

Apostila

COBIT 5

*Framework de Governança e Gestão
Corporativa de TI*

Luzia Dourado

Janeiro, 2015

<http://lmdourado.wordpress.com>

Olá, entusiastas de governança de TI!

Eis que disponibilizo mais uma versão da apostila de COBIT 5 para auxiliar nos estudos!

Devido a grande procura por este material (mais de 10.000 downloads ☺) e à publicação da versão do COBIT 5 em português, resolvi revisá-lo e atualizá-lo para estar em conformidade com a tradução oficial.

Eu não esperava que esse material pudesse ser tão procurado! Muitos estão utilizando esse material para auxiliar nos estudos para concursos e ultimamente muitos também o utilizam como forma de revisão para a prova de certificação. Fico muito feliz por isso e muito agradecida pelo feedback de vocês!

Um lembrete: não fique limitado a essa apostila! Ela foi produzida para que o leitor tome rápido conhecimento do framework, porém, é só mais uma ferramenta de estudos, ok?

Ah, e nunca se esqueçam disso:

***“O saber a gente aprende com os mestres e com os livros.
A sabedoria a gente aprende com a vida e com os humildes”.***

Cora Coralina

Bons estudos a todos! Deus os abençoe!

Força, Foco e FÉ!

Janeiro, 2015



Imdourado@hotmail.com

COBIT® é uma marca registrada da ISACA e do IT Governance Institute (ITGI). Outros nomes de produtos e marcas registradas podem ser mencionados no decorrer desta apostila, tais marcas são utilizadas apenas com finalidade de ensino, em benefício exclusivo do dono da marca, sem intenção de infringir suas regras de utilização.

Apostila COBIT 5 de Luzia Dourado está licenciado com uma Licença Creative Commons - Atribuição-Compartilhual 4.0 Internacional.

Sumário

1. INTRODUÇÃO	3
2. O QUE HÁ DE NOVO?	7
3. EVOLUÇÃO.....	9
4. PRINCÍPIOS	10
Princípio 1. Atender as necessidades das partes interessadas (<i>stakeholders</i>)	11
Princípio 2. Cobrir a organização de ponta a ponta.....	13
Princípio 3. Aplicar um <i>framework</i> único e integrado	15
Princípio 4. Possibilitar uma abordagem holística	16
Princípio 5. Distinguir a governança de gestão.....	20
5. MODELO DE REFERÊNCIA DE PROCESSOS.....	21
6. GUIA DE IMPLEMENTAÇÃO.....	25
Criar o ambiente apropriado.....	26
Reconhecer os pontos de dor (<i>pain points</i>) e eventos desencadeadores (<i>trigger events</i>)	26
Elaborar caso de negócios (business case)	27
Ciclo de Vida de Implementação.....	28
7. MODELO DE CAPACIDADE DE PROCESSOS	30
Diferenças entre o Modelo de Maturidade COBIT 4.1 e o Modelo de Capacidade COBIT 5..	30
Modelo de Maturidade COBIT 4.1	30
Modelo de Maturidade COBIT 5	31
Diferenças na Prática.....	37
Benefícios das Mudanças	39
8. PRINCIPAIS DIFERENÇAS DO COBIT 5 COM RELAÇÃO AO COBIT 4.1	40
ANEXO I: Cascata de Objetivos do <i>COBIT 5</i>	42
ANEXO II: Exemplo de Habilitador: Processos	47
ANEXO III: Domínios e Processos	48
ANEXO IV: Mapeamento de processos COBIT 5 X COBIT 4.1.....	55
ANEXO V: Descrição do Processo BAI06: Gerenciar Mudanças	57
REFERÊNCIAS BIBLIOGRÁFICAS	59

1. INTRODUÇÃO

Antes de introduzir 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 [1]:

Governança Corporativa de TI, segundo ISO/IEC 38500:



“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.”.

A norma orienta que os dirigentes da organização governem a TI por meio de três tarefas principais, conforme pode ser visto na figura 1:

- **Avaliar** o uso atual e futuro da TI;
- **Dirigir** 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.

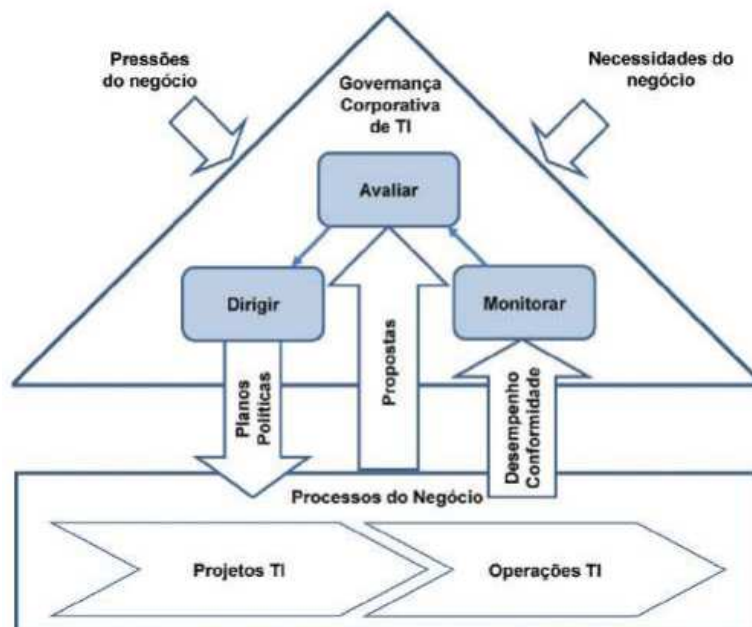


Figura 1 - Modelo de governança corporativa de TI.
Fonte: ISO/IEC 38500, pág. 13 [1]

Segundo a norma, Avaliar (**Evaluate**) significa que os dirigentes devem avaliar o uso atual e futuro da TI, incluindo as estratégias, propostas e arranjos de fornecimento (interno, externo ou ambos). Na avaliação do uso da TI, convém que os dirigentes considerem as pressões externas e internas que influenciam o negócio (mudanças tecnológicas, tendências econômicas e sociais e influências políticas), e levem em conta as necessidades atuais e futuras do negócio.

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

Monitorar (**Monitor**) significa que os dirigentes 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 corporativos 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, sendo 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 [1]:



Gestão de TI, segundo ISO/IEC 38500:

“Sistema de controles e processos necessários para alcançar os objetivos estratégicos estabelecidos pela direção da organização.”.

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.

Para quê as organizações necessitam de governança corporativa de TI?

As organizações existem para atender as necessidades de suas partes interessadas, ou seja, partes que se interessam ou são afetadas pela organização, tais como acionistas, funcionários, seus clientes, dentre outros.

Para atender aos seus objetivos estratégicos, as organizações se esforçam para:

- manter informações de alta qualidade para apoiar decisões corporativas;
- agregar valor ao negócio a partir dos investimentos em TI, ou seja, atingir os objetivos estratégicos e obter benefícios para a organização através da utilização eficiente e inovadora de TI;
- alcançar excelência operacional por meio da aplicação confiável e eficiente da tecnologia;
- manter o risco de TI em um nível aceitável;
- otimizar o custo da tecnologia e dos serviços de TI;
- cumprir as leis, regulamentos, acordos contratuais e políticas pertinentes cada vez mais presentes.

A governança corporativa de TI auxilia as organizações no alcance de seus objetivos estratégicos, por meio da **geração de valor** obtido pelo uso da TI, mantendo equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos. Para se obter essa geração de valor, é necessária a avaliação do uso da TI e das necessidades de investimentos nessa área; fornecer o direcionamento para que a TI atenda aos objetivos corporativos e monitorar as ações relacionadas a TI para estar em conformidade com o que foi planejado e para dar transparências às partes interessadas sobre os resultados alcançados.

Organizações bem-sucedidas reconhecem que a diretoria e os executivos devem aceitar que a TI é tão significativa para os negócios como qualquer outra parte da organização. Diretores e gestores - seja em funções de TI ou de negócios - devem colaborar e trabalhar em conjunto a fim de garantir que a TI esteja inclusa na abordagem de governança e gestão. Além disso, cada vez mais leis e regulamentos estão sendo aprovados e estabelecidos para atender a essa necessidade.

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, a saber:

- COBIT 4.1;
- Val IT, que pode ser usado para criar valor para o negócio por meio de investimentos de TI, sendo constituído por um conjunto de princípios orientadores e conjunto de processos e melhores práticas para apoiar e ajudar a gestão executiva em nível empresarial;
- Risk IT, dedicado a auxiliar no gerenciamento de riscos relacionados a TI;

- *Business Model for Information Security* (BMIS), que é uma abordagem holística e orientada ao negócio para a gestão de segurança da informação;
- *IT Assurance Framework* (ITAF), um modelo que fornece orientações sobre a concepção, realização e relatório de auditoria de TI, definindo termos e conceitos específicos para garantia de TI;
- *Taking Governance Forward* (TGF);
- *Board Briefing on IT Governance 2nd Edition*, que apresenta uma descrição abrangente dos conceitos de governança de TI como um livreto de referência ou como uma ferramenta para educar o board e a gerência executiva.

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 auxilia as organizações na **criação de 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.

Para quê um novo framework?

O COBIT 5 fornece a próxima geração de orientações da ISACA sobre governança corporativa e gestão de TI. Baseia-se em mais de 15 anos de uso e aplicação prática do COBIT por muitas organizações e usuários das comunidades de negócios, TI, risco, segurança e garantia. Os principais fatores para o desenvolvimento do COBIT 5 incluem as necessidades de:

- Permitir que mais partes interessadas falem sobre o que eles esperam da tecnologia da informação e tecnologias relacionadas (que benefícios e em qual nível de risco aceitável e a qual custo) e quais são suas prioridades para garantir que o valor esperado seja efetivamente obtido;
- Abordar a questão da dependência cada vez maior para o sucesso da organização em parceiros externos de TI e de negócios tais como terceirizadas, fornecedores, consultores, clientes, provedores de serviços na nuvem e demais serviços;
- Tratar a quantidade de informação, que tem aumentado significativamente;
- Administrar TI cada vez mais pervasiva; TI é cada vez mais uma parte integrante do negócio;
- Cobrir o negócio de ponta a ponta e todas as áreas responsáveis pelas funções de TI.

2. O QUE HÁ DE NOVO?

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 enablers¹** (ou habilitadores) **que otimizam investimentos em tecnologia e informação utilizados para o benefício das partes interessadas**.

