UNIVERSIDADE FEDERAL DO RIO DE JANEIRO - UFRJ

FACULDADE DE ADMINISTRAÇÃO E CIÊNCIAS CONTÁBEIS

CURSO DE GRADUAÇÃO EM ADMINISTRAÇÃO

MONOGRAFIA

TRABALHO DE CONCLUSÃO DE CURSO

Título:

Governança de Tecnologia da Informação sob a abordagem COBIT

Autor: Leonardo Costa de Andrade

Orientador: Henrique Westenberger

Outubro / 2010

GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO SOB A ABORDAGEM COBIT

Leonardo Costa de Andrade

MONOGRAFIA SUBMETIDA À FACULDADE DE ADMINISTRAÇÃO E CIÊNCIAS CONTÁBEIS DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO REQUISITO NECESSÁRIO À OBTENÇÃO DO GRAU DE BACHAREL EM ADMINISTRAÇÃO.

Aprovação da banca examinadora:

_____

_____

_____

AGRADECIMENTOS

Aos familiares e amigos que sempre me incentivaram a persistir,
e aos professores e mestres que sempre me incentivaram a me aperfeiçoar.

SUMÁRIO

GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO SOB A ABORDAGEM COBIT

Leonardo Costa de Andrade

Outubro / 2010

RESUMO

Nesta monografia é feita uma apresentação dos princípios do tema de Governança de TI e os fundamentos e processos de uma metodologia de mercado consagrada (COBIT) para sua implantação. São revistas fontes bibliográficas relacionadas que constituem as principais referências acerca do modelo usado como foco no trabalho, assim como obras de autores nacionais acerca do assunto de Governança de TI.

1. INTRODUÇÃO

Atualmente o investimento corporativo em iniciativas de tecnologia da informação é evidenciado em escala crescente em organizações de diferentes segmentos de mercado, o que transparece a relevância do assunto para o planejamento de cada empresa. De forma a garantir a entrega de valor correspondente a esses significativos investimentos, as áreas de TI das organizações devem ser administradas conforme as melhores práticas de gestão, conforme princípios de responsabilidade, prestação de contas, controle orçamentário e medição de resultados.

A Governança de Tecnologia de Informação é a disciplina que propõe a aplicação destas práticas de gestão às diferentes atividades desempenhadas pela área de TI, de forma garantir sucesso (através da comprovação de eficácia e eficiência dos esforços). Há bibliografia extensa no mercado sobre metodologias para gestão e melhores práticas de segmentos específicos de TI (desde desenvolvimento de sistemas e programação, até gerenciamento de serviços), mas para Governança de TI em um âmbito geral o modelo consagrado é o COBIT.

O COBIT é um *framework* se tornou referência para Governança de TI pois é abrangente em sua cobertura e atualmente é utilizado como base para processos de auditoria externa de conformidade em organizações que devem atender requisitos legais ou regulatórios (compulsórios ou não). Os processos propostos pelo modelo são aplicáveis em diferentes contextos e organizações, em graus variáveis de implantação definidos por níveis de maturidade.

1.1. Objetivos Principais

Este trabalho se propõe a apresentar uma visão geral do tema de Governança de TI e um detalhamento do modelo COBIT voltado à visão gerencial que a alta direção de uma organização deve ter sob os processos e atividades técnicas desempenhadas pelas diferentes equipes que podem compor uma área de TI.

1.2. Relevância do Projeto

A principal aplicação para o tema proposto é apresentar através de um modelo genérico e fundamentado em uma linguagem não-técnica uma metodologia para gestão das atividades de tecnologia de informação em uma organização, de forma transparente para profissionais de administração, desmistificando conceitos sobre a complexidade do assunto e integrando conceitos de melhores práticas de gestão para a disciplina de TI.

1.3. Estrutura da Monografia

No Capítulo 2 é apresentada a bibliografia oficial da metodologia, que fundamenta os princípios de Governança de TI, assim como obras de autores nacionais que tratam de temas correlatos, como gestão de serviços em TI e outras metodologias aplicáveis ao tema.

No Capítulo 3 é revista a fundamentação teórica do tema, de forma a embasar os conceitos e princípios para a implantação de Governança de TI, e exposta a estruturação do modelo COBIT.

No Capítulo 4 são discutidos os processos contidos no framework da metodologia, exemplificando como são evidenciados os mesmos em situações reais de utilização, quanto à relevância no cotidiano, facilidade de implementação, automatização de tarefas e utilidade de sua aplicação em contextos concretos.

No Capítulo 5 são elaborados comentários finais sobre o tema e sugeridos tópicos relacionados a serem explorados futuramente.

2. REVISÃO BIBLIOGRÁFICA

Neste capítulo é apresentada uma revisão dos principais textos utilizados na elaboração do referencial teórico, apresentados em ordem cronológica.

Em *COBIT 4.1* (*IT Governance Institute*, 2007), publicação central do corpo bibliográfico da metodologia, são apresentados os conceitos básicos da disciplina de Governança de Tecnologia da Informação, inclusive quanto à sua relevância no contexto organizacional contemporâneo, principalmente quanto às responsabilidades da TI para o negócio. Estes conceitos fundamentam os princípios e ferramentas que compõem o modelo em si, apresentados na sequência, e o conjunto de processos que visam cobrir de forma completa e abrangente todo o escopo do trabalho de TI em uma empresa.

Em *Board Briefing on IT Governance* (*IT Governance Institute*, 2003) são expostos com maior profundidade os conceitos que demonstram para o corpo executivo de uma organização a importância com a qual a Governança de TI deve ser considerada para consecução de estratégias corporativas. É a publicação dedicada à apresentação do tema para os principais decisores da organização e sua conscientização da relevância do tema.

Em *COBIT Control Practices* (*IT Governance Institute*, 2007) são detalhadas as práticas de controle que integram cada processo proposto pelo modelo na publicação central do framework COBIT, descrevendo como estas práticas mitigam riscos e propõem a geração de valor, revalidando melhores práticas de mercado que são muitas vezes incorporadas de outras metodologias de gestão de TI (voltadas para disciplinas específicas).

Em FERNANDES (2008) é discutida em maior extensão a temática da Governança de TI, com detalhamento do escopo de trabalho de toda a TI, e como o COBIT e outras metodologias de mercado se propõem a elevar o nível de gerenciamento das responsabilidades associadas à tecnologia da informação (inclusive os riscos de conformidade).

3. FUNDAMENTAÇÃO TEÓRICA

3.1. Definição de Governança de Tecnologia da Informação

A Governança de Tecnologia da Informação é uma disciplina que pode ser definida como o conjunto de liderança, processos e estruturas organizacionais vinculados à área de TI, de forma a alinhar seus esforços com os objetivos estratégicos definidos pela organização. A execução de políticas de Governança de TI traz benefícios às organizações quanto à confiança da alta administração na tomada de decisões, quanto à agilidade e flexibilidade da organização em se adaptar a mudanças de mercado, e quanto a uma maior eficiência na gestão dos recursos destinados à TI.

O tema abrange aspectos estratégicos, táticos e operacionais de gestão de ativos corporativos (como por exemplo recursos de infra-estrutura e informação) sob óticas de controle entre os diferentes níveis de gestão e operação das organizações. A importância destes ativos para a realização dos objetivos de negócio das empresas torna necessária a adoção de metodologias dedicadas de gestão, monitoramento e controle destes recursos, sob o enfoque de retorno de valor e controle de riscos. Muitas organizações dependem destes recursos para garantir a conformidade (voluntária ou mandatória) de sua operação em seus respectivos mercados, quando não dependem da própria tecnologia para a execução direta de sua atividade fim.

