pelo COBIT 5. Fonte: COBIT ® 5, Figura 25, ©2012 ISACA®

A família de produtos do COBIT 5 inclui os seguintes produtos [4]:

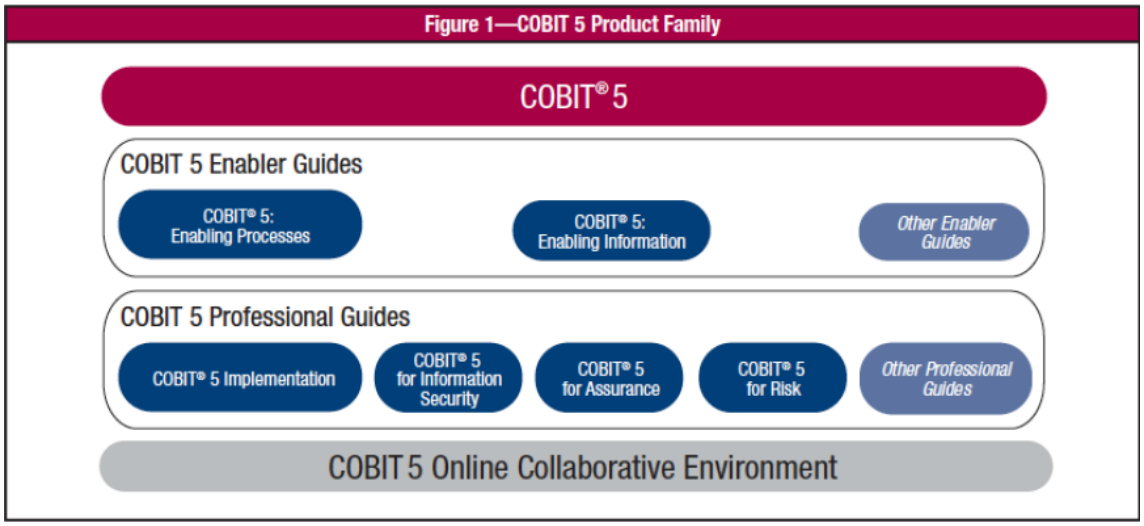

Figura 9 - Família de Produtos Fonte: COBIT ® 5, Figura 1, ©2012 ISACA®

- COBIT 5 (o framework)
- *COBIT 5 Enabler Guides*, no qual os viabilizadores de governança e gestão são discutidos em detalhe. Estes incluem:
  - *COBIT 5: Enabling Processes*
  - *COBIT 5: Enabling Information*
  - Outros guias enabler
- *COBIT 5 Professional Guides*, que incluem:
  - *COBIT 5 Implementation*
  - *COBIT 5 for Information Security*

- *COBIT 5 for Assurance*
- *COBIT 5 for Risk*
- Outros guias profissionais

Princípio 4. Possibilitar uma abordagem holística

Para apoiar a governança e a gestão de TI utilizando uma abordagem que engloba a organização como um todo, incluindo seus componentes e suas inter-relações, o COBIT 5 define um conjunto de **7 viabilizadores.**

Viabilizadores (enablers)

Viabilizadores são fatores que, individual e coletivamente, influenciam o funcionamento da governança e gestão corporativa de TI [2].

O framework COBIT 5 define 7 categorias de viabilizadores:

1. Princípios, políticas e frameworks: são os veículos que traduzem o comportamento desejado em um guia prático para a gestão cotidiana;

2. Processos: descreve um conjunto organizado de práticas e atividades para atingir certos objetivos e produzir um conjunto de saídas que auxiliem no cumprimento das metas relacionadas a TI;

3. Estruturas organizacionais: são as entidades-chave, responsáveis pela tomada de decisão em uma organização;

4. Cultura, ética e comportamento: dos indivíduos e da organização; muito frequentemente é subestimada como um fator de sucesso nas atividades de governança e gestão;

5. Informação: está difundida por toda organização. Representa todas as informações produzidas e utilizadas pela organização. É imprescindível para manter a organização em funcionamento e bem governada;

6. Serviços, infraestrutura e aplicações: inclui a infraestrutura, tecnologia e aplicações que fornecem à organização os serviços de TI;

7. Pessoas, habilidades e competências: está relacionado com as pessoas e são requeridas para que as atividades sejam executadas com sucesso e para que decisões e ações corretivas sejam realizadas de forma correta.

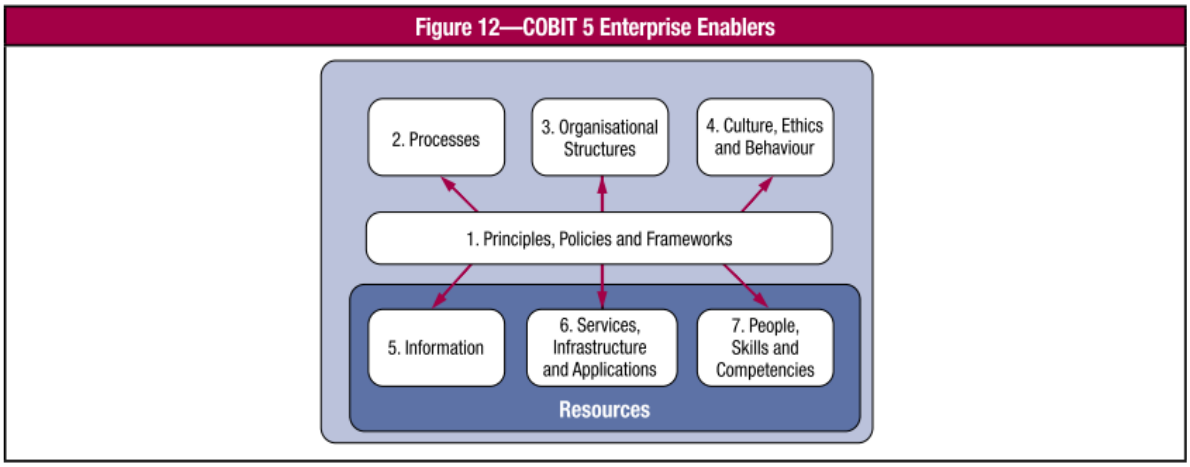

Figura 10 - Viabilizadores. Fonte: COBIT ® 5, Figura 12, ©2012 ISACA®

Alguns viabilizadores do COBIT 5 eram tratados no COBIT 4.1:

- Os recursos de TI do COBIT 4.1 – processos, aplicações, informação e infra-estrutura – são considerados viablilizadores no COBIT 5.
- O viabilizador 1.Princípios, políticas e estruturas foi mencionado em alguns processos do COBIT 4.1.
- O viabilizador 2.Processos foi fundamental para o uso no COBIT 4.1.
- O viabilizador 3.Estruturas organizacionais estava implícito, através dos papéis responsável, consultado ou informado na matriz RACI.
- O viabilizador 4.Cultura, ética e comportamento foi mencionado em alguns processos do COBIT 4.1.

Dimensões de viabilizadores

Todos os viabilizadores têm um conjunto de dimensões comuns. Este conjunto de dimensões comuns [4]:

- Fornece uma maneira comum, simples e estruturada para lidar com viabilizadores;
- Permite que a organização gerencie suas interações complexas;
- Facilita resultados bem sucedidos dos viabilizadores.

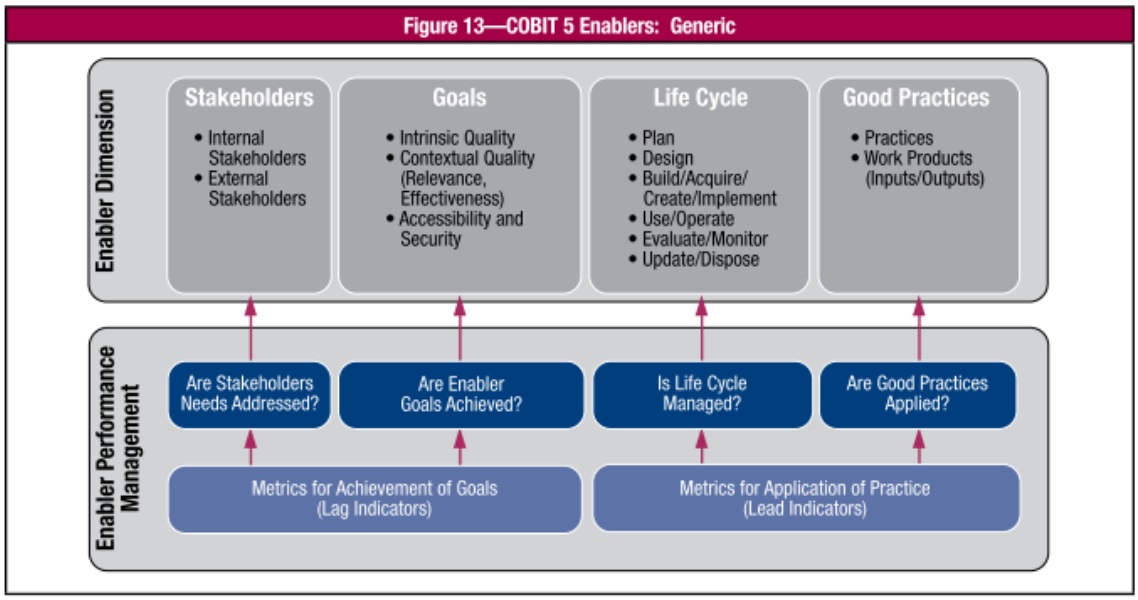

Figura 11 - Dimensões de Viabilizadores. Fonte: COBIT ® 5, Figura 13, ©2012 ISACA®

As quatro dimensões comuns para viabilizadores são:

- **Stakeholders**: cada viabilizador tem stakeholders (partes que desempenham um papel ativo e/ou têm interesse na execução). Por exemplo, os processos têm diferentes partes que executam atividades de processo e/ou que têm interesse no resultado do processo; estruturas organizacionais têm partes, cada uma com seus próprios papéis e interesses, que fazem parte da estrutura.
  Os stakeholders podem ser internos ou externos à organização, todos com seus interesses e necessidades.
  - Exemplos de stakeholders internos: executivos de negócio, conselho de administração, gerentes de negócio, auditores internos, usuários de TI, etc.
  - Exemplo de stakeholders externos: parceiros comerciais, fornecedores, governo, consumidores, auditores externos, consultores, etc.
- **Objetivos (*goals*)**: cada viabilizador tem uma série de objetivos e fornece valor pela realização destes objetivos.
  Os objetivos podem ser definidos em termos de:
  - Resultados esperados do viabilizador
  - Aplicação ou operação do próprio viabilizador

  Os objetivos de viabilizadores são o passo final da cascata de objetivos do COBIT 5. Os objetivos são divididos em categorias:
  - Qualidade intrínseca: medida em que viabilizadores funcionam com precisão, objetividade e fornecem informações precisas e objetivas.
  - Qualidade contextual: medida em que viabilizadores e seus resultados atendem ao propósito, dado o contexto em que operam.
  - Acessibilidade e segurança: medida em que viabilizadores e seus resultados são acessíveis e seguros.
- **Ciclo de vida (life cycle):** cada viabilizador tem um ciclo de vida, ou seja, é definido, criado, operado, monitorado e ajustado/atualizado ou aposentado.