O COBIT 5 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 *framework* é genérico e útil para organizações de todos os portes, sejam comerciais, sem fins lucrativos ou públicas.

Em sua quinta versão, o COBIT 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 COBIT 5 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, descritos cada um em um capítulo distinto
- ✓ Visão dos 7 habilitadores 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 RACI², 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.

¹ Enabler = viabilizador, facilitador, habilitador.

² Matriz RACI define o Responsável, Aprovador, Consultado e Informado em relação a uma tarefa.

A distinção entre 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, conforme pode ser visto na tabela 1.

Área	Qtde. de Processos	Domínios
Governança	5	Avaliar, Dirigir e Monitorar (<i>Evaluate, Direct and Monitor - EDM</i>)
Gestão	32	Alinhar, Planejar e Organizar (<i>Align, Plan and Organise - APO</i>); Construir, Adquirir e Implementar (<i>Build, Acquire and Implement - BAI</i>); Entregar, Serviços e Suporte (<i>Deliver, Service and Support - DSS</i>) Monitorar, Avaliar e Analisar (<i>Monitor, Evaluate and Assess - MEA</i>)

Tabela 1 Quantidade de processos e domínios de Governança e Gestão

COBIT 5 é:



- ✓ **Focado em governança corporativa de TI**
- ✓ **Deixa clara a distinção entre governança e gestão**
- ✓ **Fundamentado em 5 princípios de governança corporativa de TI**
- ✓ **Baseado em um conjunto holístico de 7 enablers (ou habilitadores)**
- ✓ **Possui 37 processos de TI divididos em domínios de processo de governança e de gestão**

3. EVOLUÇÃO

O COBIT surgiu, 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 conformidade (*compliance*). E atualmente, na quinta versão, é o *framework* integrador de governança e gestão de TI corporativa. A figura 2 exibe um resumo da evolução do COBIT.

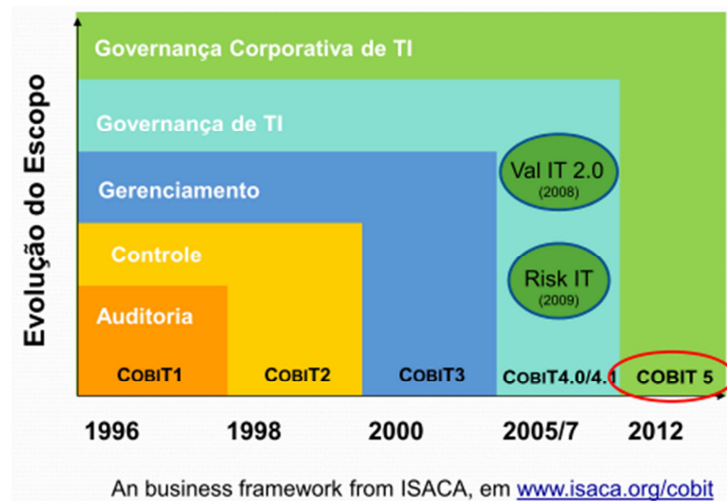


Figura 2 - Evolução do COBIT

4. PRINCÍPIOS

Conforme dito anteriormente, 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 enablers³ (ou habilitadores)** **que otimizam investimentos em tecnologia e informação utilizados para o benefício das partes interessadas.**

Os 5 princípios são (figura 3):

1. Atender às necessidades dos stakeholders (partes interessadas)
2. Cobrir a organização de ponta a ponta
3. Aplicar um *framework* (modelo) único e integrado
4. Permitir uma abordagem holística
5. Distinguir a governança da gestão



Figura 3 – Princípios do COBIT 5
Fonte: COBIT ® 5, p.15, ©2012 ISACA® [12]

Cada princípio será descrito a seguir.

³ Enabler = viabilizador, facilitador, habilitador

Princípio 1. Atender as necessidades das partes interessadas (*stakeholders*)

As organizações existem para criar valor para as partes interessadas (*stakeholders*), ou seja, para todas as partes interessadas (acionistas, auditores, fornecedores, consultores, alta administração, etc). Consequentemente, qualquer organização — comercial ou não — terá a criação de valor como um objetivo da governança (figura 4).



Figura 4 - Objetivo da Governança. Fonte: COBIT® 5, pag. 19, ©2012 ISACA® [12]

O que é criação de valor?



Criação de Valor

Obtenção de benefícios por meio da otimização do uso de recursos e dos riscos a um nível aceitável.

Os benefícios podem assumir muitas formas, por exemplo, financeiros para organizações comerciais ou de serviço público para entidades governamentais. Portanto, vale frisar que a criação de valor é o objetivo da governança! Para cada parte interessada, a criação de valor pode representar interesses diferentes e algumas vezes conflitantes.

O sistema de governança abrange negociar e decidir entre os diferentes interesses das partes interessadas 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?

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

Para isso, como pode ser visto na figura 5, há um mecanismo denominado **Cascata de Objetivos do COBIT 5** com a finalidade de desdobrar:

- os direcionadores (*drives*) e as necessidades dos *stakeholders* em objetivos corporativos;
- os objetivos corporativos em objetivos de TI;
- os objetivos de TI em objetivos para os habilitadores.



Figura 5 - Cascata de Objetivos
Fonte: COBIT® 5, p.20, ©2012 ISACA® [12]

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



A cascata de objetivos não é algo novo no COBIT 5, pois já existia no COBIT 4.1. No COBIT 4.1, os objetivos de TI são desdobrados em objetivos de processos que por sua vez, desdobram-se em objetivos de atividades. No COBIT 5, os objetivos de TI são desdobrados em objetivos de habilitadores, sendo Processos um dos habilitadores.

Que benefícios são obtidos por meio dessa cascata de objetivos?

A cascata de objetivos permite a definição de prioridades para implementação, melhoria 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 de responsabilidade;
- Filtra a base de conhecimento do COBIT 5, com base nos objetivos corporativos, para extrair a orientação pertinente para inclusão na implementação, melhoria ou garantia de projetos específicos;
- Identifica e comunica claramente como os habilitadores do COBIT (às vezes muito operacionais) são importantes para o alcance dos objetivos corporativos.

Mais detalhes sobre a [Cascata de Objetivos do COBIT 5](#) 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 da organização;
- ✓ **Cobre todas as funções e processos necessários para regular e controlar as informações da organização e tecnologias correlatas onde quer que essas informações possam ser processadas;**
- ✓ **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.

O COBIT 5 fornece uma visão holística e sistêmica sobre a governança e gestão de TI da organização (ver princípio 4), que tem por base diversos habilitadores. Os habilitadores servem para toda a organização, de ponta a ponta, ou seja, incluem todas as pessoas e todas as coisas, internas e externas, pertinentes à governança e gestão das informações e TI da organização, inclusive as atividades e responsabilidades das funções corporativas de TI bem como aquelas não relacionadas com essas funções.

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):



Figura 6 - Governança e Gestão de TI no COBIT 5
Fonte: COBIT® 5, p. 25, ©2012 ISACA® [12]

- **Habilitadores 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:** definem quem está envolvido com governança, como estão envolvidos, o que fazem e como interagem dentro do escopo da governança.

A figura 7 mostra os papéis, atividades e relacionamentos que ocorrem na governança. As partes interessadas delegam para o Conselho de Administração a definição de direção para as atividades de gestão do Corpo Diretivo 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 o Corpo Diretivo, que é monitorado pelo Conselho de Administração que presta contas do desempenho para as partes interessadas.

Vale ressaltar que o COBIT 5 fornece, para cada processo, matrizes RACI⁴, em que estão incluídos papéis relacionados a TI e ao negócio.



Figura 7 - Papéis, Atividades e Relacionamentos. Fonte: COBIT ® 5, p. 26, ©2012 ISACA® [12]

⁴ Matriz RACI define o Responsável, Aprovador, Consultado e Informado em relação a uma tarefa.

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.

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

- ❖ COBIT 5 (o *framework*)
- ❖ Guia de habilitadores do COBIT 5, no qual os habilitadores de governança e gestão são discutidos em detalhe. Estes incluem:
 - COBIT 5: Habilitador Processos (*Enabling Processes*)
 - COBIT 5: Habilitador Informação (*Enabling Information*)
 - Outros guias habilitadores
- ❖ Guias profissionais do COBIT 5, que incluem:
 - *COBIT 5* Implementação
 - *COBIT 5* para Segurança da Informação
 - *COBIT 5* para Garantia (*Assurance*)
 - *COBIT 5* para Risco
 - Outros guias profissionais
- ❖ Um ambiente colaborativo on-line, que é disponibilizado para apoiar o uso do COBIT 5

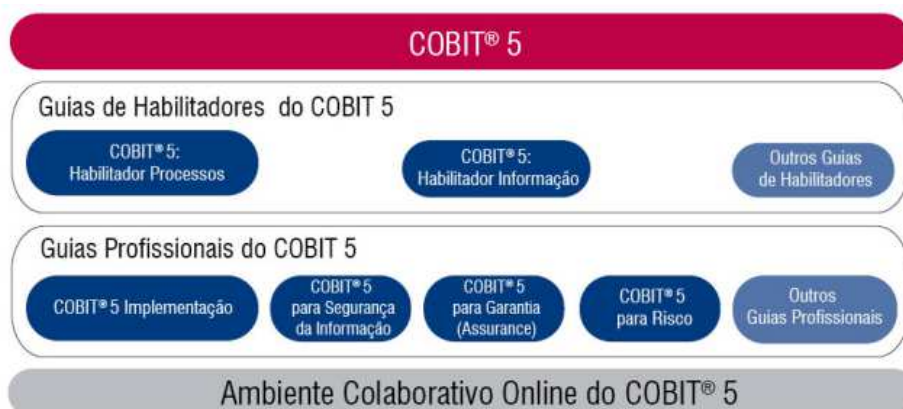


Figura 8 - Família de Produtos
Fonte: COBIT® 5, p. 28, ©2012 ISACA® [12]

Princípio 4. Possibilitar uma abordagem holística

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

Habilitadores (enablers)



Habilitadores

Fatores que, individual e coletivamente, influenciam o funcionamento da governança e gestão corporativas de TI.

Os habilitadores são orientados pela cascata de objetivos, ou seja, objetivos de TI em níveis mais alto definem o que os diferentes habilitadores deverão alcançar.