A base teórica para a Governança de TI corresponde à compreensão e à gestão do trio Valor, Risco e Controle para a tecnologia e seus benefícios e dependências. Neste contexto, é responsabilidade dos níveis hierárquicos mais altos da organização manter um planejamento para a Governança de TI que esteja alinhado estrategicamente com a própria Governança Corporativa. É este posicionamento que garantirá a otimização dos recursos disponíveis, o melhor aproveitamento de oportunidades e o surgimento de vantagem competitiva para a organização no mercado. É necessário que a alta direção da organização tenha ferramentas e métodos implantados para gerenciar riscos (prevenindo antecipadamente sua ocorrência ou elaborando planos de resposta eficazes) e disponha de informações precisas e em momento oportuno para a tomada de decisões. A alta direção deve ser capaz de responder com segurança questionamentos sobre a TI, e a prática da Governança de TI ajudará a alcançar esse conhecimento:

- Os colaboradores da empresa estão satisfeitos com a qualidade dos serviços de TI?
- Existem recursos de TI suficientes para atender expectativas e alcançar objetivos estratégicos da empresa?
- Como estão sendo gerenciados os contratos de terceirização de TI?
- Como são realizadas as principais decisões de TI?
- Há transparência quanto ao total de esforços e investimentos em TI, quanto a risco e retorno?
- Como a TI evoluiu ao longo do tempo na empresa?
- O quanto a TI é crítica no suporte às áreas de negócio?
- Quais ações a alta direção implementa para gerenciar riscos de TI?
- A alta direção comunica à TI a direção estratégica a ser seguida na organização?
- Como é feito o acompanhamento de resultados entre projetos e operações de TI na organização?

A estruturação de um modelo de Governança para TI contribui para tornar visíveis para os mais altos níveis hierárquicos das organizações os retornos sobre os investimentos em tecnologia da informação, através da definição de planos estratégicos, indicadores de desempenho e objetivos pré-estabelecidos para o desempenho destas atividades. O valor agregado aos resultados do negócio, demonstrado através destes modelos, contribui para o entendimento da relevância das atividades de TI no contexto organizacional. Há necessidade de transparência de resultados para os *stakeholders* da organização quanto a requisitos de segurança, melhor utilização de recursos e posicionamento no mercado em relação a competidores.

A Governança de TI deve englobar também os desafios da área de tecnologia da informação dentro do contexto organizacional. Serviços críticos de informática devem permanecer disponíveis conforme acordos de nível de serviço estabelecidos entre TI e áreas de negócio, sob risco de prejuízos operacionais e à imagem da organização. Há necessidade de acompanhamento contínuo dos benefícios obtidos pelos serviços oferecidos, face ao crescente nível de investimento necessário em infra-estrutura e equipes técnicas qualificadas, e ao custo de oportunidade destes investimentos (principalmente devido à crescente tendência ao *outsourcing* de soluções neste mercado). Freqüentemente, estes benefícios não são

transparentes aos investidores, dadas as características técnicas do ambiente de TI e da intangibilidade do retorno obtido na operação das empresas. O setor também demanda entradas constantes de capital para acompanhar requisitos de negócio e tecnologias emergentes, de forma a manter a organização competitiva no mercado. Conformidade com normas e legislações vigentes exige esforço adicional na implantação de diferentes serviços, o que requer maior coordenação e maior controle em aspectos como segurança e uma maior participação das áreas internas de negócio das empresas como aquelas que definem quais requisitos a TI deve atender com qualidade.

3.2. Modelo COBIT

Dentre os modelos disponíveis do mercado, o COBIT (*Control Objectives for Information and Related Technology*) é o conjunto de melhores práticas de maior relevância para a Governança de TI, tendo fundamentação baseada em um modelo de Governança Corporativa (o modelo de Controle Internos do COSO, *Committee of Sponsoring Organisations of the Treadway Commission*), e com compatibilidade com outros modelos, entre eles o PMBOK de gestão de projetos do *Project Management Institute* (PMI) e o de gestão do ciclo de vida de serviços de TI elaborado pelo *Office of Government Commerce* britânico (OGC) conhecido como ITIL (*Information Technology Infrastructure Library*). Por manter o enfoque no nível de "o quê" precisa ser realizado (e controlado), o COBIT se comporta como um modelo "guarda-chuva" que permite incorporar outras metodologias de execução propriamente ditas de atividades subordinadas (que se tornam responsáveis pela definição do "como" fazer nos segmentos subordinados da área de TI, como o desenvolvimento de aplicações ou a coordenação de uma central de atendimento técnico).

Desenvolvido em sua versão original em 1996 pelo ISACA (*Information Systems Audit and Control Association*) e mantido pelo ITGI (*IT Governance Institute*), o COBIT visa disponibilizar um conjunto de ferramentas de gestão de TI não apenas para profissionais da área, mas também para executivos de áreas de negócios e profissionais de auditoria. O modelo baseia-se em princípios de atuação como Planejamento, Direção, Controle, Responsabilidade e Prestação de Contas, e sua estrutura de organização é independente de plataformas ou tecnologias. Atualmente em sua versão 4.1 (lançada originalmente em 2007, e traduzida para

o português em 2010), o modelo é referência de mercado para Governança de TI mundialmente.

Como um modelo complementar ao de Governança Corporativa proposto pelo COSO, o COBIT se propõe a gerenciar não apenas informações financeiras, mas todas as informações de negócio de uma organização sob um conjunto de ferramentas de gerenciamento coordenado e desenvolvido através de melhores práticas do mercado de TI. Por outro lado, o COBIT concentra seu foco nos processos de TI, ao passo que a abordagem do COSO tem como escopo o controle de todos os processos internos da organização. Esta correlação entre os modelos torna o COBIT uma abordagem popular no mercado para estruturação e controle de processos em TI em cenários de auditoria de conformidade com padrões regulatórios como a norte-americana Lei Sarbannes-Oxley (SOX).

Este modelo de governança estabelecido pelo COBIT faz a correlação com requisitos de negócio definidos no nível estratégico da organização. Ele também organiza as atividades de TI com uma estrutura de processos padrão, nos quais os recursos de TI são aplicados visando eficácia e eficiência, e definindo os objetivos de controle de cada processo desempenhado. Estes processos são baseados nas melhores práticas de mercado para a gestão de TI, e organizados em quatro domínios de atuação. Cada processo possui métricas sugeridas para avaliação de desempenho e modelos de avaliação de maturidade para melhoria contínua. Também são estabelecidos papéis e responsabilidades para as atividades contidas em cada processo. Um dos benefícios oferecidos é o estabelecimento de uma linguagem comum para interface entre os níveis estratégico, tático e operacional, e o entendimento da contribuição e relevância de atividades de base para alcance de objetivos gerais dentro da organização, assim como uma maior transparência quanto às atividades desempenhadas pelas áreas de TI, principalmente para a alta direção, que garante o investimento necessário à consecução dos projetos e das atividades de operação diárias.

O COBIT propõe para a Governança de TI a implementação de controles, compostos de políticas e estruturas organizacionais, procedimentos e melhores práticas de mercado que visam garantir a realização dos objetivos de negócio. Cada um dos processos relacionados no COBIT possui objetivos de controle vinculados, que consistem em requisitos de alto nível a serem considerados e priorizados para realização dos processos.

A nível executivo, a alta direção deve considerar os objetivos propostos pelo modelo, e tomar decisões quanto a quais são aplicáveis e deverão ser implantados na organização, o modo de implementação (escopo de utilização, investimentos requeridos, grau de automação exigido), e quanto à aceitação do risco de priorização de uns em detrimento de outros (tendo em mente a percepção de criticidade para o negócio de cada processo). Há rastreabilidade intrínseca ao modelo quanto aos objetivos de controle, quanto aos processos nos quais eles estão incluídos, e quanto aos requisitos de governança que orientam a arquitetura destas práticas (políticas de desempenho e resultados).