  As fases do ciclo de vida consistem em:

- ✓ Planejar (inclui o desenvolvimento de conceitos e seleção de conceitos)
- ✓ Projetar
- ✓ Construir/adquirir/criar/implementar
- ✓ Utilizar/operar
- ✓ Avaliar/monitor
- ✓ Atualizar/eliminar

➢ **Boas práticas (good practices):** para cada um dos viabilizadores, boas práticas podem ser definidas. Boas práticas apoiam a realização dos objetivos do viabilizador. Boas práticas fornecem exemplos ou sugestões sobre a melhor forma de implementar o viabilizador, e quais os produtos de trabalho, entradas e saídas são necessários.

Gerenciamento de Desempenho dos Viabilizadores (Enabler Performance Management)

As organizações esperam resultados positivos a partir da aplicação e utilização dos viabilizadores. Para gerenciar o desempenho dos viabilizadores, as seguintes questões terão de ser monitoradas e respondidas, com base em métricas:

- As necessidades dos stakeholders foram atendidas?
- Os objetivos dos viabilizadores foram alcançados?
- O ciclo de vida do viabilizador é gerenciado?
- As boas práticas são aplicadas?

As duas primeiras questões lidam com o resultado real do viabilizador e as métricas usadas para **medir se os objetivos foram atingidos** podem ser chamadas de "indicadores de resultado" (***lag indicators***). As duas últimas lidam com o funcionamento real do viabilizador e as métricas para **medir se os objetivos serão atingidos** podem ser chamadas de "indicadores de desempenho" (***lead indicators***).

Como exemplo de um viabilizador na prática, veja no Anexo II.

Princípio 5. Separar a governança de gestão

COBIT 5 torna clara a distinção entre governança e gestão. Essas duas áreas abrangem diferentes tipos de atividades, exigem diferentes estruturas organizacionais e servem a propósitos diferentes.

A **governança** assegura que as necessidades, as condições e as opções dos stakeholders sejam **avaliadas** para determinar os objetivos de negócio a serem alcançados; define a **direção** por meio de priorização e tomada de decisão; e provê **monitoramento** de desempenho e conformidade com relação aos objetivos.

Na governança, são discutidos e aprovados as políticas e os **planos de alinhamento estratégico** (PE, PETI), a implementação de processos e os mecanismos de controle que direcionarão a gestão da TI [5].

Na maioria das organizações, **a governança é de responsabilidade do Conselho de Administração (ou Corpo Diretivo)**, sob a liderança do presidente. Responsabilidades de governança específicas podem ser delegadas a estruturas organizacionais especiais em um nível apropriado, especialmente em organizações maiores e complexas.

A **gestão** consiste em **planejar, construir, executar e monitorar** atividades alinhadas com a direção estratégica estabelecida pela governança para atingir os objetivos de negócios. Na maioria das organizações, **a gestão é da responsabilidade da gerência executiva**, sob a liderança do chefe diretor executivo (CEO).

MODELO DE REFERÊNCIA DE PROCESSOS DO COBIT 5

O modelo de referência de processos do COBIT 5 **subdivide os 37 processos de TI em duas principais áreas de atividade – governança e gestão** – divididas em domínios de processos, conforme figura abaixo:

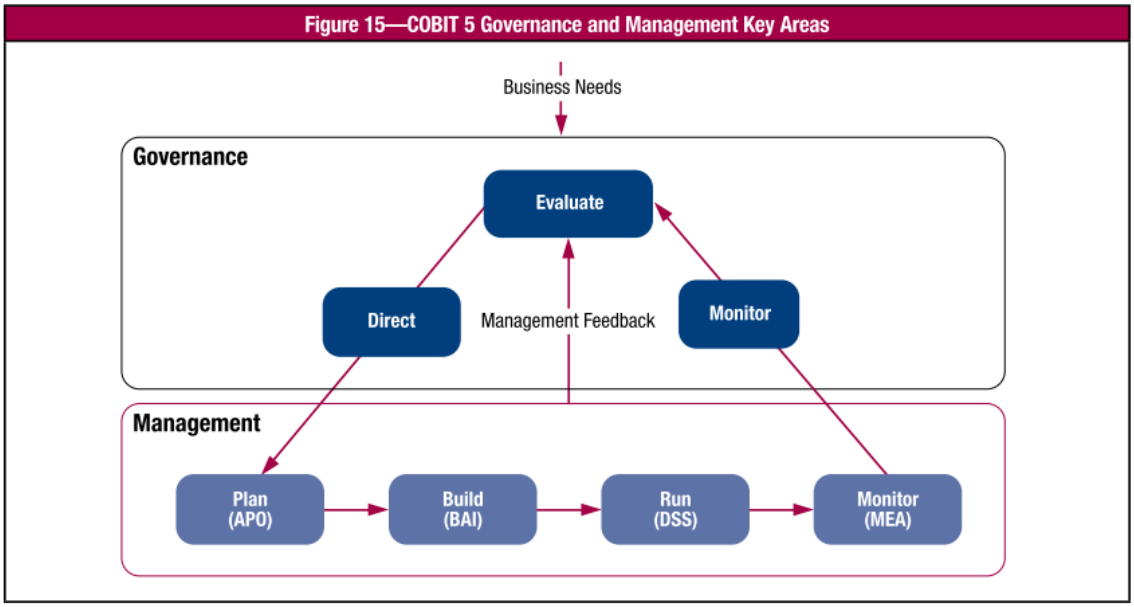

Figura 12 - Áreas chave de governança e gestão. Fonte: COBIT ® 5, Figura 15, ©2012 ISACA®

Processos de Governança

Contém **1 domínio Avaliar, Dirigir e Monitorar (EDM)** com **5 processos de governança**. Estes processos ditam as responsabilidades da alta direção para a avaliação, direcionamento e monitoração do uso dos ativos de TI para a criação de valor. Este domínio cobre a definição de um framework de governança, o estabelecimento das responsabilidades em termos de valor para a organização (ex. critérios de investimento), fatores de risco (ex. apetite ao risco) e recursos (ex. otimização de recursos), além da transparência da TI para as partes interessadas (stakeholders) [6].

Processos de Gestão

Contém **4 domínios**, de acordo com as áreas de responsabilidade de planejar, criar, executar e monitorar (PBRM) e oferece cobertura ponta a ponta de TI. Estes domínios são uma evolução da estrutura de domínios e processos do COBIT 4.1. Como pode ser visto, foi acrescentado um verbo para cada um dos domínios do COBIT 4.1. Os domínios são:

- **Alinhar, Planejar e Organizar (APO)**

  O domínio APO diz respeito à identificação de como a TI pode contribuir melhor com os objetivos de negócio. Processos específicos do domínio APO estão relacionados com a estratégia e táticas de TI, arquitetura corporativa, inovação e gerenciamento de portfólio, orçamento, qualidade, riscos e segurança. **Contém 13 processos**. [6]

- **Costruir, Adquirir e Implementar (BAI)**

  O domínio BAI torna a estratégia de TI concreta, identificando os requisitos para a TI e gerenciando o programa de investimentos em TI e projetos associados. Este domínio também endereça o gerenciamento da disponibilidade e capacidade; mudança organizacional; gerenciamento de mudanças (TI); aceite e transição; e gerenciamento de ativos, configuração e conhecimento. **Contém 10 processos**. [6]

- **Entregar, Servir e Suportar (DSS)**

  O domínio DSS se refere à entrega dos serviços de TI necessários para atender aos planos táticos e estratégicos. O domínio inclui processos para gerenciar operações, requisições de serviços e incidentes, assim como o gerenciamento de problemas, continuidade,serviços de segurança e controle de processos de negócio. **Contém 6 processos**. [6]

- **Monitorar, Avaliar e Medir (MEA) : 3 processos**.

  O domínio MEA visa monitorar o desempenho dos processos de TI, avaliando a conformidade com os objetivos e com os requisitos externos. **Contém 3 processos.**

A figura abaixo exibe os 37 processos de governança e gestão do COBIT 5. Os detalhes de cada processo estão no ***COBIT 5: Enabling Processes*** [9]**.**