O *framework* COBIT 5 define 7 categorias de habilitadores (figura 9):



Figura 9 - Habilitadores. Fonte: COBIT® 5, p. 29, ©2012 ISACA® [12]

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

2. Processos descrevem um conjunto organizado de práticas e atividades para atingir determinados objetivos e produzem um conjunto de saídas que auxiliam no cumprimento dos objetivos de 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 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 estão associadas às pessoas e são necessárias para que as atividades sejam executadas com sucesso e para que decisões e ações corretivas sejam realizadas de forma correta.

Alguns dos habilitadores definidos acima também são recursos da organização que devem ser gerenciados e governados. Isto se aplica:

- ✓ A Informação, que deve ser gerenciada como um recurso. Algumas informações, tais como relatórios de gestão e informações de inteligência organizacional são importantes habilitadores para a governança e gestão da organização.
- ✓ Serviços, infraestrutura e aplicativos.
- ✓ Pessoas, habilidades e competências.

Uma organização sempre deverá considerar um conjunto de habilitadores interligados. Ou seja, cada habilitador:

- Necessita das informações dos demais habilitadores para ser plenamente efetivo, por exemplo, processos precisam de informações e modelos organizacionais necessitam de habilidades e comportamento.
- Produz resultados para o benefício dos demais habilitadores, por exemplo, os processos geram informações, e as habilidades e o comportamento tornam os processos eficientes.

Assim, ao tratar da governança e gestão corporativa de TI, boas decisões podem ser tomadas somente quando a natureza sistêmica dos arranjos de governança e gestão for considerada. Isto significa que, para tratar de qualquer necessidade das partes interessadas, a referência de todos os habilitadores inter-relacionados deve ser analisada e tratada, se necessário. Esta mentalidade deve ser orientada pela alta administração da organização.

Alguns habilitadores do COBIT 5 eram tratados no COBIT 4.1:



Os recursos de TI do COBIT 4.1 – processos, aplicações, informação e infraestrutura – são considerados habilitadores no COBIT 5.

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

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

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

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

Dimensões de habilitadores

Todos os habilitadores têm um conjunto de dimensões comuns (figura 10). Este conjunto de dimensões comuns [4]:

- Apresenta uma maneira comum, simples e estruturada para tratar dos habilitadores;
- Permite que a organização gerencie suas interações complexas;
- Facilita resultados bem sucedidos dos habilitadores.



Figura 10 - Dimensões de Habilitadores.
Fonte: COBIT® 5, p. 30, ©2012 ISACA® [12]

As quatro dimensões comuns para habilitadores são:

- **Partes Interessadas (stakeholders):** cada habilitador tem partes interessadas (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. Partes interessadas podem ser internas ou externas à organização, todos com seus interesses e necessidades.
 - Exemplos de partes interessadas internas: executivos de negócio, conselho de administração, gerentes de negócio, auditores internos, usuários de TI, etc.
 - Exemplo de partes interessadas externas: parceiros comerciais, fornecedores, governo, consumidores, auditores externos, consultores, etc.
- **Objetivos (goals):** cada habilitador tem uma série de objetivos e criam valor pela realização destes objetivos. Os objetivos podem ser definidos em termos de:
 - Resultados esperados do habilitador
 - Aplicação ou operação do próprio habilitador

Os objetivos de habilitadores são o passo final da cascata de objetivos do COBIT 5. Os objetivos são divididos em categorias:

- Qualidade intrínseca: o quanto os habilitadores trabalham de forma precisa, objetiva e produzem resultados exatos, objetivos e confiáveis.
 - Qualidade contextual: o quanto os habilitadores e seus resultados atendem ao seu objetivo levando-se em consideração o contexto em que operam.
 - Acessibilidade e segurança: o quanto os habilitadores e seus resultados são acessíveis e seguros.
- **Ciclo de vida (life cycle)**: cada habilitador tem um ciclo de vida, desde sua criação, passando por sua vida útil/operacional até chegar ao descarte.
- 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 habilitadores, boas práticas podem ser definidas. Boas práticas apoiam a realização dos objetivos do habilitador. Boas práticas fornecem exemplos ou sugestões sobre a melhor forma de implementar o habilitador, e quais os produtos de trabalho, entradas e saídas são necessários.

Gerenciamento de Desempenho dos Habilitadores

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

- As necessidades das partes interessadas foram atendidas?
- Os objetivos dos habilitadores foram alcançados?
- O ciclo de vida do habilitador é gerenciado?
- As boas práticas são aplicadas?

As duas primeiras questões lidam com o resultado real do habilitador e os indicadores usados 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 habilitador e os indicadores para **medir se os objetivos serão atingidos** podem ser chamadas de "indicadores de desempenho" (**lead indicators**).

Como exemplo de um habilitador na prática, veja no [Anexo II](#).

Princípio 5. Distinguir 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. O ponto de vista do COBIT 5 sobre esta fundamental distinção entre governança e gestão é:

Governança



A governança garante que as necessidades, as condições e as opções das partes interessadas sejam avaliadas a fim de determinar os objetivos corporativos acordados e equilibrados; define a direção por meio de priorização e tomada de decisão; e provê monitoramento de desempenho e conformidade com relação aos objetivos estabelecidos.

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**, 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.

Gestão



A gestão consiste em planejar, construir, executar e monitorar atividades alinhadas com a direção estratégica estabelecida pela governança para atingir os objetivos corporativos.

Na maioria das organizações, **a gestão é da responsabilidade da gerência executiva**, sob a liderança do chefe diretor executivo (CEO).

5. MODELO DE REFERÊNCIA DE PROCESSOS

O modelo de referência de processo do COBIT 5 é o sucessor do modelo de processo do COBIT 4.1, e conta ainda com a integração dos modelos de processo do Risk IT e Val IT. O modelo **subdivide os 37 processos de TI em duas principais áreas de atividade – governança e gestão** – divididas em domínios de processos, conforme figura 11.

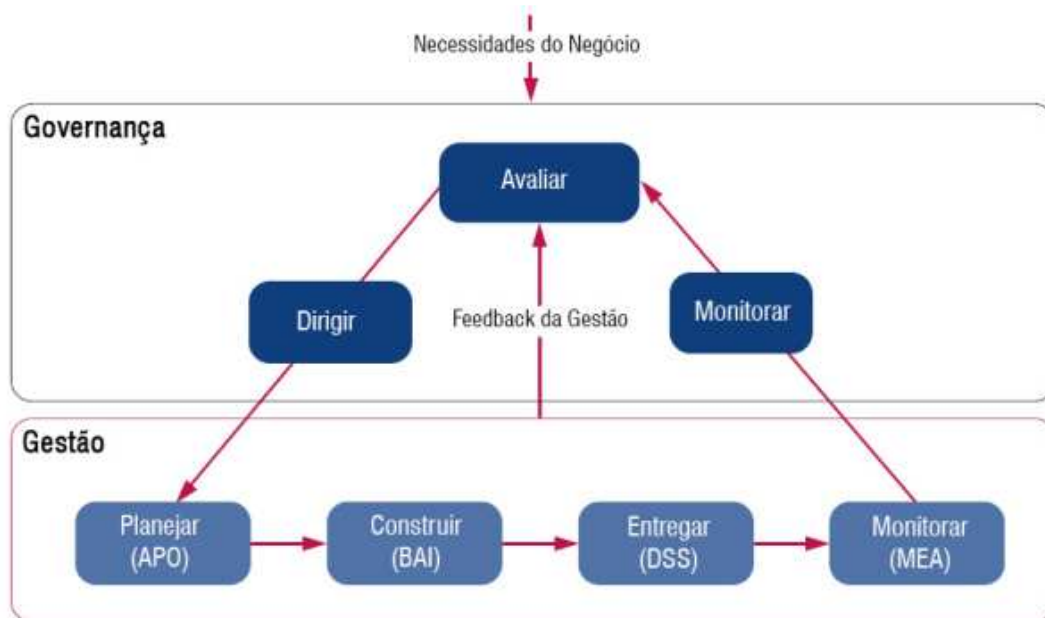


Figura 11 - Áreas chave de governança e gestão.
Fonte: COBIT® 5, p. 34, ©2012 ISACA® [12]

Processos de Governança

Contém **1 domínio Avaliar, Dirigir e Monitorar (Evaluate, Direct and Monitor - 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 [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 (Align, Plan and Organise - APO)**

O domínio APO diz respeito à identificação de como a TI pode contribuir melhor com os objetivos corporativos. 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]

- **Construir, Adquirir e Implementar (*Build, Acquire and Implement - 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, Serviços e Suporte (*Deliver, Service and Support - 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 Analisar (*Monitor, Evaluate and Assess - 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 12 exibe os 37 processos de governança e gestão do COBIT 5. Os detalhes de cada processo estão no **COBIT 5: Enabling Processes** [9].