3.3. Áreas de Foco

Na visão geral da Governança de TI, o COBIT utiliza cinco grandes áreas de foco, com as quais cada processo possui maior ou menor relevância, a saber:

• **Alinhamento Estratégico**: baseado nos princípios dos planos e operações de negócio e da contribuição dos serviços de TI para o alcance destes objetivos maiores da própria organização.
• **Entrega de Valor**: baseada nos benefícios obtidos pelos serviços de TI (resultados e valor agregado) para os objetivos de negócio da organização, tendo por base o investimento dedicado.
• **Gerenciamento de Recursos**: baseado na maior disponibilidade e na melhor utilização dos recursos definidos no modelo (*Aplicações*, *Informações*, *Infra-Estrutura* e *Pessoas*) para realização de atividades.
• **Gerenciamento de Riscos**: baseado no entendimento por todos os envolvidos dos riscos inerentes ao negócio e à TI, às necessidades de conformidade e à distribuição da gestão do risco entre os devidos responsáveis.
• **Avaliação de Desempenho**: baseado na medição e análise de resultados e avanços em projetos, utilização de recursos, desempenho de serviços, entre outros.

3.4. Critérios de Informação

O gerenciamento de informações dentro da organização é um dos princípios do modelo COBIT. Para se adequarem aos objetivos de negócio, as informações devem atender a requisitos de negócio relativos à segurança e à qualidade, por exemplo. O correto tratamento para a informação deve seguir a premissa de que *dados* devem ser convertidos em *informação*, a qual deve ser útil para agregar *conhecimento* para a organização. É uma escala crescente de aproveitamento de um recurso crucial para o sucesso da organização. A versão 4.1 do COBIT propõe sete critérios (atributos) para gerenciamento da informação corporativa:

• **Eficácia**: informações devem ser oportunas, consistentes, claras, úteis, relevantes e pertinentes ao processo de negócio.
• **Eficiência**: informações devem ser obtidas da maneira mais produtiva e econômica possível (ou seja, com o melhor uso de recursos disponíveis).
• **Confidencialidade**: informações devem ser restritas ao pessoal autorizado.
• **Integridade**: informações devem ser completas e válidas dentro do contexto organizacional.
• **Disponibilidade**: informações devem estar disponíveis para os processos de negócio sempre que necessárias.
• **Conformidade**: informações devem estar de acordo com requisitos internos e externos, de origem regulatória, normativa, contratual, etc.
• **Confiabilidade**: informações devem ser precisas e apropriadas para a execução das responsabilidades da direção da organização (isto é, devem ser confiáveis para fundamentar o processo decisório).

3.5. Objetivos de Negócio para Tecnologia da Informação

Derivados do planejamento estratégico da organização, e organizados em uma estrutura baseada no *Balanced Scorecard* (BSC), Objetivos de Negócio podem ser traçados para cumprimento pela área de TI (*Business Goals for IT*) como verdadeiros requisitos para desempenho, os quais serão vinculados aos Objetivos de TI (*IT Goals*) que contribuirão para o alcance dos resultados almejados. Por exemplo, sob a ótica do Cliente, um objetivo de negócio para TI corresponde a "*Estabelecer continuidade e disponibilidade de serviços*". Há quatro objetivos de TI que contribuem para este objetivo de negócio: 1) "*Assegurar a satisfação mútua no relacionamento com terceiros*"; 2) "*Reduzir os defeitos e re-trabalhos na entrega de serviços e soluções*"; 3) "*Assegurar o mínimo impacto para os negócios no caso de*

uma parada ou mudança nos serviços de TI"; e 4) "*Garantir que os serviços de TI ficam disponíveis de acordo com o requerido*".

Da mesma forma, para cada um dos 28 Objetivos de TI propostos no modelo, podem ser identificados dentre os 34 Processos aqueles mais relevantes para o alcance destes objetivos.

As matrizes abaixo, extraídas do COBIT 4.1, representam esta correlação entre Objetivos de Negócio, Objetivos de TI, e Processos de TI, a serem discutidos adiante.

Tabela 4.1: Correlação entre Objetivos de Negócio e Objetivos de TI:

	Objetivos de Negócio		Objetivos de TI							
Perspectiva Financeira	1	Prover um retorno de investimento adequado para os investimentos de TI relacionados aos negócios.	**24**							
	2	Gerenciar os riscos de negócios relacionados a TI.	**2**	**14**	**17**	**18**	**19**	**20**	**21**	**22**
	3	Aprimorar governança corporativa e transparência.	**2**	**18**						
Perspectiva do Cliente	4	Aprimorar orientação para clientes e serviços.	**3**	**23**						
	5	Oferecer produtos e serviços competitivos.	**5**	**24**						
	6	Estabelecer a continuidade e disponibilidade de serviços.	**10**	**16**	**22**	**23**				
	7	Criar agilidade em responder a requerimentos de negócios que mudam continuamente.	**1**	**5**	**25**					
	8	Atingir otimização dos custos para entrega de serviços.	**7**	**8**	**10**	**24**				
	9	Obter informações confiáveis e úteis para o processo de decisões estratégicas.	**2**	**4**	**12**	**20**	**26**			
Perspectiva Interna	10	Aprimorar e manter a funcionalidade dos processos de negócios.	**6**	**7**	**11**					
	11	Reduzir custos de processos.	**7**	**8**	**13**	**15**	**24**			
	12	Conformidade com leis externas, regulamentos e contratos.	**2**	**19**	**20**	**21**	**22**	**26**	**27**	
	13	Conformidade com políticas internas.	**2**	**13**						
	14	Gerenciar mudanças de negócios.	**1**	**5**	**6**	**11**	**28**			
	15	Aprimorar e manter a operação e produtividade do pessoal.	**7**	**8**	**11**	**13**				
Perspectiva de Aprendizagem	16	Gerenciar a inovação de produtos e negócios.	**5**	**25**	**28**					
	17	Contratar e manter pessoas habilitadas e motivadas.	**9**							

Tabela 4.2: Correlação entre Objetivos de TI e Processos de TI:

Objetivos de TI		Processos Relacionados									
1	Responder aos requisitos de negócios de maneira alinhada com a estratégia de negócios.	**PO1**	**PO2**	**PO4**	**PO10**	**AI1**	**AI6**	**AI7**	**DS1**	**DS3**	**ME1**
2	Responder aos requisitos de governança em linha com a Alta Direção.	**PO2**	**PO4**	**PO10**	**ME1**	**ME4**					
3	Assegurar a satisfação dos usuários finais com a oferta e níveis de serviços.	**PO3**	**AI4**	**DS1**	**DS2**	**DS7**	**DS8**	**DS10**	**DS13**		
4	Otimizar o uso da informação.	**PO4**	**DS11**								
5	Criar agilidade para TI.	**PO5**	**PO4**	**PO7**	**AI3**						
6	Definir como funções de negócios e requisitos de controles são convertidos em soluções automatizadas efetivas e eficientes.	**PO6**	**AI2**	**AI6**							
7	Adquirir e manter sistemas aplicativos integrados e padronizados.	**PO7**	**AI2**	**AI5**							
8	Adquirir e manter uma infraestrutura de TI integrada e padronizada.	**PO8**	**AI5**								
9	Adquirir e manter habilidades de TI que atendam as estratégias de TI.	**PO9**	**AI5**								
10	Assegurar a satisfação mútua no relacionamento com terceiros.	**PO10**									
11	Assegurar a integração dos aplicativos com os processos de negócios.	**PO11**	**AI4**	**AI7**							
12	Assegurar a transparência e o entendimento dos custos, benefícios, estratégia, políticas e níveis de serviços de TI.	**PO12**	**PO6**	**DS1**	**DS2**	**DS6**	**ME1**	**ME4**			
13	Assegurar apropriado uso e a performance das soluções de aplicativos e de tecnologia.	**PO13**	**AI4**	**AI7**	**DS7**	**DS8**					
14	Responsabilizar e proteger todos os ativos de TI.	**PO14**	**DS5**	**DS9**	**DS12**	**ME2**					
15	Otimizar a infraestrutura, recursos e capacidades de TI.	**PO15**	**AI3**	**DS3**	**DS7**	**DS9**					
16	Reduzir os defeitos e re-trabalhos na entrega de serviços e soluções.	**PO16**	**AI4**	**AI6**	**AI7**	**DS10**					
17	Proteger os resultados alcançados pelos objetivos de TI.	**PO17**	**DS10**	**ME2**							
18	Estabelecer claramente os impactos para os negócios resultantes de riscos de objetivos e recursos de TI.	**PO18**									
19	Assegurar que informações confidenciais e críticas são protegidas daqueles que não deveriam ter acesso às mesmas.	**PO19**	**DS5**	**DS11**	**DS12**						
20	Assegurar que transações automatizadas de negócios e trocas de informações podem ser confiáveis.	**PO20**	**AI7**	**DS5**							
21	Assegurar que os serviços e infraestrutura de TI podem resistir e recuperar-se de falhas devido a erros, ataques deliberados ou desastres.	**PO21**	**AI7**	**DS4**	**DS12**	**DS13**	**ME2**				
22	Assegurar o mínimo impacto para os negócios no caso de uma parada ou mudança nos serviços de TI.	**PO22**	**AI6**	**DS4**	**DS12**						
23	Garantir que os serviços de TI ficam disponíveis de acordo com o requerido.	**PO23**	**DS4**	**DS8**	**DS13**						
24	Aprimorar a eficiência dos custos de TI e sua contribuição para a lucratividade dos negócios.	**PO24**	**DS6**								
25	Entregar projetos no tempo certo dentro do orçamento e com os padrões de qualidade esperados.	**PO25**	**PO10**								
26	Manter a integridade da informação e da infraestrutura de processamento.	**PO26**	**DS5**								
27	Assegurar a conformidade de TI com leis, regulamentos e contratos.	**PO27**	**ME2**	**ME3**	**ME4**						
28	Assegurar que TI oferece serviços de qualidade com custo eficiente, contínuo aprimoramento e preparação para mudanças futuras.	**PO28**	**DS6**	**ME1**	**ME4**						

3.6. Recursos de Tecnologia da Informação

De forma a atingir os objetivos de negócio, os processos de TI lançam mão de recursos (competências pessoais, infra-estrutura tecnológica, etc.) a serem disponibilizados pela organização. É requerido um nível de capacidade técnica adequada para suportar cada processo de negócio, representado por uma combinação específica dos recursos propostos. Os quatro recursos de TI modelados pelo COBIT são:

• **Informações** em todas as suas formas, como entradas ou saídas de processos e sistemas;
• **Aplicações** são os sistemas automatizados ou procedimentos manuais que processam informações;
• **Infra-estrutura** compreende toda a tecnologia (equipamentos, bancos de dados, redes de telecomunicação, instalações físicas) que permite o processamento das aplicações;
• **Pessoas** necessárias (e qualificadas) para o desempenho dos processos de TI (serviços e sistemas de informações).

3.7. Domínios e Processos de TI

Os processos definidos pelo COBIT são estabelecidos dentro de um modelo genérico, contendo os mesmos atributos, definidos pelos chamados Controles de Processos. Entre estas características estão entradas e saídas típicas de cada processo, uma matriz de responsabilidade contemplando as principais atividades sugeridas do processo e os papéis principais na execução de cada uma (seguindo o modelo RACI, *Responsible/Responsável*, *Accountable/Presta Contas*, *Consulted/Consultado*, *Informed/Informado*), e métricas sugeridas para avaliação de desempenho do processo. Tais processos são organizados em quatro domínios distintos, de forma similar ao modelo PDCA (Plan-Do-Check-Act), relacionados abaixo:

• **Planejar e Organizar (*Plan and Organise, PO*)**: compreende dez processos de planejamento das atividades de TI, direcionando os esforços dos demais domínios. Consiste no alinhamento estratégico dos processos de TI com os objetivos de negócio, avaliando se as soluções providas estão de acordo com os requisitos apresentados. A organização e o

planejamento destas soluções serão elaborados também com foco na divulgação de objetivos e no gerenciamento de riscos.

PO1 Definir um Plano Estratégico de TI

PO2 Definir a Arquitetura da Informação

PO3 Determinar as Diretrizes de Tecnologia

PO4 Definir os Processos, a Organização e os Relacionamentos de TI

PO5 Gerenciar o Investimento de TI

PO6 Comunicar Metas e Diretrizes Gerenciais

PO7 Gerenciar os Recursos Humanos de TI

PO8 Gerenciar a Qualidade

PO9 Avaliar e Gerenciar os Riscos de TI

PO10 Gerenciar Projetos

• **Adquirir e Implementar (*Acquire and Implement, AI*)**: compreende sete processos de desenho e implantação de soluções, a serem suportados como serviços pela área de TI. Estas soluções devem acompanhar a evolução dos requisitos de negócio, devem ser implementadas com mínimo de impacto negativo sobre a operação (áreas de negócio) e com respeito a prazos e custos planejados e acordados.

AI1 Identificar Soluções Automatizadas

AI2 Adquirir e Manter Software Aplicativo

AI3 Adquirir e Manter Infraestrutura de Tecnologia

AI4 Habilitar Operação e Uso

AI5 Adquirir Recursos de TI

AI6 Gerenciar Mudanças

AI7 Instalar e Homologar Soluções e Mudanças

• **Entrega e Suporte (*Deliver and Support, DS*)**: compreende treze processos de operação e suporte aos usuários dos serviços disponibilizados de TI. Estes processos compreendem o acompanhamento de requisitos de segurança, o planejamento e o teste de soluções de continuidade, o gerenciamento de instalações e informações, e a utilização de sistemas de TI de forma apropriada.

DS1 Definir e Gerenciar Níveis de Serviços

DS2 Gerenciar Serviços Terceirizados

DS3 Gerenciar o Desempenho e a Capacidade

DS4 Assegurar a Continuidade dos Serviços

DS5 Garantir a Segurança dos Sistemas

DS6 Identificar e Alocar Custos

DS7 Educar e Treinar os Usuários

DS8 Gerenciar a Central de Serviço e os Incidentes

DS9 Gerenciar a Configuração

DS10 Gerenciar Problemas

DS11 Gerenciar os Dados

DS12 Gerenciar o Ambiente Físico

DS13 Gerenciar as Operações

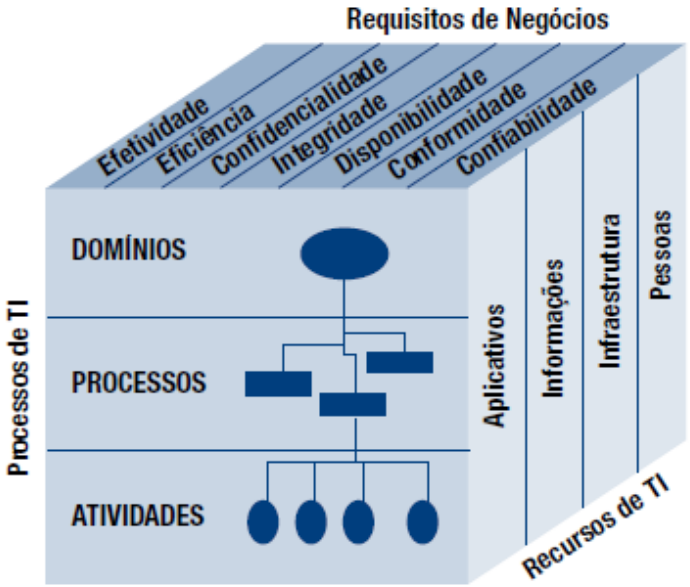
• **Monitorar e Avaliar (*Monitor and Evaluate, ME*)**: compreende quatro processos de avaliação de todos os processos anteriores para garantir que a direção planejada está sendo seguida, de maneira eficaz e eficiente. Desempenho, qualidade e conformidade dos processos são o foco, assim como a detecção e tratamento preventivo de ocorrências indesejadas no ambiente de TI.