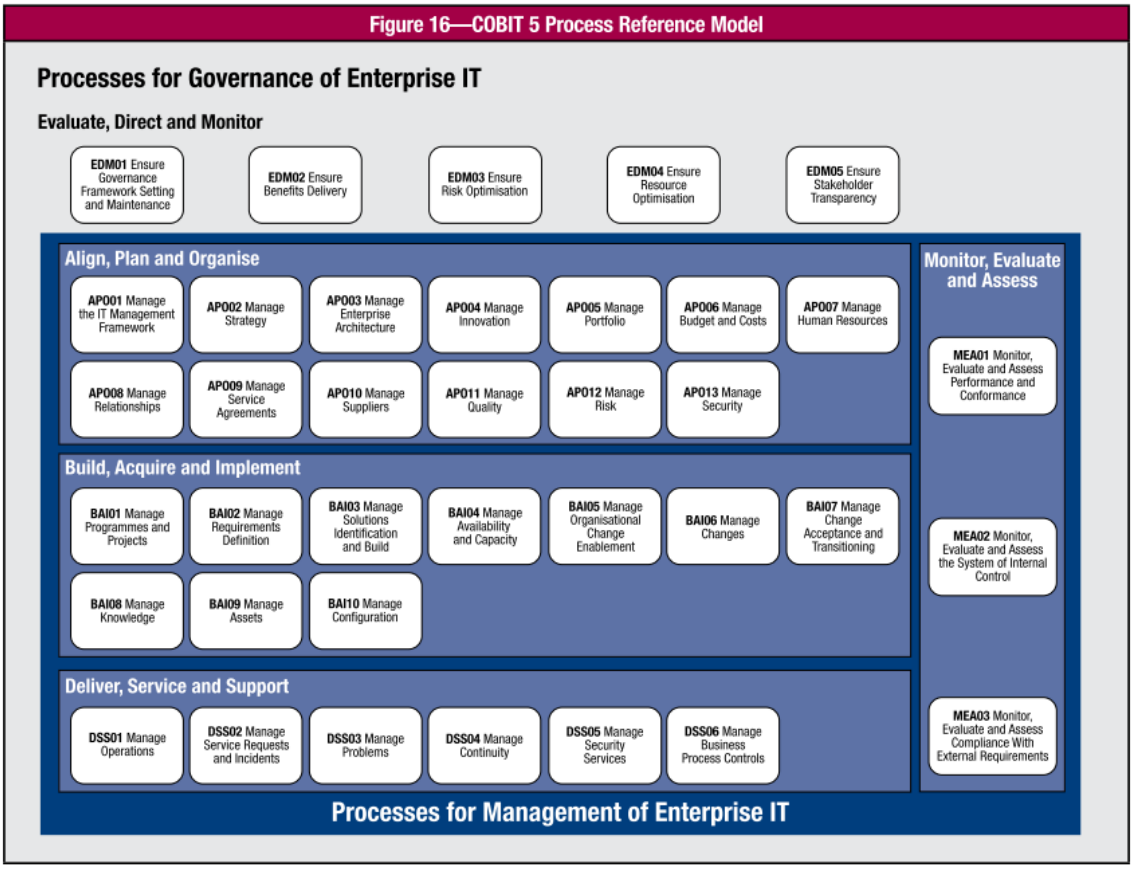

Figura 13 - Modelo de Referência de Processos. Fonte: COBIT ® 5, Figura 16, ©2012 ISACA®

No *COBIT 5: Enabling Processes*, **cada um dos 37 processos são desdobrados em práticas de governança ou práticas de gestão**. Essas práticas de governança e de gestão são equivalentes aos objetivos de controle do COBIT 4.1, práticas de gestão do Val IT e do Risk IT.

No Anexo III, encontra-se a relação de todos os processos com a respectiva descrição de cada um.

Estrutura de Processos

Para cada processo, as seguintes informações são incluídas, de acordo com o modelo de processo anteriormente explicado:

- Identificação do processo:
  - Label do Processo: o domínio (EDM, APO, BAI, DSS, MEA) e o número do processo;
  - Nome do Processo: breve descrição do processo;
  - Área do processo: governança ou gestão
  - Nome de domínio
- Descrição – uma visão do que o processo faz e como o processo alcança seu propósito
- Propósito do Processo – descrição geral do propósito do processo
- Informação de objetivos em cascata – referência e descrição dos objetivos relacionados com a TI que são essencialmente suportados pelo processo e métricas para medir o alcance dos objetivos relacionados com a TI.
- Objetivos de processos e métricas – um conjunto de metas de processo e um número limitado de exemplo de métricas.

- Matriz RACI – uma sugestão de atribuição de nível de responsabilidade por práticas de processos para diferentes funções e estruturas.
- Descrição detalhada de práticas de processo – para cada prática:
  - Título da Prática e descrição;
  - Entradas e saídas da prática, com indicação de origem e destino;
  - As atividades de processo, detalhando ainda mais as práticas;
- Guias relacionados (related guidance): associa cada processo do COBIT a outros frameworks que podem ser usados para implementar o processo.

Como exemplo, veja o Anexo IV que contém a descrição do processo BAI06: Gerenciar Mudanças.

GUIA DE IMPLEMENTAÇÃO DO COBIT 5

A ISACA oferece um guia de implementação em sua publicação ***COBIT 5 Implementation***, que é baseado em um ciclo de vida de melhoria contínua. Não se destina a ser uma abordagem prescritiva, nem uma solução completa, mas sim um guia para evitar os problemas mais comuns encontrados, alavancar as boas práticas e ajudar na geração de resultados esperados. O guia também é apoiado por um conjunto de ferramentas de implementação contendo uma variedade de recursos. O seu conteúdo inclui [4]:

- ✓ Auto-avaliação, medição e ferramentas de diagnóstico
- ✓ Apresentações destinadas a vários públicos
- ✓ Artigos relacionados e mais explicações

No documento relativo ao framework COBIT 5 é apresentada uma introdução à implementação e ao ciclo de vida de melhoria contínua e destaca uma série de tópicos importantes do ***COBIT 5 Implementation***, tais como:

- ✓ Fazer um plano de negócios (*business case*) para a implementação e melhoria da governança e gestão de TI
- ✓ Reconhecer os "pontos de dor" (pontos fracos) típicos e eventos de disparo
- ✓ Criar o ambiente adequado para a implementação
- ✓ Utilizar COBIT para identificar lacunas e orientar o desenvolvimento de viabilizadores, como políticas, processos, princípios, estruturas organizacionais, e os papéis e responsabilidades

Mas como começar a implementação?

Cada organização precisa **desenvolver seu próprio *road map* ou plano de implementação**, levando em consideração o seu contexto, ou seja, fatores do ambiente interno e externo específico da organização, tais como:

- Ética e cultura
- Leis, regulamentos e políticas aplicáveis
- Missão, visão e valores
- Políticas e práticas de governança

- Plano de negócios (*business plan*) e intenções estratégicas
- Modelo de funcionamento e nível de maturidade
- Estilo de gestão
- O apetite pelo risco
- Capacidades e recursos disponíveis
- Práticas da indústria

Em seguida, é importante **ter um ambiente apropriado para se implementar a governança corporativa de TI**. **Somente se consegue implementar governança corporativa de TI se houver patrocínio da alta direção da organização!** Uma das melhores maneiras de obter esse patrocínio e formalizar essa implementação, fornecendo um mecanismo para os executivos e para o conselho de administração (*board*) monitorar e direcionar a TI é estabelecer um **Comitê Estratégico e Executivo de TI.** Este comitê atua em nome do conselho de administração (para o qual deve prestar contas) e é responsável por definir como a TI é utilizada dentro da organização e por tomar decisões importantes relacionadas com TI que afetam a organização. Este comitê precisa ser presidido por um executivo de negócio (idealmente um membro do *board*) e terá como membros representantes das principais áreas de negócio da organização, além do CIO ou diretor de TI.

Para indicar a necessidade de uma melhor governança e gestão de TI corporativa podem existir uma série de fatores denominados **pontos de dor (*pain points*) ou eventos de gatilho (*trigger events*)** que podem ser utilizados como o ponto de partida para iniciativas de implementação.

Pontos de dor são problemas que a organização está enfrentando ou os pontos fracos da organização. Exemplos de alguns dos pontos de dor conforme identificados no ***COBIT 5 Implementation*** são:

- Frustração do negócio com iniciativas fracassadas, elevando os custos de TI e uma percepção de baixo valor para o negócio;
- Incidentes significativos relacionados com riscos de TI, tais como perda de dados;
- Problemas de prestação de serviços de terceirização, como falha consistente para atender aos níveis de serviço acordados;
- Ausência de cumprimento de requisitos legais ou contratuais;
- Resultados da auditoria sobre o mau desempenho de TI;
- Falha de transparência nos gastos de TI;
- Desperdício de recursos em projetos que não geram valor para o negócio;
- Insatisfação da equipe de TI;
- Relutância dos membros do conselho ou diretores em se envolver com a implementação.

Além desses pontos de dor, outros eventos em ambiente interno e externo da empresa podem sinalizar ou desencadear um foco na governança e gestão corporativa de TI. Exemplos de evento de gatilho (*trigger events*) são:

- Fusão, aquisição ou alienação;
- Mudança no mercado, na economia ou na posição competitiva;

- Mudança no modelo operacional de negócios ou acordos de fornecimento;
- Novas exigências regulatórias ou de conformidade;
- Mudança significativa de tecnologia ou mudança de paradigma;
- Auditoria externa.

Para garantir o sucesso de iniciativas de implementação pelo uso do COBIT, a necessidade de agir deve ser amplamente reconhecida e comunicada dentro da organização. **A iniciativa deve ser de propriedade de um patrocinador, envolver todos os *stakeholders* e ser baseada em um caso de negócio (*business case*)**. Inicialmente, esta pode estar em uma perspectiva estratégica, começando com uma compreensão clara dos resultados de negócio desejados e progredindo para uma descrição detalhada das tarefas críticas e metas, bem como papéis-chave e responsabilidades. O caso de negócio é uma ferramenta valiosa disponível para a gestão para orientar a criação de valor para o negócio. No mínimo, o plano de negócios deve incluir o seguinte:

- Os benefícios a serem alcançados e o seu alinhamento com a estratégia de negócios;
- As mudanças de negócios necessárias para criar o valor previsto. Isso poderia ser baseado em **análise de *gap*** e deve indicar claramente o que está no escopo e o que está fora do escopo;
- Os investimentos necessários para realizar as mudanças na governança e gestão de TI (com base em estimativas de projetos necessários);
- O custos operacionais de TI e do negócio;
- O risco inerente nas iniciativas, incluindo quaisquer restrições ou dependências (com base em desafios e fatores de sucesso);
- Papéis, responsabilidades e obrigações relacionados com a iniciativa;
- Como o investimento e a criação de valor serão monitorados durante todo o ciclo de vida econômico, e as métricas a serem utilizadas (com base em objetivos e métricas).

Ciclo de Vida de Implementação

A aplicação de uma abordagem de ciclo de vida de melhoria contínua fornece um método para as organizações enfrentarem a complexidade e os desafios normalmente encontrados durante a implementação da governança corporativa de TI.