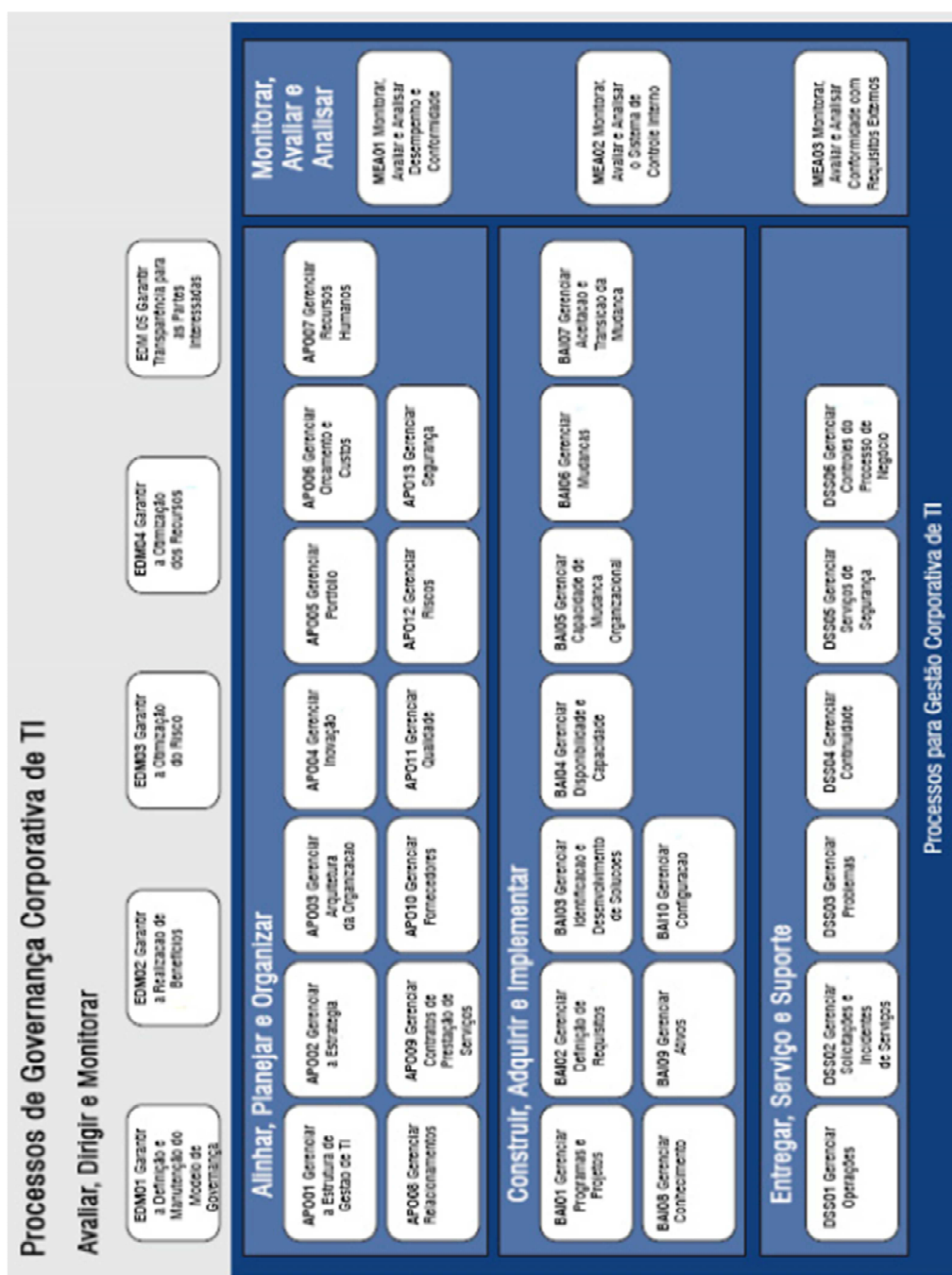


Figura 12 - Modelo de Referência de Processos.
Fonte: COBIT® 5, p. 35, ©2012 ISACA® [12]

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.

6. GUIA DE IMPLEMENTAÇÃO

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]:

- ✓ Ferramentas de autoavaliação, medição e diagnóstico
- ✓ Apresentações destinadas a vários públicos
- ✓ Artigos relacionados explicações adicionais

No documento relativo ao *framework* COBIT 5 é apresentada uma introdução à implementação e ao ciclo de vida de melhoria contínua.

Mas como começar a implementação?

O COBIT 5 apresenta uma abordagem de implementação baseada na melhoria contínua, sendo necessário:

- ✓ Criar o ambiente apropriado para a implementação;
- ✓ Reconhecer os pontos de dor (*pain points*) típicos e eventos desencadeadores (*trigger events*);
- ✓ Adotar um ciclo de vida de implementação;
- ✓ Elaborar caso de negócios (*business case*) para a implementação e melhoria da governança e gestão de TI.

Antes da 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
- Appetite ao risco
- Capacidades e recursos disponíveis
- Práticas da indústria

A abordagem ideal à governança e gestão corporativa de TI será diferente para cada organização e o contexto deve ser entendido e considerado a fim de adotar e adaptar o COBIT com eficiência na implementação dos habilitadores de governança e gestão de TI da organização.

Criar o ambiente apropriado

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.

Reconhecer os pontos de dor (*pain points*) e eventos desencadeadores (*trigger events*)

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 desencadeadores (*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 para o negócio, tais como perda de dados ou falha em projetos;
- Problemas com terceirização da prestação de serviços, tais como o não cumprimento de forma consistente dos níveis de serviço acordados;
- Ausência de cumprimento de requisitos legais ou contratuais;
- Resultados da auditoria sobre o fraco 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 ações de governança e gestão corporativa de TI, ou seja, que faz a TI atuar em resposta a esses eventos. 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.
- Uma nova estratégia ou de negócio.

Elaborar caso de negócios (business case)

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 todas partes interessadas e ser baseada em um caso de negócio (*business case*).** Inicialmente, isto pode ser feito em alto nível do ponto de vista estratégico, 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.** Um caso de negócio justifica um projeto ou solução proposta com base nos seus benefícios esperados e serve para dar suporte à decisão de implementar ou não tal projeto ou solução.

No mínimo, o caso de negócios deve incluir o seguinte:

- Os benefícios almejados para a organização, seu alinhamento com a estratégia de negócios e os respectivos responsáveis pelo benefício (que serão os responsáveis na organização pela sua garantia). Isto pode basear-se em pontos fracos e eventos desencadeadores;
- 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 incluído no escopo e o que não está;
- 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 como os indicadores serão utilizados (com base em objetivos e métricas).

O caso de negócio não é um documento estático definitivo, mas uma ferramenta operacional e dinâmica que deve ser continuamente atualizada para refletir a atual visão do futuro para que uma visão da viabilidade do programa possa ser mantida.

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:

- **Ciclo de vida principal de melhoria contínua** - Este não é um projeto isolado.
- **Capacitação da mudança** – aborda os aspectos comportamentais e culturais, de forma a garantir que todas as partes interessadas estão preparadas e comprometidas com as mudanças necessárias para alcançar um estado futuro desejado.
- **Gestão do programa**

O ciclo de vida possui **7 fases** como está ilustrado na figura 13:

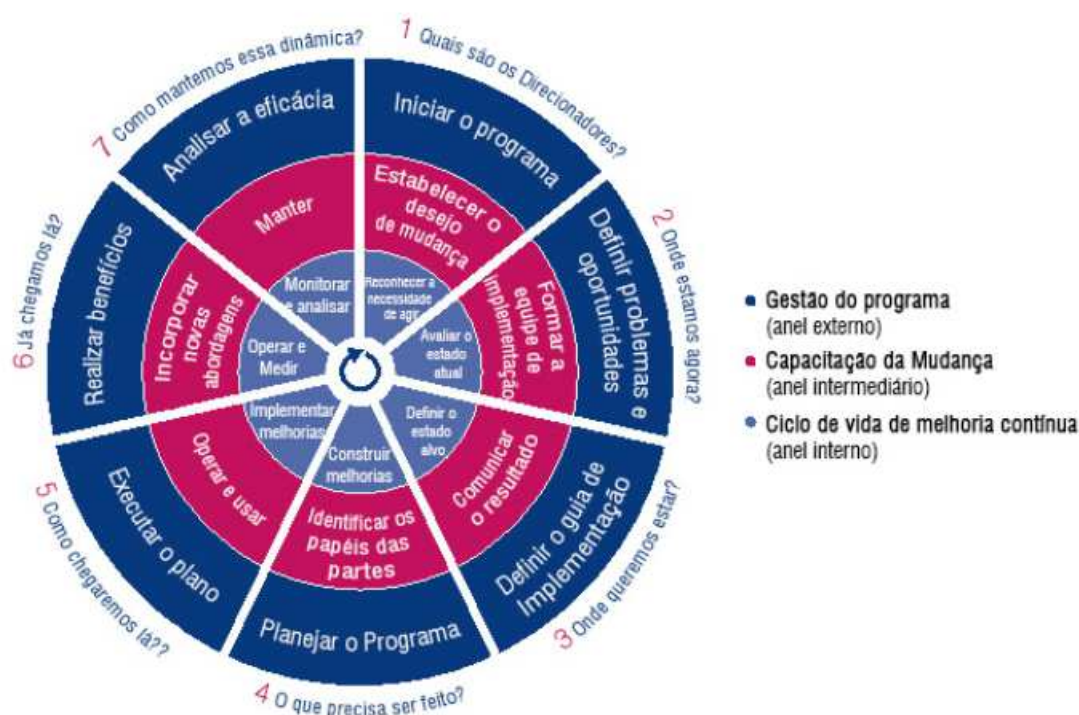


Figura 13 - Fases do Ciclo de Vida.

Fonte: COBIT® 5, p. 39, ©2012 ISACA® [12]

Fase 1- Quais são os direcionadores?: começa com o reconhecimento e aceitação da necessidade de uma iniciativa de implementação ou melhoria. Identifica os pontos de dor atuais e os direcionadores de mudança que cria um desejo de mudança nos níveis de gestão

executiva. Um direcionador de mudança é um evento interno ou externo, condição ou problema que serve como um estímulo para a mudança.

Fase 2 – Onde estamos agora?: está focada em definir o escopo da iniciativa de implementação ou melhoria utilizando o mapeamento dos objetivos corporativos com os objetivos de TI para os processos de TI associados, considerando como cenários de risco também poderiam destacar os principais processos em que se deve concentrar. Uma vez priorizados os objetivos corporativos, objetivos de TI e processos associados mais importantes, é realizado uma avaliação do estado atual, e problemas ou deficiências são identificados realizando-se uma avaliação de capacidade de processo nos processos críticos selecionados. A presença de pontos de dor específicos também poderia contribuir para a seleção de processos de TI em que se deve concentrar. 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 perda da dinâmica, foco e adesão das partes interessadas.

Fase 3 – Onde queremos estar?: um objetivo de melhoria é definido e seguido por uma análise mais detalhada para identificar as lacunas e as possíveis soluções. Devem ser priorizadas as iniciativas que são mais fáceis de realizar e as susceptíveis de produzir os maiores benefícios.

Fase 4 – O que precisa ser feito?: planeja soluções práticas por meio 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 – Como chegaremos lá?: as soluções propostas são implementadas na forma de práticas diárias. As medidas podem ser definidas e o monitoramento estabelecido, utilizando metas e indicadores do COBIT para garantir que o alinhamento de negócios seja alcançado e mantido e o desempenho possa ser medido.

Fase 6 – Já chegamos lá?: concentra-se na operação sustentável dos habilitadores novos ou melhorados e o monitoramento da realização dos benefícios esperados.

Fase 7 – Como mantemos essa dinâmica?: o sucesso global da iniciativa é revisado, outros requisitos para a governança ou gestão de organizações de TI são identificadas e a necessidade de melhoria contínua é reforçada.

7. 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, ele proporcionará meios para medir o desempenho de qualquer um dos processos de governança (baseados em EDM) ou processos de gestão (baseados em PBRM) e permitirá a identificação das áreas que precisam ser melhoradas.