ME1 Monitorar e Avaliar o Desempenho de TI

ME2 Monitorar e Avaliar os Controles Internos

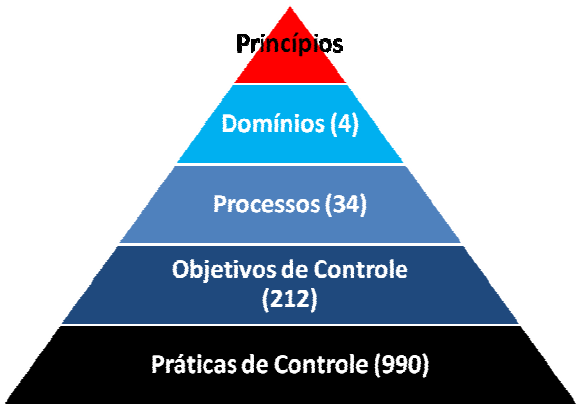
ME3 Assegurar a Conformidade com Requisitos Externos

ME4 Prover Governança de TI



Os trinta e quatro processos distribuídos entre esses domínios são previstos no modelo COBIT para garantir uma visão completa da Governança de TI, embora na prática as organizações implementarão gradualmente cada processo, ou apenas alguns destes controles, de acordo com sua percepção de prioridades e a aplicabilidade de cada processo ao contexto interno de cada

organização. Para contribuir com o entendimento e a implantação de cada processo e seus respectivos objetivos de controle, a biblioteca de referência do COBIT possui uma publicação específica contendo as Práticas de Controle (*COBIT Control Practices*), que consistem em sugestões de melhores práticas de mercado para alcançar cada Objetivo de Controle, assim como os princípios de condução de valor e administração de risco vinculados a cada um destes objetivos.



3.8. Avaliação de Desempenho

Três níveis de objetivos e métricas são definidos no modelo COBIT:

- **Objetivos gerais para a TI**, originados das expectativas de negócio da alta direção em relação às contribuições que a área de tecnologia da informação pode prover.
- **Objetivos dos processos de TI**, contemplando os resultados de cada processo e como estes contribuem para o alcance de objetivos maiores.
- **Objetivos das atividades** contidas em cada processo de TI, indicadores do desempenho dos processos.

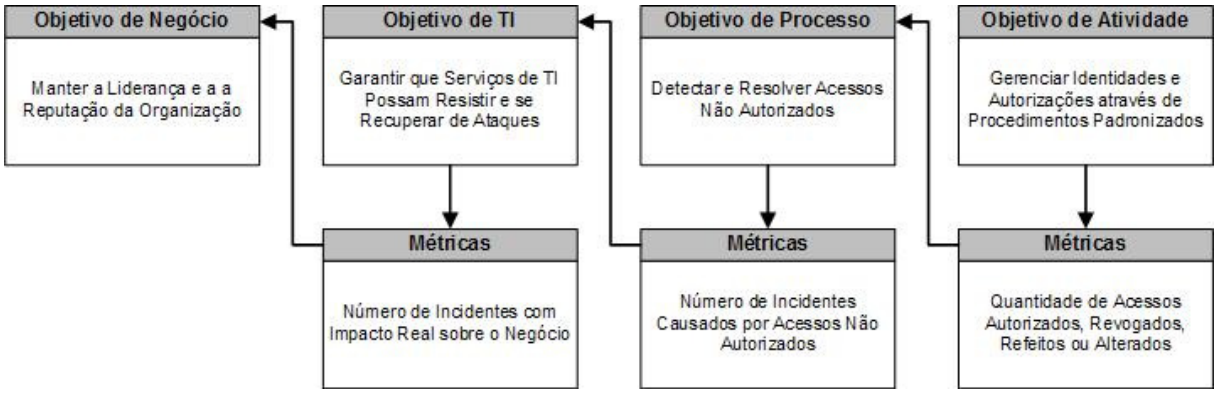
Estes objetivos são definidos do nível mais alto da organização em direção ao nível operacional. Os objetivos são avaliados através de métricas específicas; estas, por sua vez, são feitas da operação em direção aos objetivos de negócio, de forma que a cada nível há consolidação de múltiplos indicadores para verificar a conformidade com metas superiores.

As métricas são classificadas no COBIT em duas categorias:

• **Medidas de Resultados** (*Key Goal Indicators, KGIs*), que correspondem às verificações ao término da execução de cada processo, apurando se os objetivos foram alcançados. É portanto um indicador de eficácia. Como é apurada após os fatos concluídos, é também denominada de indicador histórico.

• **Indicadores de Performance** (*Key Performance Indicators, KPIs*), são avaliações do desempenho corrente do processo, antes de sua conclusão, e portanto são indicadores de eficiência. Como avalia a evolução gradual de um processo e a probabilidade de sucesso ao término, é denominado também de indicador futuro.

Como exemplo deste fluxo, segue abaixo o fluxo de uma das métricas do processo **DS5** (**Garantir a Segurança de Sistemas**, *Ensure Systems Security*), desde o nível de atividade (mais operacional), até o objetivo de negócio da organização (nível mais estratégico) para o qual seus objetivos de atividade, processo e TI contribuem.



3.9. Modelos de Maturidade

Outro enfoque do *framework* COBIT é a definição por parte da organização do caminho a percorrer para atingir sua Visão de negócio, tendo como ponto de partida uma avaliação da situação presente (ponto "*as is*", segundo a modelagem de processos de negócio). A alta direção da organização deverá planejar como os esforços da área de Tecnologia da Informação irão contribuir para o ponto "*to be*", estabelecendo metas a serem cumpridas, sempre alinhadas com o planejamento estratégico. A avaliação da distância entre o cenário atual e o desejado representa o "*gap*" a ser percorrido pelos projetos de melhoria. Esse planejamento é comumente realizado quando a organização realiza uma auto-avaliação, respondendo algumas perguntas fundamentais:

- *Onde estamos?*
- *Onde desejamos chegar?*
- *Como chegaremos lá?*
- *Como saberemos se chegamos?*

Para estas medições, são empregados modelos de maturidade para cada processo que permitem a crítica do status presente e as referências para melhoria, incluindo aspectos como nível de formalização dos processos desempenhados, ferramentas e automação para suporte ao processo, competências dedicadas para execução de cada processo, definição de papéis e responsabilidades, e avaliação de desempenho de cada processo. Categorizados de ***0*** (Inexistentes) a ***5*** (Otimizados) quanto à sua maturidade, os processos podem ser avaliados pelos *stakeholders* quanto à sua adequação e necessidade de melhoria.

• **Nível 0 (Inexistente)**: ausência de um processo identificável; a organização sequer reconhece a necessidade de implementação e execução das tarefas pertinentes.