Existem **3 componentes** inter-relacionados neste ciclo de vida:

- **Melhoria contínua (núcleo)**
- **Habilitação de mudança (2º anel)**
- **Gestão do programa (3º anel)**

O ciclo de vida possui **7 fases** como está ilustrado na figura abaixo [4]:

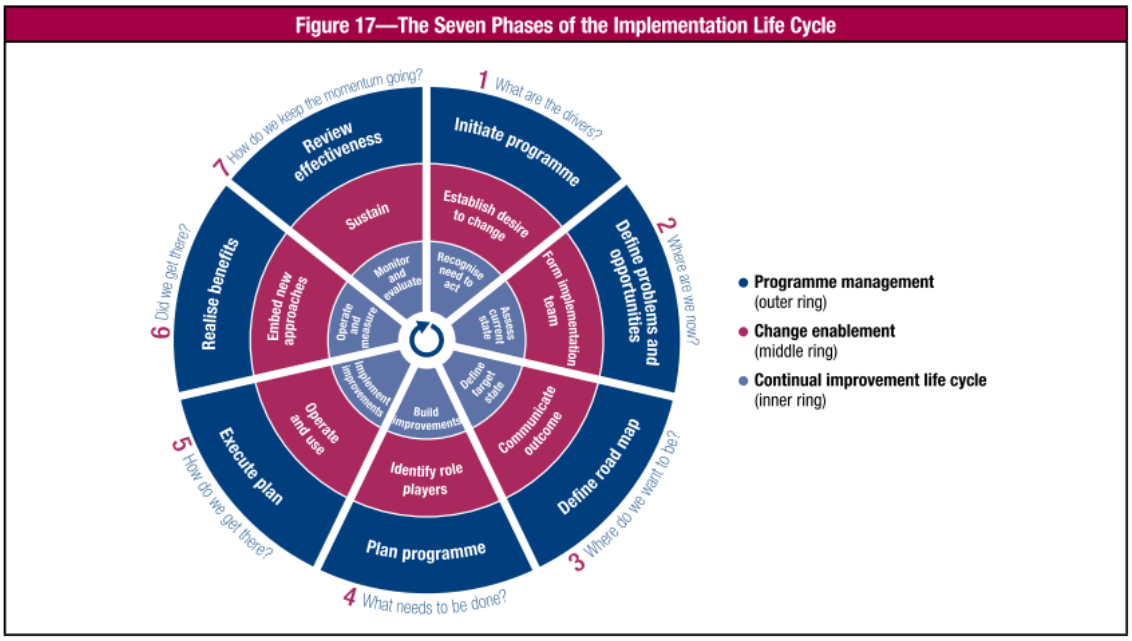

Figura 14 - Fases do Ciclo de Vida. Fonte: COBIT ® 5, Figura 17, ©2012 ISACA®

Fase 1: começa com o reconhecimento e concordância da necessidade de uma iniciativa de implementação ou melhoria. Identifica os pontos de dor atuais e cria um desejo de mudança nos níveis de gestão executiva.

Fase 2: está focada em definir o escopo da iniciativa de implementação ou melhoria utilizando o mapeamento dos objetivos de negócio com os objetivos de TI para os processos de TI associados, considerando como cenários de risco também poderiam destacar os processos-chave em que se deve concentrar. Uma avaliação do estado atual é então realizada, e problemas ou deficiências são identificados pela realização de uma avaliação de capacidade de processo. Iniciativas em larga escala devem ser estruturadas como várias iterações do ciclo de vida – para qualquer iniciativa de implementação superior a seis meses, há um risco de perder o impulso e o foco dos stakeholders.

Fase 3: um meta de melhoria é definida e seguida por uma análise mais detalhada para identificar as lacunas e as possíveis soluções. Deve ser dada prioridade às iniciativas que são mais fáceis de realizar e as susceptíveis de produzir os maiores benefícios.

Fase 4: planeja soluções práticas através da definição de projetos apoiados por casos de negócios justificáveis. Um plano de mudança para execução também é desenvolvido. Um caso de negócio bem desenvolvido ajuda a garantir que os benefícios do projeto são identificados e monitorados.

Fase 5: as soluções propostas são implementadas nas práticas do dia-a-dia. As medidas podem ser definidas e o monitoramento estabelecido, utilizando metas e métricas do COBIT para garantir que o alinhamento de negócios seja alcançado e mantido e o desempenho possa ser medido.

Fase 6: incide sobre a operação sustentável dos viabilizadores novos ou melhorados e o monitoramento da realização dos benefícios esperados.

Fase 7: o sucesso global da iniciativa é revista, outras exigências para a governança ou gestão de organizações de TI são identificadas e a necessidade de melhoria contínua é reforçada.

MODELO DE CAPACIDADE DE PROCESSOS

Usuários do COBIT 4.1 estão familiarizados com o modelo de maturidade de processo incluído nesse framework. Este modelo é utilizado para medir o nível de maturidade atual ("as-is") dos processos relacionados a TI de uma organização, para definir o nível de maturidade desejado ("to-be") e para determinar o *gap* entre eles e como melhorar o processo para alcançar o nível de maturidade desejado [4] .

O COBIT 5 apresenta um novo modelo para a avaliação da **capacidade** dos processos de TI da organização baseado na norma ISO/IEC 15504 de Engenharia de Software (norma de avaliação de processos).

Este modelo vai alcançar os mesmos objetivos gerais de avaliação do processo e suporte a melhoria de processos, ou seja, irá fornecer um meio de mensurar o desempenho de qualquer um dos processos de governança ou de gestão.

Os detalhes da abordagem de avaliação de capacidade COBIT 5 estão contidos na publicação ***COBIT ® Process Assessment Model (PAM): Using COBIT 5.***

Embora esta abordagem forneça informações valiosas sobre o estado dos processos, **vale lembrar que processos são apenas um dos sete viabilizadores de governança e gestão**. Por consequência, as avaliações de processo não irão fornecer um quadro completo sobre o estado de governança de uma organização. Para isso, os outros viabilizadores precisam ser avaliados também.

Diferenças entre o Modelo de Maturidade do COBIT 4.1 e o Modelo de Capacidade do COBIT 5

Para utilizar o modelo de maturidade do COBIT 4.1 para a melhoria do processo são necessários os seguintes componentes do COBIT 4.1:

- Em primeiro lugar, uma avaliação precisa ser feita se os objetivos de controle para o processo forem cumpridas;
- Em seguida, o modelo de maturidade que existe para cada processo pode ser usado para obter o nível de maturidade do processo;
- Além disso, o modelo de maturidade genérico do COBIT 4.1 fornece seis atributos distintos que são aplicáveis para cada processo e que ajudam na obtenção de uma visão mais detalhada sobre o nível de maturidade dos processos;
- Controles de processos são objetivos de controle genérico que também precisam ser revistos quando uma avaliação do processo é realizada. Controles de processos se sobrepõem parcialmente com os atributos do modelo de maturidade genérico.

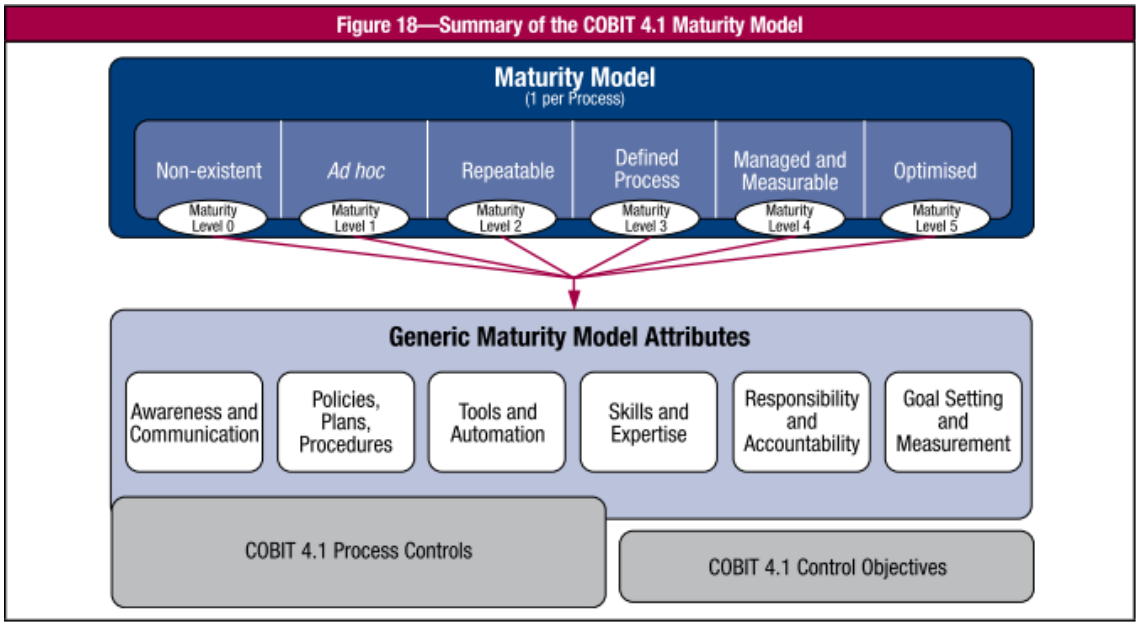

Figura 15 - Modelo de Maturidade do COBIT 4.1. Fonte: : COBIT ® 5, Figura 18, ©2012 ISACA®

O modelo de capacidade de processos do COBIT 5 é exibido na figura abaixo.