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 habilitadores 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 habilitadores precisam ser avaliados também!**



Para se obter um quadro completo sobre o estado de governança de uma organização, todos os habilitadores precisam ser avaliados!

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

Modelo de Maturidade COBIT 4.1

Para utilizar o modelo de maturidade do COBIT 4.1 para a melhoria do processo são necessários os seguintes componentes do COBIT 4.1 (figura 14):

- Em primeiro lugar, uma avaliação deverá ser realizada para confirmar se os objetivos de controle do processo foram atingidos;
- 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 aplicáveis para cada processo e que ajudam na obtenção de uma visão mais detalhada do nível de maturidade dos processos;

- Controles de processos são objetivos de controle genéricos que também precisam ser analisados quando uma avaliação do processo for realizada. Controles de processos se sobrepõem parcialmente com os atributos genéricos do modelo de maturidade.

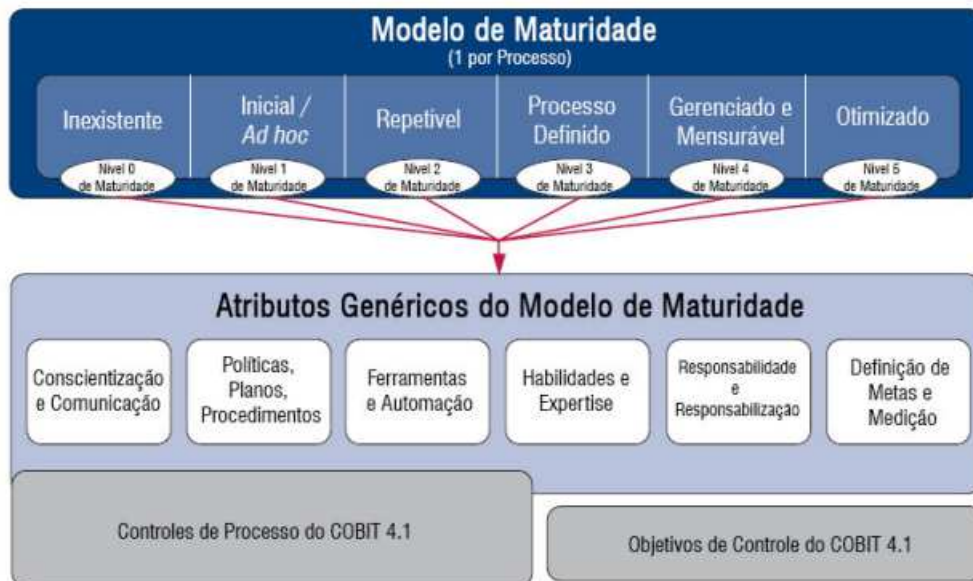


Figura 14 - Modelo de Maturidade do COBIT 4.1.
Fonte: : COBIT ® 5, p. 43, ©2012 ISACA® [12]

Modelo de Capacidade COBIT 5

O modelo de capacidade de processos do COBIT 5 é exibido na figura 15.

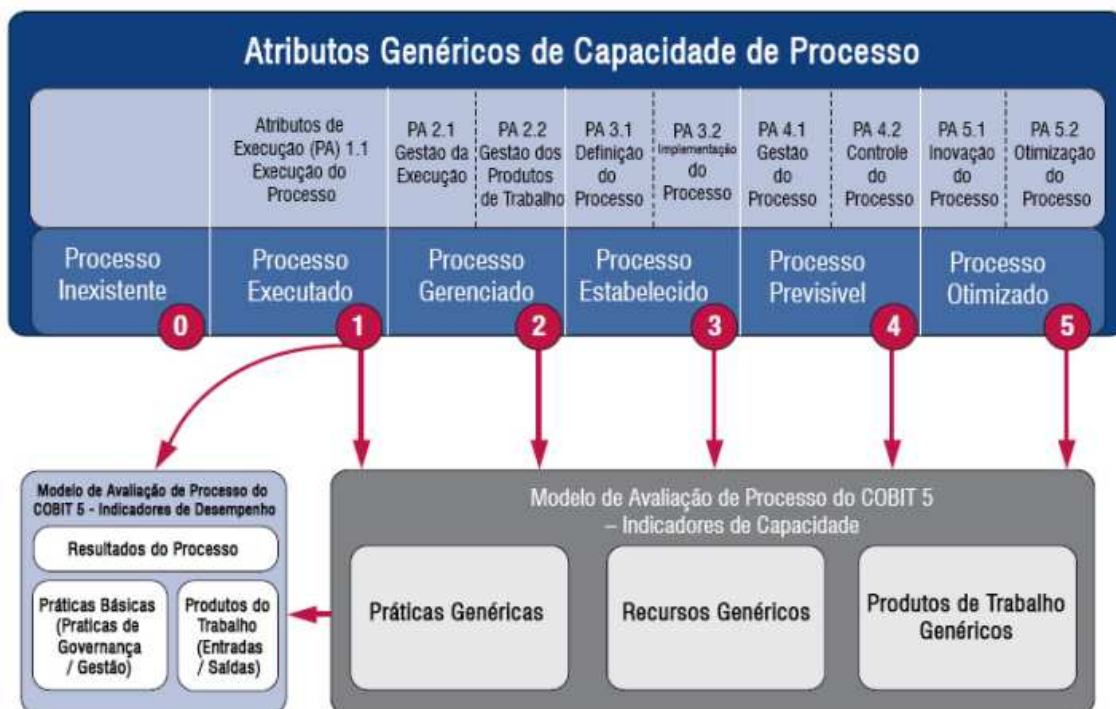


Figura 15 - Modelo de Capacidade de Processos.
Fonte: COBIT ® 5, p. 44, ©2012 ISACA® [12]

Níveis de capacidade

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. **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 níveis de capacidade são:

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

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

Nível 2 - Processo Gerenciado: 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. Possui os atributos PA2.1 – Gerenciamento de Desempenho (Performance Management) e PA2.2 – Gerenciamento de Produto de Trabalho (Work Product Management).

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

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

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



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).

Atributos de processo

Atributos de processo (PA – Process Attributes) 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 9 atributos de processo são:

- PA1.1 – Desempenho do Processo (Process Performance)
- PA2.1 – Gestão do Desempenho (Performance Management)
- PA2.2 – Gestão dos Produtos de Trabalho (Work Product Management)
- PA3.1 – Definição do Processo (Process Definition)
- PA3.2 – Implementação do Processo (Process Deployment)
- PA4.1 – Gestão do Processo (Process Management)
- PA4.2 – Controle do Processo (Process Control)
- PA5.1 – Inovação do Processo (Process Innovation)
- PA5.2 – Otimização do Processo (Process Optimization)

Vale destacar que o nível 1 apresenta um método de avaliação diferente dos demais. O Atributo PA 1.1 – Execução do Processo utiliza práticas e produtos de trabalho (artefatos associados à execução do processo) específicos de cada processo, enquanto os demais atributos se baseiam em práticas e produtos de trabalho genéricos aplicáveis a todos os processos [13].

A seguir são apresentadas as descrições e os resultados esperados para cada atributo [13][14].

PA1.1 – Desempenho do Processo: avalia se o processo atinge o seu objetivo. É avaliado se as atividades básicas e os produtos de trabalho do processo são executados de alguma forma, não sendo necessária a formalização e documentação dos mesmos.

PA2.1 – Gestão do Desempenho: avalia se o desempenho do processo é gerenciado. Como resultado da plena realização desse atributo:

- ✓ os objetivos de desempenho do processo são definidos;
- ✓ o desempenho do processo é planejado, monitorado e ajustado para atingir o planejado;
- ✓ responsabilidades para execução do processo são definidas, atribuídas e comunicadas;
- ✓ recursos e informações necessárias para executar o processo são identificados, estão disponíveis, alocados e utilizados;
- ✓ interface entre as partes envolvidas no processo são gerenciadas para garantir a eficácia na comunicação e clareza na definição de responsabilidades.

PA2.2 – Gestão dos Produtos de Trabalho: avalia se os produtos de trabalho produzido pelo processo são apropriadamente gerenciados. Como resultado da plena realização desse atributo:

- ✓ requisitos para os produtos de trabalho do processo são definidos;

- ✓ requisitos para documentação e controle dos produtos de trabalho são definidos;
- ✓ produtos de trabalho do processo são devidamente identificados e controlados;
- ✓ produtos de trabalho do processo são revisados de acordo com os critérios definidos e ajustados para atender aos requisitos.

PA3.1 – Definição do Processo: busca avaliar se um processo padrão é mantido de forma que auxilie a implantação de um processo definido. Como resultado da plena realização desse atributo:

- ✓ um processo padrão, incluindo orientações para adaptação, é definido e descreve os elementos fundamentais que devem ser incorporados a um processo definido;
- ✓ a sequência e interação do processo padrão com outros processos são determinadas;
- ✓ papéis e competências necessárias para a realização de um processo são identificados como parte do processo padrão;
- ✓ infraestrutura necessária e ambiente de trabalho para a realização do processo são identificados;
- ✓ métodos para monitorar a eficácia e adequação do processo são determinados.

PA3.2 – Implementação do Processo: busca avaliar se um processo padrão é eficientemente implantado como um processo definido. Como resultado da plena realização desse atributo:

- ✓ um processo definido é implantado baseado na escolha e adequação de um processo padrão;
- ✓ papéis e responsabilidades para executar o processo definido são alocados e comunicados;
- ✓ atores do processo definido possuem experiência e são adequadamente treinados;
- ✓ recursos e informações necessárias para a execução do processo definido estão disponíveis, alocados e são utilizados;
- ✓ infraestrutura e ambientes necessários para a execução do processo definido estão disponíveis, são gerenciados e mantidos;
- ✓ os dados apropriados são coletados e analisados para entendimento do comportamento, demonstração da efetividade e avaliação de melhorias contínuas do processo definido.

PA4.1 – Gestão do Processo: busca avaliar se resultados de medição de desempenho do processo são utilizados para garantir o atingimento de objetivos do processo, em suporte a metas de negócio. Como resultado da plena realização desse atributo:

- ✓ necessidades de informação do processo são definidas de acordo com os objetivos de negócio;
- ✓ os objetivos de medição do processo são derivados da necessidade de informação do mesmo;
- ✓ objetivos quantitativos para o desempenho do processo são estabelecidos de acordo com as necessidades do negócio;

- ✓ medidas e frequência de medição são identificadas e definidas de acordo com os objetivos de medição do processo e os objetivos quantitativos para o desempenho do processo;
- ✓ os resultados de medição são coletados, analisados e reportados a fim de avaliar e os objetivos quantitativos do processo são atingidos.