• **Nível 1 (Inicial/*Ad Hoc*)**: o processo é desempenhado de maneira informal e não-padronizada, embora já possa existir a ciência por parte do corpo executivo de que há necessidade de melhoria. Como não há padrões sendo seguidos, a abordagem pode ser definida como caótica.

• **Nível 2 (Repetível, mas Intuitivo)**: processos são desempenhados de maneira similar por diferentes indivíduos, mas ainda há ausência de formalização, e os resultados dependem principalmente das competências individuais (ao invés de um conjunto de procedimentos padronizados). Neste nível de maturidade, o padrão de resposta do processo às demandas é geralmente reativo.

• **Nível 3 (Definido)**: procedimentos para execução do processo estão formalizados e divulgados para treinamento e capacitação, embora os resultados da execução não são avaliados e portanto não há tratamento de desvios por uma função gerencial. O planejamento do processo através da formalização permite uma abordagem proativa para resolução das demandas.

• **Nível 4 (Gerenciado e Mensurável)**: há gerenciamento das rotinas de execução do processo, de forma a avaliar a conformidade com os procedimentos definidos e tratar os resultados inesperados. Ferramentas e automação podem estar em utilização para execução e controle das tarefas. O processo é controlado com um nível de qualidade compatível ao de um serviço de qualidade definida para os respectivos clientes.

• **Nível 5 (Otimizado)**: o processo segue as melhores práticas do mercado, está sob monitoração constante com foco na melhoria contínua, e a TI contribui para execução dos processos de negócio de forma a garantir eficiência, qualidade e agilidade diante de mudanças. A proposta neste nível é garantir uma entrega crescente de valor para aqueles que dependem das saídas do processo.

3.10. Evolução do Modelo

Devido à utilização do modelo em situações reais de mercado e à característica colaborativa de sugestões de melhoria pela comunidade usuária para aperfeiçoamento constante, o COBIT apresenta evolução contínua visando agregar requisitos e práticas relevantes para aplicação no cotidiano. Em 2010 já se discute a nova versão (5) do modelo, incluindo temas como a chamada "TI verde", conjunto de práticas visando economia e sustentabilidade como uso racional do consumo de energia elétrica e utilização de insumos recicláveis na operação dos serviços de tecnologia. Conceitos como gerenciamento da informação e atenção aos requisitos dos *stakeholders* do negócio estão sendo discutidos em maior profundidade para esta nova revisão, de forma a adequar o modelo às necessidades de mercado avaliadas como gradualmente mais relevantes no contexto organizacional. Esta busca de incorporação de novas tendências em Governança de TI, assim como a modelagem do framework em busca de uma maior integração do acervo de publicações sobre o tema, são duas premissas fundamentais estabelecidas pelo ITGI na elaboração da versão 5 do COBIT.

4. APLICAÇÕES PRÁTICAS

Neste capítulo será apresentado, a partir do quadro teórico elaborado no capítulo 3, um conjunto de aplicações práticas dos princípios estabelecidos para o modelo, verificando sua validade em um contexto real e sugerindo sugestões de implantação e observações em cada conceito.

A primeira observação quanto à aplicação prática da disciplina de Governança de TI (e por conseqüência do modelo COBIT) é a necessidade de participação ativa da alta direção da organização na implantação e no apoio à metodologia escolhida. Por um lado, a área de TI deve receber do nível estratégico a direção na qual seus esforços devem ser canalizados. Baseados em análises críticas de cenários de risco (ameaças e oportunidades), tanto alta direção quanto a TI devem estar alinhados no que diz respeito a quais objetivos estratégicos perseguir. Ainda, as atividades desempenhadas pelas equipes de TI e os investimentos selecionados para perseguir estes objetivos devem estar fundamentados em dois pilares fundamentais, o orçamento necessário para custear os recursos definidos para cada demanda (infra-estrutura e profissionais) e a autoridade necessária para implementar as ações planejadas junto às demais áreas de negócio da organização. Esta análise é o foco do Alinhamento Estratégico proposto pelo COBIT.

Por outro lado, tendo o patrocínio da alta direção para perseguição dos objetivos propostos, a área de TI deve dispor de um profissional com um perfil hierárquico compatível com a responsabilidade assumida e com acesso à alta administração para expor demandas e soluções para os desafios de rotina e eventuais que a operação da tecnologia da informação cria. Embora esta posição normalmente sugira uma posição de Diretor de TI (também denominado CIO, *Chief Information Officer* ou CTO, *Chief Technology Officer*), é comum encontrar no mercado um profissional responsável por toda a TI com perfil apenas de gerente ou mesmo coordenador até em empresas de maior porte, subordinado frequentemente ao gestor da área administrativa ou financeira, quando não há percepção por parte dos líderes da administração do valor ou da criticidade da TI para a operação da empresa. Este posicionamento da função do líder da TI no organograma funcional da organização pode comprometer a autonomia necessária para execução dos projetos de tecnologia conforme seu planejamento e requisitos

acordados, ou ainda prejudicar a implantação de diretrizes de operação por conflitos políticos intransponíveis para um profissional sem respaldo hierárquico.

Obviamente, cabe a este profissional líder de TI dar transparência dos problemas vinculados à sua gestão e das soluções propostas para resolvê-los, mesmo que não exista por parte da alta administração uma percepção do valor da TI para o negócio. Independente do quanto o conselho enxergue mérito na atuação de TI, é responsabilidade do gestor desta área apresentar soluções e melhorias também para situações fora do escopo básico do seu trabalho: a TI é uma área de apoio, e a visibilidade alcançada ao se recomendar novas soluções ao negócio das demais áreas da organização agrega uma percepção de maior valor para os esforços realizados.

Quanto à percepção do valor entregue, será sempre mais complexo demonstrar para a alta administração os ganhos intangíveis de uma nova solução de TI para a operação. Um novo sistema que otimize o fluxo de trabalho de uma linha de produção, por exemplo, reduzindo custos com material e mão-de-obra empregados no processo, pode gerar indicadores numéricos claros para uma análise quantitativa. Outros benefícios porém podem ser mais elaborados em seu processo de aferição, resultando por exemplo em melhorias da imagem da empresa no mercado (refletindo-se em vendas diretas de bens ou serviços, menor necessidade de investimentos em publicidade ou maior captação de recursos humanos qualificados e motivados). O ponto pertinente neste tópico é honrar as expectativas da alta administração, se possível superando-as. Em projetos onde prazos, custos e qualidade estejam definidos desde o princípio, é relativamente fácil manter o foco na Entrega de Valor; no cotidiano onde há a preocupação em manter a operação de rotinas regulares sem desvios, o resultado esperado (sucesso) é dificilmente percebido, via de regra.

Considerando ainda os princípios fundamentais do framework COBIT, é importante ressaltar que cada processo implementado possui maiores chances de cumprir seus objetivos planejados quando a sistemática proposta pelo modelo é seguida na etapa de desenho, conforme os Controles de Processo. Os processos deverão ter objetivos pré-definidos para sua execução, sendo estes sempre que possível específicos, mensuráveis e realistas em sua descrição. O COBIT sugere a metodologia SMART para definição destes atributos (*Specific, Measurable, Actionable, Realistic, Results-Oriented, Timely*); a organização deve definir como este princípio melhor lhe atenderá. Ainda como um dos princípios dos Controles de

Processo, deve se assegurar que o processo seja repetível e previsível, capaz de oferecer sempre os resultados esperados em sua performance; em outras palavras, deve ser consistente com as expectativas dos interessados.