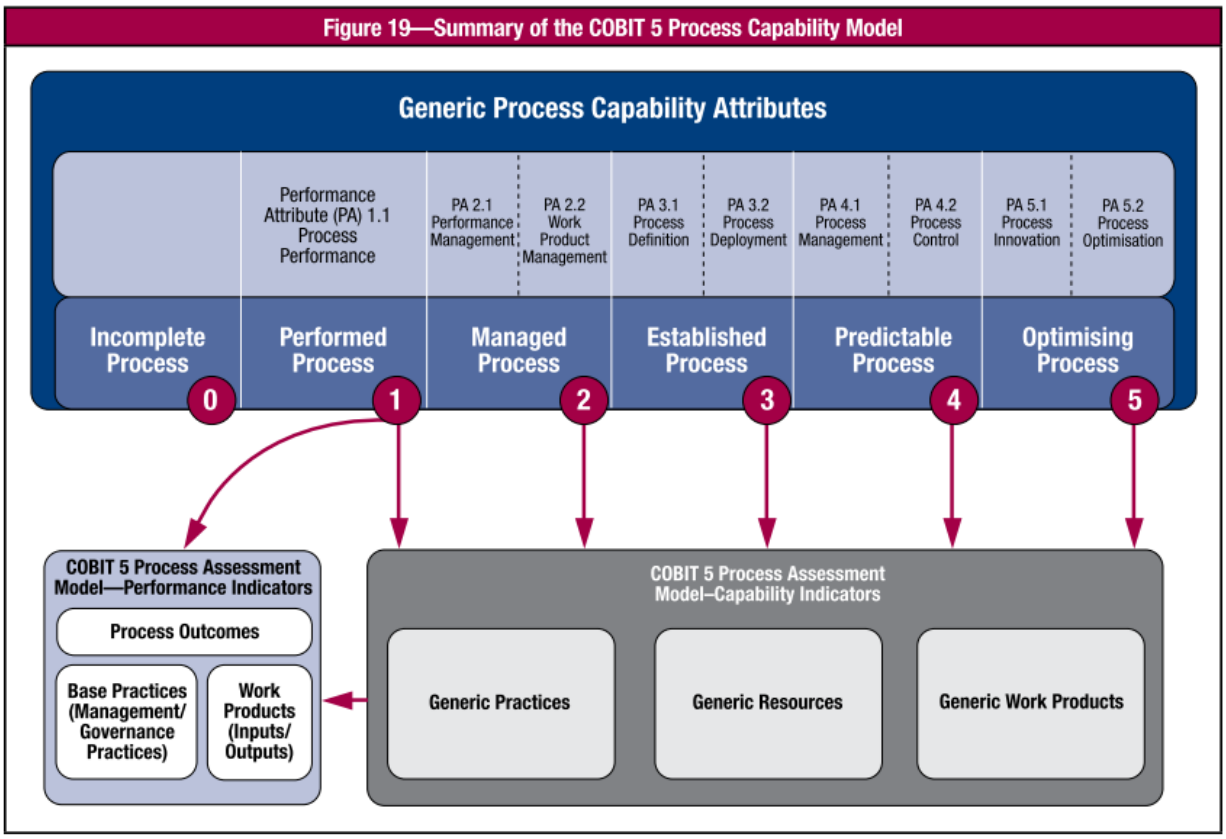

Figura 16 - Modelo de Capacidade de Processos. Fonte: COBIT ® 5, Figura 19, ©2012 ISACA®

O modelo contém **6 níveis de capacidade**, em uma escala de 0 a 5, porém com nome e significado bem diferentes dos níveis de maturidade do COBIT 4.1 e **9 atributos de processo** (PA – Process Attributes). Atributos de processo determinam se um processo alcançou um determinado nível de capacidade, medindo um aspecto particular da capacidade de um processo. **Cada nível de capacidade de processo possui um conjunto de atributos de processo que devem ser avaliados para o alcance do nível em questão**. Os atributos de processo são:

- PA1.1 – Process Performance
- PA2.1 – Performance Management
- PA2.2 – Work Product Management
- PA3.1 – Process Definition
- PA3.2 – Process Deployment
- PA4.1 – Process Management
- PA4.2 – Process Control
- PA5.1 – Process Innovation
- PA5.2 – Process Optimization

Cada atributo de processo é avaliado com base na seguinte escala:

- **N (não alcançado)**: há pouca ou nenhuma evidência de realização do atributo de processo no processo avaliado (0% a 15% de realização).
- **P (parcialmente alcançado)**: há alguma evidência de realização do atributo de processo no processo avaliado. Alguns aspectos da realização do atributo podem ser imprevisíveis (15% a 50% de realização).

- **L (largamente alcançado)**: há evidência de uma realização significativa do atributo de processo no processo avaliado. Algumas fraquezas relacionadas a este atributo podem existir no processo avaliado (50% a 85% de realização).
- **F (totalmente alcançado)**: há evidência de uma realização completa do atributo de processo no processo avaliado. Não há deficiências significativas associadas a este atributo no processo avaliado (85% a 100% de realização).

Os níveis de capacidade são:

Nível 0 - Processo Incompleto: o processo não está implementado ou não atinge seu objetivo. Nesse nível, há pouca ou nenhuma evidência de realização sistemática da finalidade do processo.

Nível 1 - Processo Realizado: possui o atributo PA1.1 – Process Performance (Desempenho do Processo). O processo está implementado e atinge seu objetivo.

Nível 2 - Processo Gerenciado: possui os atributos PA2.1 – Performance Management (Gerenciamento de Desempenho) e PA2.2 – Work Product Management (Gerenciamento de Produto de Trabalho). O processo realizado anteriormente descrito é implementado de forma gerenciada (planejado, monitorado e ajustado) e seus produtos de trabalho estão devidamente estabelecidos, controlados e mantidos.

Nível 3 - Processo Estabelecido: possui os atributos PA3.1 – Process Definition (Definição de Processo) e PA3.2 – Process Deployment (Implementação de Processo). O processo gerenciado anteriormente descrito é implementado usando um processo definido que é capaz de alcançar os seus resultados de processo.

Nível 4 - Processo Previsível: possui os atributos PA4.1 – Process Management (Gerenciamento do Processo) e PA4.2 – Process Control (Controle do Processo). O processo estabelecido anteriormente descrito opera dentro de limites definidos para alcançar seus resultados de processo.

Nível 5 - Processo Em Otimização: possui os atributos PA5.1 – Process Innovation (Inovação de Processo) e PA5.2 – Process Optimization (Otimização de Processo). O processo previsível anteriormente descrito é continuamente melhorado para atender aos objetivos de negócio.

Cada nível de capacidade só pode ser alcançado quando o nível inferior for plenamente alcançado. Por exemplo, uma capacidade de processo nível 3 (Processo Estabelecido), exige que os atributos Definição de Processos e Implementação do Processo sejam amplamente realizados, além da plena realização dos atributos do nível de capacidade 2 (Processo Gerenciado).

A partir das descrições anteriores, é evidente que há algumas diferenças práticas associadas com a mudança no modelo de avaliação dos processos. Os usuários precisam estar cientes dessas mudanças e estar preparado para levá-los em conta em seus planos de ação. As principais alterações a serem consideradas incluem:

- Embora seja tentador comparar os resultados da avaliação entre COBIT 4.1 e COBIT 5 por causa da aparente semelhança com a escala de números e palavras usadas para

descrever estas, tal comparação é difícil por causa da diferenças no escopo, no foco e na intenção, como pode ser visto na tabela 1.

- Em geral, **a pontuação será menor com o modelo de capacidade de processo do COBIT 5**. No modelo de maturidade do COBIT 4.1, um processo pode atingir nível 1 ou 2, sem alcançar plenamente todos os objetivos do processo ; no COBIT 5, isso resultará em uma pontuação mais baixa de 0 ou 1.
- **Não existe mais um modelo de maturidade específico por processo** incluído com a descrição de processos detalhados em COBIT 5 porque a abordagem de avaliação de capacidade da norma ISO/IEC 15504 não exige isso e ainda proíbe esta abordagem. Em vez disso, as informações definidas na ISO/IEC 15504 estão no modelo de referência de processo do COBIT 5:
    - Descrição do processo, com as declarações de propósito;
    - Práticas-base, que são o equivalente de práticas de processos de governança ou de gestão do COBIT 5;
    - Produtos de trabalho, que são o equivalente às entradas e saídas no COBIT 5.
- O modelo de maturidade COBIT 4.1 produziu um perfil de maturidade da empresa. O principal objetivo desse perfil era identificar em quais dimensões ou para quais atributos houve deficiências específicas que precisavam de melhoria. **Em COBIT 5 o modelo de avaliação fornece uma escala de medida para cada atributo de processo e orientações sobre como aplicá-lo, portanto, para cada processo uma avaliação pode ser feita para cada um dos nove atributos de processo**.

Comparação Tabela de Níveis de Maturidade (COBIT 4.1) Níveis de Capacidade de Processo (COBIT 5)	
COBIT 4.1	**COBIT 5**
Nível 5: Processo Otimizado - processos são refinados ao nível de boa prática, baseados nos resultados de melhoria contínua. A TI é utilizada de forma integrada para automatizar o fluxo de trbalho, fornecendo ferramentas para melhorar a qualidade e efetividade, fazendo com que a organização seja rápida para se adaptar.	**Nível 5: Processo em Otimização** - o nível 4 Processo Previsível é continuamente melhorado para atender metas de negócio atuais e projetadas.
Nível 4: Gerenciado e Mensurável - gerenciamento monitora e mede conformidade com procedimentos e toma ações onde processos parecem não funcionar efetivamente. Processos estão sob melhoria constante e fornecem boa prática. Automação e ferramentas são usadas de forma limitada ou fragmentada.	**Nível 4: Processo Previsível** - o nível 3 Processo Estabelecido agora opera dentro de limites definidos para alcançar seus resultados de processo.
Nível 3: Processo Definido - procedimentos são padronizados, documentados e comunicados por meio de treinamento. É obrigátorio que estes processos sejam seguidos; entretanto, é pouco provável que desvios sejam detectados. Os próprios procedimentos não são sofisticados, mas são a formalização de práticas existentes.	**Nível 3: Processo Estabelecido** - o nível 2 Processo Gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resulados de processo.
	Nível 2: Processo Gerenciado - o nível 1 Processo Realizado é agora implementado de forma gerenciada (planejado, monitorado e ajustado) e seus produtos de trabalho são estabelecidos, controlados e mantidos apropriadamente.
Nível 2: Repetível mas Intuitivo - processos são desenvolvidos de forma que procedimentos similiares são seguidos por pessoas diferentes que estão executando a mesma tarefa. Não há treinamento ou comunicação formal de procedimentos padronizados e a responsabilidade é deixada a cargo do indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e, portanto, erros podem ocorrer.	**Nível 1: Processo Realizado** - o processo implementado alcança seu propósito de processo. **Obs.: É possível que algum processo classificado como nível 1 seja classificado como nível 0 de acordo com a ISO/IEC 15504, se o resultado do processo não for alcançado.**
Nível 1: Inicial/Ad-hoc - há evidência que a organização reconheceu que questões existem e precisam ser tratadas. Não há, entretanto, nenhum processo padronizado; em vez disto, existem abordagens *ad hoc* que tendem a ser aplicadas por indivíduos. A abordagem geral de gerenciamento é desorganizada.	
Nível 0: Nâo existente - completa falta de qualquer processo reconhecível. A organização ainda não reconheceu que existe uma questão a ser tratada.	**Nível 0: Processo Incompleto** - o processo não é implementado ou não consegue alcançar seu propósito

Tabela 1 - Comparação Niveis de Maturidade COBIT 4 x Níveis de Capacidade COBIT 5

PRINCIPAIS MUDANÇAS DO COBIT 5 COM RELAÇÃO AO COBIT 4.1

As principais mudanças no COBIT 5 com relação ao COBIT 4.1 são [7]:

1. Novos princípios de governança corporativa de TI, conforme visto na seção Princípios do COBIT 5.

2. Aumento do foco nos viabilizadores (enablers)

Os recursos de TI do COBIT 4.1 – processos, aplicações, informação e infra-estrutura – são considerados viablilizadores no COBIT 5.