PA4.2 – Controle do Processo: busca avaliar se o processo é quantitativamente gerenciado, de modo que seja estável e previsível dentro de limites preestabelecidos. Como resultado da plena realização desse atributo:

- ✓ técnicas de controle e análise são definidas e aplicadas;
- ✓ limites de variação do processo são definidos para uma performance normal do processo;
- ✓ os dados de medição são analisados para causas especiais de variação;
- ✓ ações corretivas são tomadas para endereçar as variações observadas e
- ✓ os limites de controle são reestabelecido (se necessário) de acordo com ações corretivas.

PA5.1 – Inovação do Processo: busca avaliar se mudanças para o processo são identificadas através de análises de causas comuns de variação no desempenho e da investigação de abordagens inovadoras para a definição e implementação do processo. Como resultado da plena realização desse atributo:

- ✓ objetivos de melhoria do processo são definidos de acordo com os objetivos de negócio;
- ✓ dados apropriados são analisados para a identificação de causas comuns às variações do processo;
- ✓ dados apropriados são analisados para identificar oportunidades para melhores práticas e inovação;
- ✓ oportunidades de melhorias derivadas de novas tecnologias e conceitos de processo são identificadas;
- ✓ uma estratégia de implementação é estabelecida para atingimento dos objetivos de melhoria.

PA5.2 – Otimização do Processo: busca avaliar se mudanças em definições, gerenciamento e desempenho do processo causaram impactos efetivos no atingimento do objetivo de melhorias. Como resultado da plena realização desse atributo:

- ✓ os impactos de todas as mudanças propostas são avaliados frente aos objetivos do processo definido e padrão;
- ✓ a implementação de todas as mudanças acordadas é gerenciada para garantir que qualquer interrupção no desempenho do processo é entendida e corrigida;
- ✓ com base no desempenho atual, a eficácia da mudança no processo é avaliada em função dos requisitos de produtos definidos e objetivos de processo para determinar se os resultados são devidos às causas identificadas.

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

Escala	Descrição	% de realização
N (não alcançado)	Há pouca ou nenhuma evidência de realização do atributo de processo no processo avaliado	0% a 15%
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%
L (largamente alcançado)	Há evidências 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%
F (totalmente alcançado)	Há evidências 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%

Tabela 2 Escala de avaliação dos atributos de processo.

Fonte: [13]



O alcance de um determinado nível de capacidade requer que os atributos para este nível estejam totalmente ou largamente (F ou L) alcançados e os atributos para todos os níveis inferiores estejam "totalmente" (F) alcançados.

Portanto, para o alcance do nível 2, por exemplo, é preciso que o PA 2.1 e PA 2.2 sejam avaliados como F ou L e o PA 1.1 seja avaliado como F (figura 16). [13]

Atributos

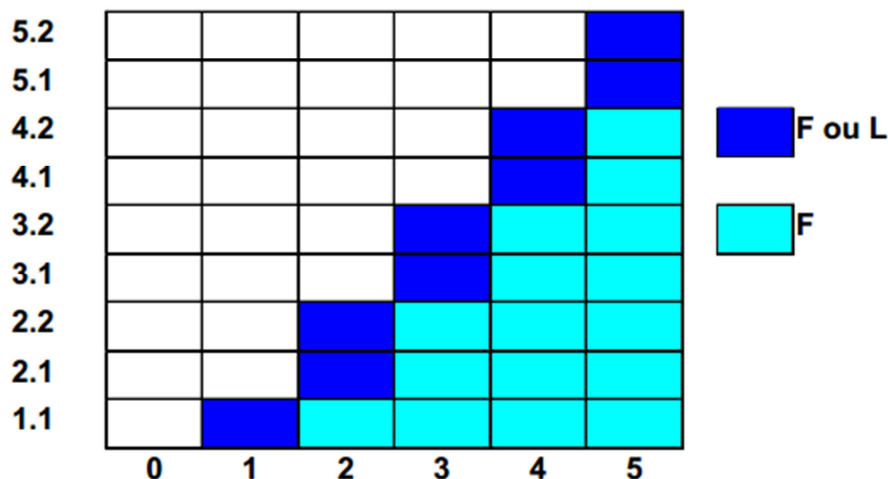


Figura 16 Avaliação dos atributos por nível de capacidade.

Fonte: [15]

Diferenças na Prática

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.**



O modelo de maturidade do COBIT 4.1 não é considerado compatível com o modelo da ISO/IEC 15504 porque os métodos usam diferentes atributos e escalas de medição!

Níveis de Maturidade (COBIT 4.1) x Níveis de Capacidade de Processo (COBIT 5)	
COBIT 4.1	COBIT 5 (com base na ISO/IEC 15504)
Nível 5: Processo Otimizado - processos são refinados ao nível de boa prática, baseados nos resultados de melhoria contínua e modelagem da maturidade com outras organizações. A TI é utilizada de forma integrada para automatizar o fluxo de trabalho, fornecendo ferramentas para melhorar a qualidade e eficácia, fazendo com que a organização se adapte rapidamente.	Nível 5: Processo em Otimização - o nível 4 Processo Previsível é continuamente melhorado para atender objetivos corporativos atuais ou previstos.
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 obrigatório 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 resultados 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 similares 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.
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 disso, existem abordagens <i>ad hoc</i> que tendem a ser aplicadas por indivíduos. A abordagem geral de gerenciamento é desorganizada.	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 0: Não 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 3 - Comparação Níveis de Maturidade COBIT 4 x Níveis de Capacidade COBIT 5. Fonte: COBIT® 5, p. 46, ©2012 ISACA® [12]

Benefícios das Mudanças

Os benefícios do modelo de capacidade de processo do COBIT 5, comparados com os modelos de maturidade do COBIT 4.1 incluem:

- ❖ Maior ênfase no processo que está sendo realizado para confirmar que está efetivamente alcançando seus objetivos e os resultados esperados.
- ❖ Simplificação do conteúdo por meio da eliminação da duplicação, porque a avaliação do modelo de maturidade do COBIT 4.1 exigia o uso de diversos componentes específicos, inclusive o modelo de maturidade genérico, modelos de maturidades do processo, objetivos de controle e controles de processo para apoiar a avaliação do processo.
- ❖ Maior confiabilidade e repetitividade das atividades e análises da avaliação da capacidade do processo, reduzindo debates e desentendimentos entre as partes interessadas em relação aos resultados da avaliação.
- ❖ Maior uso dos resultados da avaliação da capacidade do processo, visto que o novo modelo estabelece uma base para a realização de avaliações mais rigorosas e formais, tanto para finalidades internas como externas em potencial.
- ❖ Conformidade com um padrão de avaliação de processo geralmente aceito e, portanto, um forte apoio à abordagem de avaliação do processo no mercado.

8. PRINCIPAIS DIFERENÇAS DO COBIT 5 COM RELAÇÃO AO COBIT 4.1

O COBIT 5 trouxe uma série de mudanças em relação à última versão, o CobiT 4.1. A tabela abaixo apresenta as principais diferenças entre as versões [7][16]:

	COBIT 4.1	COBIT 5
GOVERNANÇA E GESTÃO	Não diferencia claramente domínios de Governança e de Gestão de TI	Há uma diferenciação clara entre domínios de Governança e de Gestão de TI
INTEGRAÇÃO DOS MODELOS	Frameworks como COBIT 4.1, <i>Val IT</i> , <i>Risk IT</i> e <i>ITIL</i> são tratados separadamente	Integra diferentes frameworks e normas de Governança de TI em um único modelo
PRINCÍPIOS	Não se baseia nos princípios de Governança de TI (GEIT) conforme previsto nos frameworks <i>Val IT</i> e <i>Risk IT</i>	Novos princípios de governança corporativa de TI: 1. Atender as necessidades dos stakeholders (partes interessadas) 2. Cobrir a organização de ponta a ponta 3. Aplicar um framework (modelo) único e integrado 4. Permitir uma abordagem holística 5. Distinguir a governança da gestão
HABILITADORES	Esse conceito é difundido na estrutura do documento, não possuindo um tópico específico que o aborde de forma individual.	Grande enfoque nos habilitadores. São apresentados 7 categorias: 1.Princípios, políticas e frameworks 2.Processos 3.Estruturas organizacionais 4.Cultura, ética e comportamento 5. Informação 6.Serviços, infraestrutura e aplicações 7.Pessoas, habilidades e competências
MODELO DE PROCESSOS	Modelo de processos contendo 4 domínios de gestão que contemplam 34 processos	Modelo de processos apresenta 1 domínio de Governança (com 5 processos) e 4 domínios de gestão (com 32 processos) que contemplam 37 processos, cobrindo atividades corporativas de ponta a ponta, ou seja, das áreas de negócio e funções de TI.
OBJETIVOS E MÉTRICAS	Apresenta cascata de objetivos, desdobrando os objetivos de negócio em objetivos de TI, que por sua vez eram desdobrados em objetivos de processos e estes em objetivos de atividades. Apresenta alguns poucos exemplos de métricas para os objetivos de TI,	COBIT 5 segue o mesmo conceito de objetivos métricas como no COBIT 4.1, <i>Val IT</i> e <i>RiskIT</i> . Os objetivos de negócios são desdobrados em objetivos de TI, e estes em objetivos de habilitadores que refletem uma visão de nível corporativo. Apresenta maior número de exemplos

	objetivos de processo e objetivos de atividades.	de métricas para os objetivos de TI e objetivos de processos. Apesar de serem apresentadas métricas em um nível a menos do que na versão anterior (não possui objetivos de atividades), essas informações são apresentadas de maneira mais estruturada.
ENTRADAS E SAÍDAS	Apresenta entradas e saídas somente para os processos.	Apresenta entradas e saídas para cada prática de gerenciamento.
PRÁTICAS E ATIVIDADES	Há objetivos e práticas de controle.	As práticas de gestão e de governança do 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.
MATRIZ RACI	Apresenta número reduzido de papéis para os processos de TI.	Fornece uma matriz RACI escrevendo 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 gerenciamento, permitindo uma melhor definição das responsabilidades dos papéis ou nível de envolvimento na concepção e implementação de processos.
MODELO DE CAPACIDADE	Modelo de maturidade de processos baseado no CMM (Capacity Maturity Model). No modelo de maturidade, os atributos utilizados para avaliação estão presentes em todos os níveis e evoluem de acordo com a maturidade do processo.	COBIT 5 descontinua o modelo de maturidade. Modelo de capacidade de processos baseado na norma ISO/IEC 15504. No modelo de capacidade, os atributos são genéricos e exclusivos para cada nível, ou seja, cada nível de capacidade será determinado por um ou dois atributos específicos. O modelo de maturidade do COBIT 4.1 não é considerado compatível com o modelo da ISO/IEC 15504 porque os métodos usam diferentes atributos e escalas de medição.