Uma função da organização deverá sempre ser eleita como o proprietário (dono) do processo, com autoridade para planejá-lo, implementá-lo, revisioná-lo e melhorá-lo, baseado na percepção de desempenho. Este papel será definido entre os demais envolvidos entre uma Matriz de Responsabilidade do processo (sugerida no COBIT pelo modelo RACI). Este colaborador deverá ser sempre único em cada processo, seguindo a lógica que apenas um indivíduo presta contas pelo resultado final de seu desempenho (embora vários possam ser responsáveis pela execução de diferentes etapas do processo, e tantos outros devam ser consultados ou informados do avanço de cada ação).

Outra característica vital no desenho (planejamento) de cada processo é a necessidade de se documentar todas as informações necessárias à sua execução (entre políticas, planos e procedimentos pertinentes). O COBIT recomenda cuidados quanto à manutenção, revisão pela função competente, divulgação entre os interessados e uso para treinamento de toda documentação relacionada aos processos de TI, de forma a mitigar riscos intrínsecos à operação, como por exemplo a utilização de documentos desatualizados ou a concentração de informações entre apenas alguns indivíduos (e não entre todos os que a necessitam).

O último princípio dos controles genéricos de processos é a promoção da melhoria contínua de cada processo. Este aspecto está diretamente relacionado aos indicadores de resultado e desempenho selecionados para mensurar cada um. A definição quanto ao que é medido, e qual o valor (meta) a ser alcançado nessa medição, é o principal substrato para quantificar a evolução de qualidade no processo. A experiência comprova que a organização deve sempre priorizar o estabelecimento de poucos indicadores de alta qualidade, em detrimento de um número alto de indicadores que não sejam representativos da real execução das atividades de cada processo. Ainda, estes indicadores devem traduzir informações úteis quanto à qualidade dos produtos (entregas) finais do processo, quanto à melhor utilização dos recursos disponíveis para a realização do mesmo (respeitando os princípios de eficiência e economicidade) e quanto à velocidade de execução das tarefas.

A utilização destes indicadores é uma prática a ser valorizada pois possui aplicações reais em outros modelos (como por exemplo o *Balanced Scorecard*) e é subsídio para processos de auditoria interna e externa, independentes do COBIT e mesmo de práticas de Governança de TI. A coleta, o armazenamento, a análise crítica e os planos de ação decorrentes destes indicadores são evidências de melhoria contínua, e quando se encontram rastreadas são fundamentais em processos de certificação ISO, por exemplo, demonstrando a maturidade organizacional da empresa.

Da mesma forma que o COBIT sugere os Controles de Processo para o planejamento dos processos internos de TI, a perspectiva de alinhamento da Governança de TI às necessidades de negócios da organização insere no COBIT outro método de atenção às melhores práticas, através dos chamados Controles de Aplicações. Estes consistem em aspectos fundamentais na elaboração de sistemas corporativos que traduzem as preocupações que a TI deve respeitar para implementar estas aplicações. O desenvolvimento destes sistemas (a programação propriamente dita) pode estar seguindo uma metodologia específica como o CMMI (*Capability Maturity Model Integration*), por exemplo, mas os Controles de Aplicações são requisitos maiores e absolutos que toda aplicação corporativa deve contemplar em sua construção. Quanto a este aspecto, o de planejamento de aplicações, o COBIT segrega as responsabilidades entre as áreas de negócio (definindo os requisitos e regras de negócio que as aplicações aplicarão às informações processadas, e utilizando-as na operação diária) e a área de TI (que implementará estes requisitos e regras nas ferramentas).

No início do ciclo de utilização das aplicações, o COBIT propõe controle sobre as informações a serem inseridas nos sistemas, tanto quanto à autorização e a qualificação das equipes responsáveis por estes dados fontes, como também pela segregação de tarefas a serem desempenhadas, de forma que indivíduos distintos sejam responsáveis por pontos diferentes de processamento dos dados. Estas aplicações deverão também ser capazes de levantar alertas quanto a erros de processamento de certas informações (sem prejuízo do processamento de informações corretas), de encaminhar as saídas destes sistemas para correta utilização das pessoas apropriadas, e de garantir a confidencialidade e integridade dos dados durante quaisquer transmissões entre partes.

Observa-se no mercado atualmente um nicho de trabalho especializado para a disciplina chamada Teste de Software, na qual metodologias específicas são aplicadas como controle de qualidade dos requisitos apresentados na elaboração dos projetos de desenvolvimento de aplicações. Essa área de atuação busca corrigir tanto falhas de implantação de regras de negócio de alto nível quanto problemas de integração de sistemas não passíveis de detecção em momentos de programação pontual de funções de sistema (testes unitários). Como há demanda constante entre as organizações para aquisição de sistemas cada vez mais adaptáveis às suas necessidades particulares, é natural a evolução do controle de qualidade destes serviços contratados de customização de software.

4.1. Processos do Domínio *Planejar & Organizar*

Os processos contidos no domínio Planejar & Organizar são todos voltados ao estabelecimento em alto nível das diretrizes a serem seguidas na execução das atividades sob a responsabilidade da TI. Infelizmente, na prática é observado que são tópicos frequentemente negligenciados no cotidiano das empresas quanto à maturidade com o qual são tratados. Geralmente a abordagem para essa esfera da Governança de TI é altamente informal, ou pelo menos não documentada, de forma que a TI segue as políticas aplicáveis às demais áreas da organização (quanto a avaliação de riscos no investimento em projetos ou quanto às políticas de recursos humanos, por exemplo) devido a ausência de processos próprios e apropriados às suas características, ou a uma não-percepção de necessidades diferenciadas para atender às suas demandas. Também pode ocorrer a decisão por não investir esforços na elaboração de planejamentos mais elaborados nos cenários de pequenas e médias empresas onde a aplicabilidade de cada processo COBIT pode não ser pertinente (como por exemplo no **PO2, *Definir a Arquitetura da Informação***, que propõe a classificação de dados que circulam nos sistemas de TI e é mais crítico em cenários onde há alta integração entre diferentes aplicações).

O processo mais crítico a ser estabelecido nesse contexto seria o **PO4, *Definir os Processos, a Organização e os Relacionamentos de TI***, onde questões fundamentais para a TI em qualquer empresa precisam ser resolvidas. Entre elas, a definição do planejamento dos processos a serem desempenhados pela TI; o estabelecimento das responsabilidades decisórias sobre a

priorização, execução e monitoração dos processos; e o posicionamento da TI dentro do organograma funcional (inclusive a organização interna da TI como departamento). Também são abordados nesse processo aspectos gerais da organização dos recursos humanos, como segregação de tarefas e a dependência da TI em pessoas-chave. Esses aspectos são elaborados com maior profundidade no **PO7, *Gerenciar os Recursos Humanos de TI***, que complementa o assunto com objetivos de controle voltados à captação e manutenção de profissionais capacitados (**PO7.3 *Preenchimento de Vagas***, **PO7.4 *Treinamento do Pessoal***) e a gestão do risco nessa área (**PO7.8 *Mudança e Desligamento de Cargo***).

O processo seguinte, **PO5, *Gerenciar o Investimento de TI***, é aquele no qual o gestor de TI poderá melhor demonstrar para a alta direção da organização sua responsabilidade com o investimento confiado à área de TI. Tanto nas despesas decorrentes da operação contínua (incluindo custos com folha de profissionais quanto manutenção da infra-estrutura atual) quanto nos orçamentos programados para cada novo projeto de TI iniciado, o percentual de receita da empresa reinvestido nas demandas de TI será observado criticamente pela alta direção como um ponto nebuloso de valor difícil de quantificar. Por este motivo, o COBIT propõe além de um objetivo de controle específico para seleção de investimentos (**PO5.2, *Priorização dentro do Orçamento de TI***), dois outros para mensurar o retorno da TI, **PO5.4 *Gerenciamento de Custo*** e **PO5.5 *Gerenciamento de Benefícios***, de forma a dar transparência ao processo.