O viabilizador 1.Princípios, políticas e estruturas foi mencionado em alguns processos do COBIT 4.1.

O viabilizador 2.Processos era a parte central no COBIT 4.1.

O viabilizador 3.Estruturas organizacionais estava implícito, através dos papéis responsável, consultado ou informado na matriz RACI.

O viabilizador 4.Cultura, ética e comportamento foi mencionado em alguns processos do COBIT 4.1.

3. Novo Modelo de Referência de Processos

COBIT 5 baseia-se no modelo de referência com um novo domínio de governança e vários processos novos e modificados que agora cobrem atividades corporativas de ponta a ponta, ou seja, das áreas de negócio e funções de TI.

COBIT 5 consolida COBIT 4.1, Val IT e Risk IT em um único framework e está atualizado para se alinhar com as melhores práticas atuais-por exemplo, ITIL, TOGAF.

4. Processos novos e modificados

Outra mudança visível do COBIT 5 ocorre nos domínios e processos [8]. Na versão 4.1 havia quatro domínios e 34 processos. Na versão 5, há cinco domínios e 37 processos.

COBIT 5 introduz cinco novos processos de governança no domínio EDM (Avaliar, Dirigir e Monitorar), sendo os outros quatro domínios sofreram mudança com relação ao COBIT 4.1 e estão definidos como processos de gestão, conforme tabela abaixo [8]:

COBIT 4.1	**COBIT 5**
Plan and Organize (Planejar e Organizar) **10 processos**	Align, Plan and organize (Alinhar, Planejar e organizar) **13 processos**
Acquire and Implement (Adquirir e Implementar)	Build, Acquire and Implement (Construir, Adquirir e Implementar)

7 processos	**10 processos**
Deliver and Support (Entregar e Suportar) **13 processos**	Deliver, Service and Support (Entregar, Servir e Suportar) **6 processos**
Monitor and Evaluate (Monitorar e Avaliar) **4 processos**	Monitor, Evaluate and Assess (Monitorar, Avaliar e Medir) **3 processos**

Figura 17 - Comparativo COBIT 4.1 x COBIT 5

Há vários processos novos e modificados, em particular [7]:

- ✓ APO03 Gerenciar a Arquitetura Corporativa
- ✓ APO04 Gerenciar a Inovação
- ✓ APO05 Gerenciar o Portfólio
- ✓ APO06 Gerenciar Orçamento e Custos
- ✓ APO08 Gerenciar as Relações
- ✓ APO13 Gerenciar a Segurança
- ✓ BAI05 Gerenciar a Implementação de Mudança Organizacional
- ✓ BAI08 Gerenciar o Conhecimento
- ✓ BAI09 Gerenciar os Ativos
- ✓ DSS05 Gerenciar Serviços de Segurança
- ✓ DSS06 Gerenciar os Controles de Processos de Negócio

Os processos do COBIT 5 cobrem as atividades de negócio e de TI de ponta a ponta, ou seja, uma visão completa de nível corporativo, além de tornar o envolvimento, responsabilidades e obrigações dos stakeholders no uso de TI mais explícita e transparente.

5. Práticas e atividades

As práticas de gestão e de governança do COBIT 5 são equivalentes aos objetivos de controle do COBIT 4.1 e dos processos de Val IT e Risk IT. As atividades do COBIT 5 são equivalentes às práticas de controle do COBIT 4.1 e das práticas do Val IT e Risk IT.

6. Objetivos e Métricas

COBIT 5 segue os mesmos conceitos de objetivos e métricas do COBIT 4.1, Val IT e Risk IT.

7. Entradas e saídas

COBIT 5 provê entradas e saídas para cada prática de gestão, enquanto o COBIT 4.1 provê somente no nível de processo. Isso fornece um guia mais detalhado para o desenho dos processos.

8. Matriz RACI

COBIT 5 fornece uma matriz RACI descrevendo papéis e responsabilidades de forma similar ao COBIT 4.1, porém oferece uma gama mais completa, detalhada e mais clara dos papéis para cada prática de gestão, permitindo uma melhor definição das responsabilidades dos papéis ou nível de envolvimento na concepção e implementação de processos.

9. Modelo de Capacidade de Processo

COBIT 5 descontinua o modelo de maturidade baseado no CMM e usado pelo COBIT 4.1. COBIT 5 é apoiado pelo novo modelo de capacidade de processos baseado na norma ISO/IEC 15504.

O modelo de maturidade do COBIT 4.1, Val IT e Risk IT baseadas em CMM não são considerados compatíveis com o modelo ISO/IEC 15504 no qual o COBIT 5 se baseia, porque os modelos usam diferentes atributos e escalas de medição.

ANEXO I: *COBIT 5 Goals Cascade*

O ***COBIT 5 Goals Cascade*** (cascata de objetivos) tem a finalidade de desdobrar [4]:

- os direcionadores (drivers) e as necessidades dos stakeholders em objetivos de negócio;

- os objetivos de negócio em objetivos de TI;

- os objetivos de TI em objetivos para os viabilizadores.

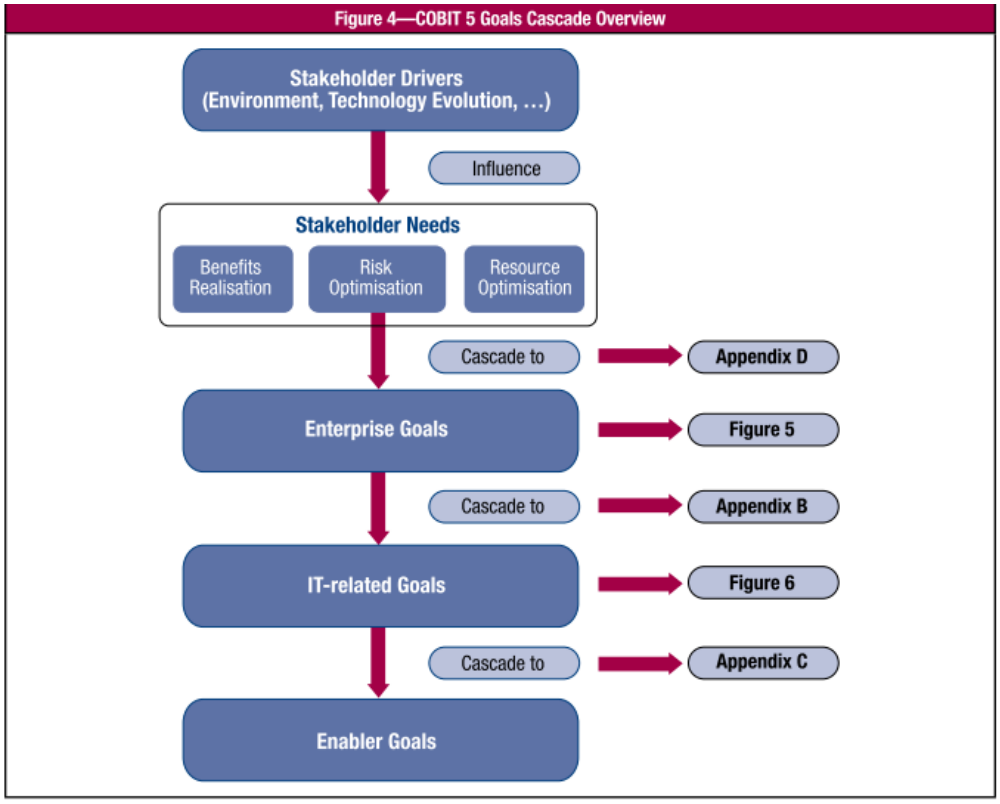

Figura 18 - Cascata de Objetivos. Fonte: COBIT ® 5, Figura 14, ©2012 ISACA®

Esse desdobramento é descrito nos quatro passos a seguir:

Passo 1: Direcionadores de Stakeholders (Stakeholder Drivers) influenciam as Necessidades dos Stakeholders

As necessidades dos stakeholders são influenciadas por um número de direcionadores (ou motivadores), como por exemplo, mudanças na estratégia do negócio, mudança no ambiente do negócio (entrada de novos concorrentes), mudanças nas leis e regulamentos vigentes e novas tecnologias.

Tomando a legislação como exemplo de direcionador, tem-se, no Brasil, a Lei nº 12.965, mais conhecida como o Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Um dos temas que a lei trata é a neutralidade da rede, em que o "responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. [10]" Isso visa garantir que todos os conteúdos e usuários sejam tratados da mesma maneira. Como exemplo prático, as operadoras de

telecomunicações, que proveem o acesso à Internet, podem ter uma oferta diversificada de banda, mas não podem bloquear ou limitar a velocidade de tráfego, dentro do pacote de banda contratado, para determinados aplicativos, sites ou conteúdos na rede [11]. Além disso, a lei determina que as operadoras deverão garantir a qualidade contratada da conexão à internet.

Essa lei se torna um direcionador de stakeholders influencia as necessidades dos stakeholders: as dos usuários de internet (stakeholder externo), que agora tem a garantia de que a qualidade de sua conexão será conforme contratado, e caso não seja, poderá reclamar seus direitos, e as do corpo diretivo da operadora de telecomunicações (stakeholder interno), que precisa se preocupar em adaptar o negócio para atender a essa obrigação (já que deverá modificar a oferta de seus serviços), pois caso não cumpram, poderá ocorrer a perda de clientes, impactando na criação de valor para o negócio.

Passo 2: Necessidades dos Stakeholders desdobrados em Objetivos de Negócio

As necessidades dos stakeholders podem ser relacionadas a um conjunto de objetivos de negócio genéricos definidos pelo COBIT 5. O framework define 17 objetivos de negócio genéricos que podem ser desenvolvidos usando as dimensões do *Balanced Scoredcard* (BSC) e representam uma lista de objetivos comumente usados por uma organização. Embora essa lista não seja exaustiva, a maioria dos objetivos específicos de uma organização pode ser mapeada para um ou mais objetivos de negócio genéricos.

A lista de objetivos de negócio genéricos, como mostrado na figura abaixo, incluem as seguintes informações:

- A dimensão BSC ao qual o objetivo pertence;
- Objetivos de negócio;
- O relacionamento do objetivo de negócio com os três objetivos principais de governança – realização de benefícios, otimização de risco e otimização de recursos (‘P’ indica relacionamento primário e ‘S’ relacionamento secundário).