Tabela 4 Diferenças entre COBIT 4.1 e COBIT 5.

Fonte: [7][16] adaptado

ANEXO I: Cascata de Objetivos do COBIT 5

A **Cascata de Objetivos do COBIT 5**, de acordo com a figura 17, tem a finalidade de desdobrar [4]:

- direcionadores (drivers) e as necessidades das partes interessadas em objetivos corporativos;
- objetivos corporativos em objetivos de TI;
- objetivos de TI em objetivos para os habilitadores.



Figura 17 - Cascata de Objetivos.
Fonte: COBIT ® 5, p. 20, ©2012 ISACA® [12]

Esse desdobramento é descrito nos quatro passos a seguir:

Passo 1: Direcionadores de Partes Interessadas (Stakeholders) Influenciam as Necessidades dos Stakeholders

As necessidades das partes interessadas 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 pode se tornar um direcionador de partes interessadas de uma operadora de telecomunicações, influenciando as necessidades destas: as dos usuários de internet (parte interessada externa), 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 Conselho de Administração da operadora de telecomunicações (parte interessada interna), 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 das Partes Interessadas (Stakeholders) desdobradas em Objetivos Corporativos

As necessidades das partes interessadas podem ser relacionadas a um conjunto de objetivos corporativos genéricos definidos pelo COBIT 5. O documento do *framework* define objetivos corporativos genéricos que podem ser desenvolvidos usando as dimensões do *Balanced Scorecard* (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 corporativos genéricos. O mapeamento das necessidades das partes interessadas, em formato de perguntas, em objetivos corporativos é apresentado no apêndice D do documento do *framework*.

A lista de 17 objetivos corporativos genéricos definidos pelo COBIT 5, como mostrado na figura 18, incluem as seguintes informações:

- A dimensão BSC ao qual o objetivo corporativo pertence;
- Objetivos corporativos;
- O relacionamento do objetivo corporativo 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).

Dimensão BSC	Objetivo corporativo	Relação com Objetivos de Governança		
		Realização de Benefícios	Otimização de Risco	Otimização de Recursos
Financeira	1. Valor dos investimentos da organização percebidos pelas partes interessadas	P		S
	2. Portfólio de produtos e serviços competitivos	P	P	S
	3. Gestão do risco do negócio (salvaguarda de ativos)		P	S
	4. Conformidade com as leis e regulamentos externos		P	
	5. Transparência financeira	P	S	S
Cliente	6. Cultura de serviço orientada ao cliente	P		S
	7. Continuidade e disponibilidade do serviço de negócio		P	
	8. Respostas rápidas para um ambiente de negócios em mudança	P		S
	9. Tomada de decisão estratégica com base na informação	P	P	P
	10. Otimização dos custos de prestação de serviços	P		P
Interna	11. Otimização da funcionalidade do processo de negócio	P		P
	12. Otimização dos custos do processo de negócio	P		P
	13. Gestão de programas de mudanças de negócios	P	P	S
	14. Produtividade operacional e da equipe	P		P
	15. Conformidade com as políticas internas		P	
Treinamento e Crescimento	16. Pessoas qualificadas e motivadas	S	P	P
	17. Cultura de inovação de produtos e negócios	P		

Figura 18 - Objetivos corporativos.
Fonte: COBIT® 5, p. 21, ©2012 ISACA® [12]

Passo 3: Objetivos corporativos desdobrados em Objetivos de TI

O alcance dos objetivos corporativos exige uma série de resultados relacionados a TI⁵, que são representados pelos objetivos relacionados a TI. COBIT 5 define 17 objetivos relacionados a TI, conforme apresentado na figura 19:

Dimensão BSC de TI	Objetivo da Informação e Tecnologia Relacionada	
Financeira	01	Alinhamento da estratégia de negócios e de TI
	02	Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos
	03	Compromisso da gerência executiva com a tomada de decisões de TI
	04	Gestão de risco organizacional de TI
	05	Benefícios obtidos pelo investimento de TI e portfólio de serviços
	06	Transparência dos custos, benefícios e riscos de TI
Cliente	07	Prestação de serviços de TI em consonância com os requisitos de negócio
	08	Uso adequado de aplicativos, informações e soluções tecnológicas
Interna	09	Agilidade de TI
	10	Segurança da informação, infraestrutura de processamento e aplicativos
	11	Otimização de ativos, recursos e capacidades de TI
	12	Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia
	13	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos
	14	Disponibilidade de informações úteis e confiáveis para a tomada de decisão
	15	Conformidade de TI com as políticas internas
Treinamento e Crescimento	16	Equipes de TI e de negócios motivadas e qualificadas
	17	Conhecimento, expertise e iniciativas para inovação dos negócios

Figura 19 - Objetivos de TI. Fonte: COBIT® 5, p. 21, ©2012 ISACA® [12]

A tabela de mapeamento dos objetivos corporativos em objetivos de TI está apresentada no Apêndice B do documento do framework, e demonstra como cada objetivo corporativo é apoiado por diversos objetivos de TI.

Passo 4: Objetivos de TI desdobrados em Objetivos de Habilitadores

Atingir os objetivos relacionados a TI requer a aplicação e uso bem-sucedidos de um conjunto de habilitadores. Habilitadores incluem:

- ✓ Princípios, políticas e *frameworks*
- ✓ Processos
- ✓ Estruturas organizacionais
- ✓ Cultura, ética e comportamento

⁵ Os resultados de TI não são obviamente o único benefício intermediário necessário para a consecução dos objetivos corporativos. Todas as demais áreas funcionais de uma organização, tais como finanças e marketing, também contribuem para a consecução dos objetivos corporativos, mas no contexto do COBIT 5 somente as atividades e os objetivos de TI são considerados

- ✓ Informação
- ✓ Serviços, infraestrutura e aplicações
- ✓ Pessoas, habilidades e competências

Para cada habilitador, um conjunto de objetivos específicos e relevantes pode ser definido para suportar os objetivos relacionados a TI. Para o habilitador Processos (figura 20), por exemplo, os objetivos e suas métricas são fornecidos nas descrições detalhadas de cada processo. O documento do COBIT 5, em seu Apêndice C, contém o mapeamento entre os objetivos de TI e os processos pertinentes, que por sua vez contém os respectivos objetivos do processo.

Usando a Cascata de Objetivos do COBIT 5 com Atenção



A cascata de objetivos - com suas tabelas de mapeamento entre os objetivos corporativos e os objetivos de TI e entre os objetivos de TI e os habilitadores do COBIT 5 (inclusive processos) - não contém a verdade universal, e os usuários não devem tentar usá-lo de uma forma puramente mecânica, mas sim como um orientador.

Há várias razões para isso, entre as quais:

- ✓ Cada organização tem prioridades diferentes em seus objetivos, e essas prioridades podem mudar com o tempo.
- ✓ As tabelas de mapeamento não fazem distinção entre o porte da organização e/ou o setor em que ela está inserida. Elas representam uma espécie de denominador comum de como, no geral, os diferentes níveis de objetivos se inter-relacionam.
- ✓ Os indicadores usados no mapeamento consideram dois níveis de importância ou relevância, sugerindo a existência de 'discretos' níveis de relevância, considerando que, de fato, o mapeamento será parecido com uma constante com vários níveis de correspondência.

ANEXO II: Exemplo de Habilitador: Processos

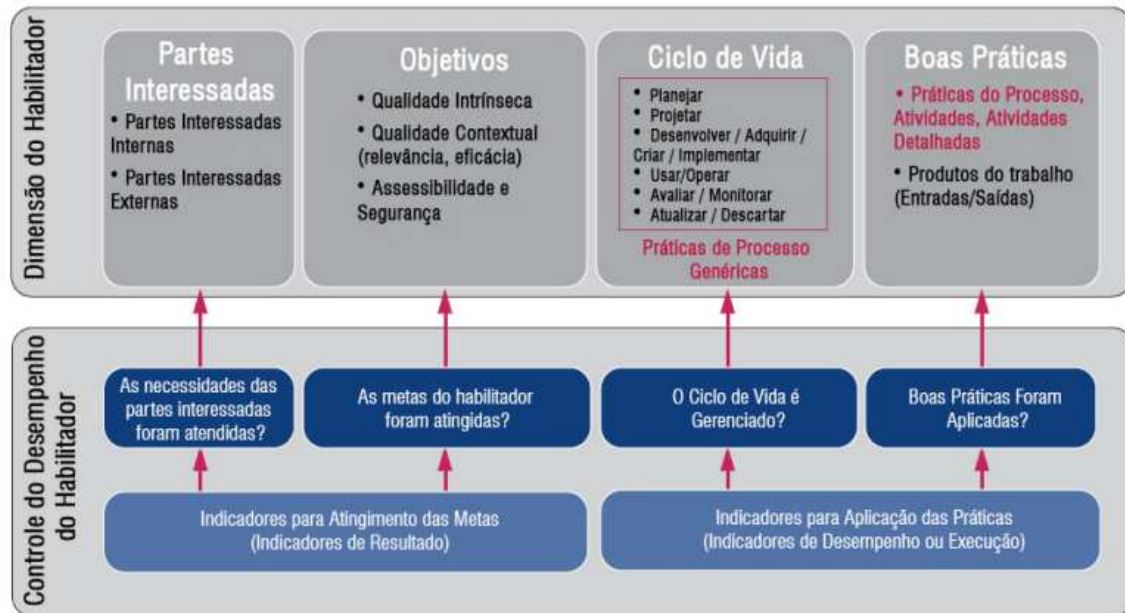


Figura 20 - Habilitador Processos.
Fonte: COBIT® 5, p. 73, ©2012 ISACA® [12]

Partes Interessadas: como pode ser visto na figura 20, partes interessadas do processo incluem todos os atores do processo, ou seja, todas as partes que são responsáveis, para 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

DOMÍNIO AVALIAR, DIRIGIR E MONITORAR (EDM)

Avaliar, Dirigir e Monitorar		
EDM01	Garantir a Definição e Manutenção do <i>Framework</i> 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	Garantir a Realização 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 na TI a custos aceitáveis.
EDM03	Garantir 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	Garantir 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	Garantir 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.