Figure 4—COBIT 5 Enterprise Goals				
		Relation to Governance Objectives		
BSC Dimension	Enterprise Goal	Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Figura 19 - Objetivos de Negócio.
Fonte: COBIT ® 5, Figura 4, ©2012 ISACA®

Passo 3: Objetivos de Negócio desdobrados em Objetivos de TI

O alcance dos objetivos de negócio exige uma série de resultados relacionados a TI, que são representados pelos objetivos relacionados a TI. COBIT 5 define 17 objetivos relacionados a TI, fornecendo exemplos de métricas para mensurar cada um dos objetivos. As métricas dos objetivos de TI podem ser vistas no detalhamento do viabilizador Processos. A lista de objetivos de TI é exibida na figura abaixo:

Figure 5—IT-related Goals		
IT BSC Dimension	Information and Related Technology Goal	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

Figura 20 - Objetivos de TI. Fonte: COBIT ® 5, Figura 5, ©2012 ISACA®

Passo 4: Objetivos de TI desdobrados em Objetivos de Viabilizadores

Alcançar os objetivos relacionados a TI requer a aplicação e uso bem-sucedidos de um conjunto de viabilizadores. Viabilizadores incluem:

- ✓ Princípios, políticas e frameworks
- ✓ Processos
- ✓ Estruturas organizacionais
- ✓ Cultura, ética e comportamento
- ✓ Informação
- ✓ Serviços, infraestrutura e aplicações
- ✓ Pessoas, habilidades e competências

Para cada viabilizador, um conjunto de objetivos específicos e relevantes pode ser definido para suportar os objetivos relacionados a TI. Para o viabilizador Processos, por exemplo, os objetivos e suas métricas são fornecidos nas descrições detalhadas de cada processo.

ANEXO II: Exemplo de Viabilizador: Processos

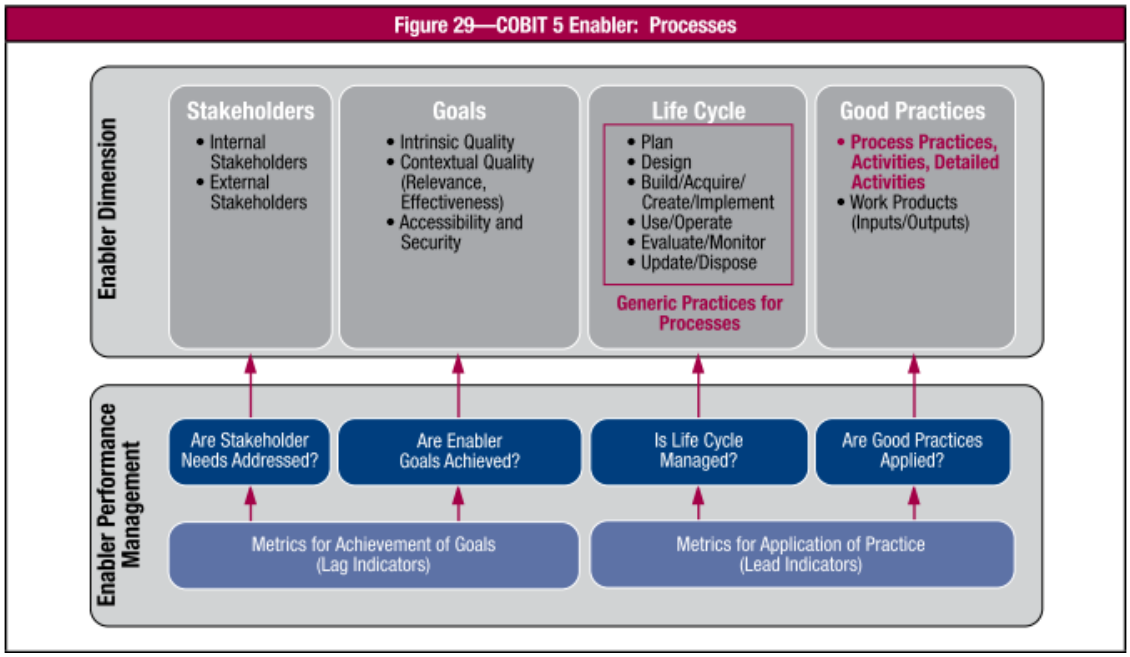

Figura 21 - Viabilizador Processos. Fonte: Fonte: COBIT ® 5, Figura 29, ©2012 ISACA®

Stakeholders: stakeholders do processo incluem todos os atores do processo, ou seja, todos as partes que são responsáveis, pra o qual são prestadas contas, consultadas e informadas (RACI) para as atividades do processo. Por isso, a matriz RACI para cada processo descrita no *COBIT 5: Enabling Process* pode ser utilizada.

Objetivos: para cada processo, os objetivos adequados e métricas relacionadas precisam ser definidos. Por exemplo, para o processo de APO08 Gerenciar relacionamentos pode-se encontrar um conjunto de objetivos de processo e métricas, tais como:

- Objetivo: estratégias de negócios, planos e requisitos são bem compreendidos, documentados e aprovados.
- Métrica: Percentual de programas alinhados com os requisitos de negócio

Ciclo de vida: cada processo tem um ciclo de vida, ou seja, ele tem que ser criado, executado e monitorado e ajustado quando necessário. Para se definir um processo, pode-se usar vários elementos do *COBIT 5: Enabling Process*, ou seja, definir responsabilidades e dividir o processo em práticas e atividades, e definir produtos de trabalho do processo (entradas e saídas). Numa fase posterior, o processo precisa ser mais robusto e eficiente, e para essa finalidade é necessário elevar o nível de capacidade do processo.

Boas práticas: *COBIT 5: Enabling Process* descreve para cada processo as boas práticas em termos de práticas de processo, atividades e atividades detalhadas.

ANEXO III: DOMÍNIOS E PROCESSOS DO COBIT 5

Avaliar, Dirigir e Monitorar		
EDM01	Assegurar o Estabelecimento e Manutenção do Framework de Governança	Analisa e articula os requisitos para a governança corporativa de TI, coloca em prática e mantém estruturas, princípios, processos e práticas, com clareza de responsabilidades e autoridade para alcançar a missão, as metas e os objetivos da organização.
EDM02	Assegurar a Entrega de Benefícios	Otimiza a contribuição de valor para o negócio a partir dos processos de negócios, serviços e ativos de TI resultantes de investimentos realizados pela TI a custos aceitáveis.
EDM03	Assegurar a Otimização de Riscos	Assegura que o apetite e tolerância a riscos da organização são compreendidos, articulados e comunicados e que o risco ao valor da organização relacionado ao uso de TI é identificado e controlado.
EDM04	Assegurar a Otimização de Recursos	Assegura que as capacidades adequadas e suficientes relacionadas à TI (pessoas, processos e tecnologia) estão disponíveis para apoiar os objetivos da organização de forma eficaz a um custo ótimo.
EDM05	Assegurar a Transparência para as partes interessadas	Assegura que a medição e relatórios de desempenho e conformidade da TI corporativa sejam transparentes para os stakeholders aprovarem as metas, métricas e as ações corretivas necessárias.

Alinhar, Planejar e Organizar		
APO01	Gerenciar o Framework de Gestão de TI	Esclarece e mantém a missão e visão da governança de TI da organização. Implementa e mantém mecanismos e autoridades para gerenciar a informação e o uso da TI na organização.
APO02	Gerenciar a Estratégia	Fornece uma visão holística do negócio e ambiente de TI atual, a direção futura, e as iniciativas necessárias para migrar para o ambiente futuro desejado.
APO03	Gerenciar a Arquitetura Corporativa	Estabelece uma arquitetura comum que consiste em processos de negócios, informações, dados, aplicação e tecnologia para realizar de forma eficaz e eficiente as estratégias de negócio e de TI por meio da criação de modelos e práticas-chave que descrevem arquitetura de linha de base.
APO04	Gerenciar a Inovação	Mantém uma consciência de TI e tendências de serviços relacionados, identifica oportunidades de inovação e planeja como se beneficiar da inovação em relação às necessidades do negócio. Influencia o planejamento estratégico e as decisões de arquitetura corporativa.
APO05	Gerenciar o Portfólio	Executa o conjunto de orientações estratégicas para os investimentos alinhados com a visão de arquitetura corporativa e as características desejadas do investimento e considerar as restrições de recursos e de orçamento. Avalia, prioriza programas e serviços, gerencia demanda dentro das restrições de recursos e de orçamento, com base no seu alinhamento com os objetivos estratégicos e risco. Move programas selecionados para o portfólio de serviços para execução. Monitora o desempenho de todo o portfólio de serviços e programas, propondo os ajustes necessários em resposta ao programa e desempenho do serviço ou mudança de prioridades da organização.
APO06	Gerenciar Orçamento e Custos	Administrar as atividades financeiras relacionadas a TI tantos nas funções de negócios e de TI, abrangendo orçamento, gestão de custos e benefícios e priorização dos gastos com o uso de práticas formais de orçamento e de um sistema justo e equitativo de alocação de custos para a organização.
APO07	Gerenciar Recursos Humanos	Fornece uma abordagem estruturada para garantir a estruturação ideal, colocação, direitos de decisão e as habilidades dos recursos humanos. Isso inclui a comunicação de papéis e responsabilidades definidas, planos de aprendizagem e de crescimento, e as expectativas de desempenho, com o apoio de pessoas competentes e motivadas.
APO08	Gerenciar as Relações	Gerencia o relacionamento entre o negócio e TI de uma maneira formal e transparente, que garanta foco na realização de um objetivo comum.

APO09	Gerenciar os Acordos de Serviço	Alinha serviços de TI e níveis de serviço com as necessidades e expectativas da organização, incluindo identificação, especificação, projeto, publicação, acordo, e acompanhamento de serviços de TI, níveis de serviço e indicadores de desempenho.
APO10	Gerenciar os Fornecedores	Gerencia serviços relacionados a TI prestados por todos os tipos de fornecedores para atender às necessidades organizacionais, incluindo a seleção de fornecedores, gestão de relacionamentos, gestão de contratos e revisão e monitoramento de desempenho de fornecedores para a efetividade e conformidade.
APO11	Gerenciar a Qualidade	Define e comunica os requisitos de qualidade em todos os processos, os procedimentos e os resultados das organizações, incluindo controles, monitoramento contínuo, e o uso de práticas comprovadas e padrões na melhoria contínua e esforços de eficiência.
APO12	Gerenciar os Riscos	Identificar continuamente, avaliar e reduzir os riscos relacionados a TI dentro dos níveis de tolerância estabelecidos pela diretoria executiva da organização.
APO13	Gerenciar a Segurança	Define, opera e monitora um sistema para a gestão de segurança da informação.

Construir, Adquirir e Implementar		
BAI01	Gerenciar Programas e Projetos	Gerenciar todos os programas e projetos do portfólio de investimentos em alinhamento com a estratégia da organização e de forma coordenada. Inicia, planeja, controla e executa programas e projetos, e finaliza com uma revisão pós-implementação.
BAI02	Gerenciar a Definição de Requisitos	Identifica soluções e analisa os requisitos antes da aquisição ou criação para assegurar que eles estão em conformidade com os requisitos estratégicos corporativos que cobrem os processos de negócio, aplicações, informações/ dados, infra-estrutura e serviços. Coordena com as partes interessadas afetadas a revisão de opções viáveis, incluindo custos e benefícios, análise de risco e aprovação de requisitos e soluções propostas.
BAI03	Gerenciar a Identificação e Construção de Soluções	Estabelece e mantém soluções identificadas em conformidade com os requisitos da organização abrangendo design, desenvolvimento, aquisição/terceirização e parcerias com fornecedores/vendedores. Gerencia configuração, teste de preparação, testes, requisitos de gestão e manutenção dos processos de negócio, aplicações, informações/dados, infra-estrutura e serviços.
BAI04	Gerenciar a Disponibilidade e Capacidade	Equilibra as necessidades atuais e futuras de disponibilidade, desempenho e capacidade de prestação de serviços de baixo custo. Inclui a avaliação de capacidades atuais, a previsão das necessidades futuras com base em requisitos de negócios, análise de impactos nos negócios e avaliação de risco para planejar e implementar ações para atender as necessidades identificadas.
BAI05	Gerenciar a Implementação de Mudança Organizacional	Maximiza a probabilidade de implementar com sucesso a mudança organizacional sustentável em toda a organização de forma rápida e com risco reduzido, cobrindo o ciclo de vida completo da mudança e todas as partes interessadas afetadas no negócio e TI.
BAI06	Gerenciar Mudanças	Gerencia todas as mudanças de uma maneira controlada, incluindo mudanças de padrão e de manutenção de emergência relacionadas com os processos de negócio, aplicações e infraestrutura. Isto inclui os padrões de mudança e procedimentos, avaliação de impacto, priorização e autorização, mudanças emergenciais, acompanhamento, elaboração de relatórios, encerramento e documentação.
BAI07	Gerenciar Aceite e Transição de Mudança	Aceita e produz formalmente novas soluções operacionais, incluindo planejamento de implementação do sistema, e conversão de dados, testes de aceitação, comunicação, preparação de liberação, promoção para produção de processos de negócios e serviços de TI novos ou alterados, suporte de produção e uma revisão pós-implementação.

BAI08	Gerenciar o Conhecimento	Mantém a disponibilidade de conhecimento relevante, atual, validado e confiável para suportar todas as atividades do processo e facilitar a tomada de decisão. Plano para a identificação, coleta, organização, manutenção, utilização e retirada de conhecimento.
BAI09	Gerenciar os Ativos	Gerencia os ativos de TI através de seu ciclo de vida para assegurar que seu uso agrega valor a um custo ideal. Os ativos permanecem operacionais e fisicamente protegidos e aqueles que são fundamentais para apoiar a capacidade de serviço são confiáveis e disponíveis.
BAI10	Gerenciar a Configuração	Define e mantém as descrições e as relações entre os principais recursos e as capacidades necessárias para prestar serviços de TI, incluindo a coleta de informações de configuração, o estabelecimento de linhas de base, verificação e auditoria de informações de configuração e atualizar o repositório de configuração.

Entregar, Servir e Suportar		
DSS01	Gerenciar as operações	Coordena e executa as atividades e procedimentos operacionais necessários para entregar serviços de TI internos e terceirizados, incluindo a execução de procedimentos operacionais, padrões pré-definidos e as atividades exigidas.
DSS02	Gerenciar Requisições de Serviço e Incidentes	Fornecer uma resposta rápida e eficaz às solicitações dos usuários e resolução de todos os tipos de incidentes. Restaurar o serviço normal; recorde e atender às solicitações dos usuários e registro, investigar, diagnosticar, escalar e solucionar incidentes.
DSS03	Gerenciar Problemas	Identifica e classifica os problemas e suas causas-raízes e fornece resolução para prevenir incidentes recorrentes. Fornece recomendações de melhorias.
DSS04	Gerenciar a Continuidade	Estabelece e mantém um plano para permitir o negócio e TI responder a incidentes e interrupções, a fim de continuar a operação de processos críticos de negócios e serviços de TI necessários e mantém a disponibilidade de informações em um nível aceitável para a organização.
DSS05	Gerenciar Serviços de Segurança	Protege informações da organização para manter o nível de risco aceitável para a segurança da informação da organização, de acordo com a política de segurança. Estabelece e mantém as funções de segurança da informação e privilégios de acesso e realiza o monitoramento de segurança.
DSS06	Gerenciar os Controles de Processos de Negócio	Define e mantém controles de processo de negócio apropriados para assegurar que as informações relacionadas e processadas satisfaz todos os requisitos de controle de informações relevantes.

Monitorar, Avaliar e Medir		
MEA01	Monitorar, Avaliar e Medir o Desempenho e Conformidade	Coleta, valida e avalia os objetivos e métricas do processo de negócios e de TI. Monitora se os processos estão realizando conforme metas e métricas de desempenho e conformidade acordadas e fornece informação que é sistemática e oportuna.
MEA02	Monitorar, Avaliar e Medir o Sistema de Controle Interno	Monitora e avalia continuamente o ambiente de controle, incluindo auto-avaliações e análises de avaliações independentes. Permite a gestão de identificar deficiências de controle e ineficiências e iniciar ações de melhoria.
MEA03	Monitorar, Avaliar e Medir a Conformidade com Requisitos Externos	Avalia se processos de TI e processos de negócios suportados pela TI estão em conformidade com as leis, regulamentos e exigências contratuais. Obtém a garantia de que os requisitos foram identificados e respeitados, e integrá-los à conformidade com o cumprimento global da organização.

ANEXO IV: Descrição do Processo BAI06: Gerenciar Mudanças

BAI06 Manage Changes	**Area: Management** **Domain: Build, Acquire and Implement**
Process Description Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.	
Process Purpose Statement Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Authorised changes are made in a timely manner and with minimal errors.	• Amount of rework caused by failed changes • Reduced time and effort required to make changes • Number and age of backlogged change requests
2. Impact assessments reveal the effect of the change on all affected components.	• Percent of unsuccessful changes due to inadequate impact assessments
3. All emergency changes are reviewed and authorised after the change.	• Percent of total changes that are emergency fixes • Number of emergency changes not authorised after the change
4. Key stakeholders are kept informed of all aspects of the change.	• Stakeholder feedback ratings on satisfaction with communications

BAI06 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

BAI06 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
BAI06.01 Evaluate, prioritise and authorise change requests. Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled.	**From**	**Description**	**Description**	**To**
	BAI03.05	Integrated and configured solution components	Impact assessments	Internal
	DSS02.03	Approved service requests	Approved requests for change	BAI07.01
	DSS03.03	Proposed solutions to known errors		
	DSS03.05	Identified sustainable solutions	Change plan and schedule	BAI07.01
	DSS04.08	Approved changes to the plans		
	DSS06.01	Root cause analyses and recommendations		
Activities				
1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.				
2. Categorise all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.				
3. Prioritise all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change.				
4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate.				
5. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.				
6. Plan and schedule all approved changes.				
7. Consider the impact of contracted services providers (e.g., of outsourced business processing, infrastructure, application development and shared services) on the change management process, including integration of organisational change management processes with change management processes of service providers and the impact on contractual terms and SLAs.				
Management Practice	**Inputs**		**Outputs**	
BAI06.02 Manage emergency changes. Carefully manage emergency changes to minimise further incidents and make sure the change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorised after the change.	**From**	**Description**	**Description**	**To**
			Post-implementation review of emergency changes	Internal
Activities				
1. Ensure that a documented procedure exists to declare, assess, give preliminary approval, authorise after the change and record an emergency change.				
2. Verify that all emergency access arrangements for changes are appropriately authorised, documented and revoked after the change has been applied.				
3. Monitor all emergency changes, and conduct post-implementation reviews involving all concerned parties. The review should consider and initiate corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity.				
4. Define what constitutes an emergency change.				

REFERÊNCIAS BIBLIOGRÁFICAS

[1] International Organization for Standardization. **ISO/IEC 38500 – Corporate governance of information technology.** ISO, 2008, 22p.

[2] ABREU, Vladimir Ferraz de; FERNANDES, Aguinaldo Aragon. **Implantando a Governança de TI: da estratégia à gestão dos processos e serviços.** Rio de Janeiro: Brasport, 2006.

[3] Vaz, Wesley. **Palestra COBIT 5: Aspectos Gerais.** II Enauti. 2013. Acesso em: http://www.tc.df.gov.br/seset/encontrodeti/download/COBIT 5%20MINI%20CURSO%20ENAUTI%20-%206%20-%202013%20-%20FORMATADO.pdf

[4]. **COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.** USA, 2012

[5] PwC. **Por que conhecer o COBIT ® 5.**
Acesso em: www.pwc.com.br/

[6] GAEA. **Compreendendo os principais conceitos do COBIT 5.**
Acesso em: http://www.gaea.com.br/cms/compreendendo-os-principais-conceitos-do-COBIT -5-parte-v/

[7] ISACA. **Comparing COBIT 4.1 and COBIT 5**.
Acesso em: http://www.isaca.org/COBIT /Documents/Compare-with-4.1.pdf

[8] Gentil, Frederico A. S., **Novidades do COBIT 5**.
Acesso em: http://fredgentil.com.br/artigos/novidades-do-COBIT -5/

[9] ISACA. ***COBIT 5: Enabling Process***. USA, 2012.

[10] BRASIL. Lei n° 12.965/2014, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Acesso em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

[11] CGI.br. **O CGI.br e o Marco Civil da Internet**.
Acesso em: http://www.cgi.br