Tabela 5 Domínio Avaliar, Dirigir e Monitorar (EDM)

DOMÍNIO ALINHAR, PLANEJAR E ORGANIZAR (APO)

Alinhar, Planejar e Organizar		
APO01	Gerenciar a Estrutura 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 da Organização	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.

Alinhar, Planejar e Organizar (cont.)		
APO06	Gerenciar Orçamento e Custos	Gerenciar as atividades financeiras relacionadas a TI tanto nas funções de negócios como de TI, abrangendo orçamento, gerenciamento 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	Fornecer 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 Relacionamentos	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 Contratos de Prestação de Serviços	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 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 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 Riscos	Identificar continuamente, avaliar e reduzir os riscos relacionados a TI dentro dos níveis de tolerância estabelecidos pela diretoria executiva da organização.
APO13	Gerenciar Segurança	Define, opera e monitora um sistema para a gestão de segurança da informação.

Tabela 6 Domínio Alinhar, Planejar e Organizar (APO)

DOMÍNIO CONSTRUIR, ADQUIRIR E IMPLEMENTAR (BAI)

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 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 Identificação e Desenvolvimento 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 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 Capacidade 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.

Construir, Adquirir e Implementar (cont.)		
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 Aceitação 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 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 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 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.

Tabela 7 Domínio Construir, Adquirir e Implementar (BAI)

DOMÍNIO ENTREGAR, SERVIÇOS E SUPORTE (DSS)

Entregar, Serviços e Suporte		
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 Solicitação de Serviços e Incidentes	Fornecer uma resposta rápida e eficaz às solicitações dos usuários e resolução de todos os tipos de incidentes. Restaurar o serviço normal; registre e atenda às solicitações dos usuários e registre, investigue, diagnostique, escale e resolva 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 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 satisfazem todos os requisitos de controle de informações relevantes.

Tabela 8 Domínio Entregar, Serviços e Suporte (DSS)

DOMÍNIO MONITORAR, AVALIAR E ANALISAR (MEA)

Monitorar, Avaliar e Analisar		
MEA01	Monitorar, Avaliar e Analisar 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 Analisar 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 Analisar 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.

Tabela 9 Domínio Monitorar, Avaliar e Analisar (MEA)

ANEXO IV: Mapeamento de processos COBIT 5 X COBIT 4.1

Esse mapeamento é uma adaptação da tabela de mapeamento dos objetivos de controle do COBIT 4.1 para as práticas de gerenciamento do COBIT 5 [9]. Os processos destacados em verde são novos processos do COBIT5.

Avaliar, Dirigir e Monitorar (EDM)	
EDM01 Garantir a Definição e Manutenção do Framework de Governança	PO3 Determinar a Direção Tecnológica ME4 Fornecer Governança de TI
EDM02 Garantir a Realização de Benefícios	PO1 Definir um Plano Estratégico de TI ME4 Fornecer Governança de TI
EDM03 Garantir a Otimização de Riscos	PO6 Comunicar Metas e Diretivas Gerenciais PO9 Avaliar e Gerenciar Riscos ME4 Fornecer Governança de TI
EDM04 Garantir a Otimização de Recursos	ME4 Fornecer Governança de TI
EDM05 Garantir Transparência para as Partes Interessadas	-

Tabela 10 COBIT 5 x COBIT 4.1: Domínio EDM. Fonte: COBIT® 5: Enabling Process, p. 217, ©2012 ISACA® [9]

Alinhar, Planejar e Organizar (APO)	
APO01 Gerenciar a Estrutura de Gestão de TI	PO2 Definir a Arquitetura de Informação PO3 Determinar a Direção Tecnológica PO4 Definir Processos de TI, Organização e Relacionamento PO6 Comunicar Metas e Diretivas Gerenciais PO7 Gerenciar Recursos Humanos PO9 Avaliar e Gerenciar Riscos
APO02 Gerenciar a Estratégia	PO1 Definir um Plano Estratégico de TI PO3 Determinar a Direção Tecnológica
APO03 Gerenciar a Arquitetura da Organização	PO2 Definir a Arquitetura de Informação PO3 Determinar a Direção Tecnológica
APO04 Gerenciar a Inovação	PO3 Determinar a Direção Tecnológica
APO05 Gerenciar o Portfólio	PO1 Definir um Plano Estratégico de TI PO5 Gerenciar o Investimento em TI
APO06 Gerenciar Orçamento e Custos	DS6 Identificar e Alocar Custos PO5 Gerenciar o Investimento em TI
APO07 Gerenciar Recursos Humanos	DS7 Educar e Treinar usuários PO4 Definir Processos de TI, Organização e Relacionamento PO7 Gerenciar Recursos Humanos
APO08 Gerenciar Relacionamentos	-
APO09 Gerenciar Contratos de Prestação de Serviços	DS1 Definir níveis de Serviços
APO10 Gerenciar Fornecedores	AI5 Obter Recursos de TI DS2 Gerenciar Serviços de Terceiros
APO11 Gerenciar Qualidade	PO4 Definir Processos de TI, Organização e Relacionamento PO8 Gerenciar Qualidade
APO12 Gerenciar Riscos	PO9 Avaliar e Gerenciar Riscos
APO13 Gerenciar Segurança	DS5 Garantir Segurança dos Sistemas

Tabela 11 COBIT 5 x COBIT 4.1: Domínio APO. Fonte: COBIT® 5: Enabling Process, p. 217, ©2012 ISACA® [9]

Construir, Adquirir e Implementar (BAI)	
BAI01 Gerenciar Programas e Projetos	PO10 Gerenciar Projetos
BAI02 Gerenciar Definição de Requisitos	AI1 Identificar soluções automatizadas
BAI03 Gerenciar Identificação e Desenvolvimento de Soluções	Controles AC
	AI2 Adquirir e manter software aplicativo
	AI3 Adquirir e manter arquitetura tecnológica
	AI5 Obter Recursos de TI
BAI04 Gerenciar Disponibilidade e Capacidade	DS3 Gerenciar Performance e Capacidade
BAI05 Gerenciar Capacidade de Mudança Organizacional	AI4 Manter operação e uso
	AI7 Instalar e certificar Soluções e Mudanças
BAI06 Gerenciar Mudanças	AI6 Gerenciar mudanças
BAI07 Gerenciar Aceitação e Transição de Mudança	AI7 Instalar e certificar Soluções e Mudanças
BAI08 Gerenciar Conhecimento	AI4 Manter operação e uso
BAI09 Gerenciar Ativos	-
BAI10 Gerenciar Configuração	DS9 Gerenciar a Configuração

Tabela 12 COBIT 5 x COBIT 4.1: Domínio BAI. Fonte: COBIT® 5: Enabling Process, p. 217, ©2012 ISACA®[9]

Entregar, Serviços e Suporte (DSS)	
DSS01 Gerenciar as operações	DS11 Gerenciar Dados
	DS12 Gerenciar os Ambientes Físicos
	DS13 Gerenciar Operações
DSS02 Gerenciar Solicitação de Serviços e Incidentes	DS5 Garantir Segurança dos Sistemas
	DS8 Gerenciar Service Desk e Incidentes
	DS9 Gerenciar a Configuração
DSS03 Gerenciar Problemas	DS10 Gerenciar Problemas
DSS04 Gerenciar Continuidade	DS4 Garantir Continuidade dos Serviços
	DS11 Gerenciar Dados
DSS05 Gerenciar Serviços de Segurança	DS5 Garantir Segurança dos Sistemas
	DS11 Gerenciar Dados
	DS12 Gerenciar os Ambientes Físicos
	DS13 Gerenciar Operações
DSS06 Gerenciar os Controles de Processos de Negócio	Controles AC
	DS11 Gerenciar Dados

Tabela 13 COBIT 5 x COBIT 4.1: Domínio DSS. Fonte: COBIT® 5: Enabling Process, p. 217, ©2012 ISACA®[9]

Monitorar, Avaliar e Analisar (MEA)	
MEA01 Monitorar, Avaliar e Analisar o Desempenho e Conformidade	ME1 Monitorar e Avaliar a Performance de TI
MEA02 Monitorar, Avaliar e Analisar o Sistema de Controle Interno	ME2 Monitorar e Avaliar Controle Interno
	ME4 Fornecer Governança de TI
MEA03 Monitorar, Avaliar e Analisar a Conformidade com Requisitos Externos	ME3 Assegurar Conformidade Regulatória

Tabela 14 COBIT 5 x COBIT 4.1: Domínio MEA. Fonte: COBIT® 5: Enabling Process, p. 217, ©2012 ISACA®[9]

ANEXO V: 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Percent of unsuccessful changes due to inadequate impact assessments	
3. All emergency changes are reviewed and authorised after the change.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I
BAI06.03 Track and report change status.					C	R			C									A	R
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C

Tabela 15 Processo BAI06 Gerenciar Mudanças Fonte: COBIT® 5: Enabling Process, p. 149, ©2012 ISACA® [9]

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/package 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.				

Tabela 16 Processo BAI06 Gerenciar Mudanças (cont.) Fonte: COBIT® 5: Enabling Process, p. 150, ©2012 ISACA® [9]

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%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 nº 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>
- [12] **COBIT 5: Modelo Corporativo para Governança e Gestão de TI da Organização**, USA, 2012
- [13] **COBIT 5 Como avaliar a maturidade dos processos de acordo com o novo modelo?**, Bridge Consulting, 2013. Acesso em: http://www.blog.bridgeconsulting.com.br/wp-content/uploads/2013/09/CobIT_5_Avalia%C3%A7%C3%A3o_de_Maturidade.pdf
- [14] **COBIT Process Assessment Model (PAM): Using COBIT 4.1**. USA, 2011.
- [15] **IINF326 - Modelos de Qualidade de SW - Mario L. Côrtes**. Acesso em: <http://www.ic.unicamp.br/~cortes/inf326/transp/cap7.pdf>
- [16] **COBIT 5: Apresentação do novo framework da ISACA**, Bridge Consulting, 2013. Acesso em: <http://www.blog.bridgeconsulting.com.br/wp-content/uploads/2013/02/Apresenta%C3%A7%C3%A3o-do-CobIT-5.pdf>