No domínio *Planejar & Organizar* também está incluso o processo **PO8, *Gerenciar a Qualidade***, que utiliza princípios padrão de mercado para estabelecer diretrizes para a atuação de TI. Entre eles, o princípio do foco no cliente como direcionador dos esforços da TI (muitas vezes este cliente sendo interno à própria empresa), e a monitoração e análise crítica de resultados em alto nível como base para a melhoria contínua de processos. Este processo é o que propõe a adoção das melhores práticas de mercado para atuação em todos os demais processos do framework COBIT de forma a alcançar os melhores resultados, e a definição dos requisitos de qualidade que definirão se estes resultados estão sendo obtidos conforme o esperado. É importante observar que na implantação de quaisquer novos processos de TI, estes requisitos de qualidade deverão ser definidos a partir da observação do histórico de desempenho das atividades, quando houver, e das expectativas de satisfação dos clientes do serviço de TI estabelecido, de forma a se estabelecer características realistas.

De forma a refletir a conquista de uma expressão cada vez maior no mercado da disciplina de Gerenciamento de Projetos, com metodologias consagradas e altamente valorizadas como o PMBOK e o PRINCE2, o COBIT incluiu no domínio Planejar & Organizar um processo exclusivo para propor objetivos de controle voltados à gestão interna de projetos de TI, **PO10, *Gerenciar Projetos***. De forma análoga a metodologia de gestão de projetos do *Project Management Institute* (PMI), esses objetivos de controle contemplam as diferentes fases do ciclo de vida do projeto (**PO10.6 *Fase de Início do Projeto***, **PO10.13 *Medição de Desempenho, Monitoramento e Reporte do Projeto***, **PO10.14 *Conclusão do Projeto***), assim como diferentes áreas de conhecimento (**PO10.5 *Declaração do Escopo do Projeto***, **PO10.7 *Plano Integrado de Projeto***, **PO10.8 *Recursos do Projeto***, **PO10.9 *Gestão de Risco do Projeto***, **PO10.10 *Plano de Qualidade de Projeto***). Para a gestão de riscos, independente de sua avaliação em projetos de TI, o COBIT propõe ainda um processo próprio e separado, **PO9, *Avaliar e Gerenciar os Riscos de TI***, no qual novamente melhores práticas de mercado são recomendadas, como a classificação dos riscos com base em probabilidade de ocorrência e o impacto nos negócios, seu mapeamento de acordo com os responsáveis em definir e implementar os planos de ação necessários, e a tolerância e aceitação dos riscos baseado na relação custo-benefício de cada plano de ação proposto.

4.2. Processos do Domínio *Adquirir & Implementar*

No domínio *Adquirir & Implementar* começam a surgir as aplicações práticas do modelo COBIT, devido ao momento de decisão entre soluções de plataformas e tecnologias específicas para atender às demandas da organização.

No processo **AI1, *Identificar Soluções Automatizadas***, por exemplo, as áreas de negócio devem trabalhar com a TI para definir quais requisitos cada solução de TI deve atender para alcançar os resultados necessários. Encontram-se nesta análise os requisitos técnicos que devem estar presentes na solução, assim como características auxiliares que influenciarão a escolha no processo de aquisição pela organização. Tanto TI quanto áreas de negócio devem estar alinhadas quanto à priorização de características como integração da solução ao ambiente da empresa, investimento necessário, cronograma de implantação, de forma a

manter todas as expectativas quanto ao projeto de acordo com a realidade (em um cenário ideal, conseguindo uma realidade que se encaixe nas expectativas gerais).

De grande aplicabilidade no mercado atualmente, o processo **AI2, *Adquirir e Manter Software Aplicativo***, descreve os objetivos de controle a serem seguidos na implementação de aplicações corporativas de alto valor para a organização. Tanto o atendimento dos requisitos básicos a serem atendidos na solução, quanto a manutenção da aplicação no período posterior à fase inicial de implantação, os principais aspectos da gestão de um sistema de alta criticidade estão contemplados no processo. Observa-se uma grande relevância do processo no contexto de mercado atual, onde os custos de implementação de um sistema vital para os negócios da empresa são significativos (entre licenciamento do software, treinamento de equipes envolvidas, investimento em infra-estrutura de hardware, entre outros). Contratando uma solução inédita e própria ou trazendo do mercado uma solução pronta a ser customizada ao ambiente corporativo, os riscos de um projeto como esse podem ser fator crítico na imagem da TI dentro da organização. Para um bom planejamento do projeto, recomenda-se o uso dos Controles de Aplicações discutidos anteriormente, para uma visão abrangente dos requisitos técnicos da solução selecionada.

De maneira similar a este, o processo **AI3, *Adquirir e Manter Infraestrutura de Tecnologia,*** reforça através de seus objetivos de controle a importância dos componentes de infra-estrutura, não só no momento da seleção e aquisição dos ativos, mas também através da monitoração e custódia de cada um, quanto à responsabilidade e ao melhor uso de cada componente dessa infra-estrutura. O processo prevê o desenvolvimento de planos regulares de manutenção e monitoração de disponibilidade de forma a garantir a qualidade e o desempenho dos componentes e dispositivos do ambiente.

O processo seguinte, **AI4, *Habilitar Operação e Uso***, é focado no treinamento de todos os colaboradores envolvidos na operação da solução de TI. É pertinente aos líderes das áreas de negócio, porque é o processo que transfere a propriedade da aplicação para a utilização de suas respectivas equipes. Também é pertinente aos colaboradores que farão uso regular do sistema em suas rotinas de trabalho, assim como para os profissionais de TI que deverão estar capacitados a dar o suporte técnico e operacional necessário para o desenvolvimento destas atividades. Para facilitar essa multiplicação do conhecimento, o processo propõe a

documentação de todos os aspectos relevantes à operação da ferramenta logo em seu primeiro objetivo de controle, **AI4.1, *Planejamento para Soluções Operacionais***. É importante ressaltar que há também grande nicho de mercado para atender essas demandas de treinamento, com cursos voltados tanto para profissionais que usarão a aplicação em suas rotinas diárias, como para profissionais de TI que buscam se qualificar no suporte técnico a essas ferramentas (inclusive com opções de certificação).

De forma complementar aos processos **AI2** e **AI3**, o processo **AI5, *Adquirir Recursos de TI***, propõe a execução de um procedimento de aquisição em TI com planejamento consistente, alinhados com as demais práticas da organização para contratação de fornecedores, visando sempre o estabelecimento de contratos com responsabilidades claras para todas as partes. Tendo em vista esses princípios, a TI deve sempre que possível buscar apoio na execução do processo junto à área de aquisições (de forma a recrutar os especialistas em negociações contratuais) e à área jurídica (de forma a assegurar que todos os requisitos legais e contratuais com terceiros sejam respeitados).

Os demais processos do domínio *Adquirir & Implementar* trabalham de forma conjugada para tratar mudanças e evoluções na infra-estrutura e aplicações do ambiente de TI: **AI6, *Gerenciar Mudanças*** e **AI7, *Instalar e Homologar Soluções e Mudanças***. De modo característico, a forma como estas atividades são tratadas no cotidiano de uma organização são um dos principais indicadores de maturidade geral da área de TI. O princípio básico que rege ambos os processos é que eles deves seguir um planejamento documentado, que contemple os riscos inerentes à atividade, como uma indisponibilidade de um serviço crítico, e o plano de retorno à situação anterior em caso de falhas na implementação do novo serviço.

4.3. Processos do Domínio *Entregar & Suportar*

Para o domínio Entregar & Suportar, os processos propostos pelo COBIT se voltam menos para novos projetos e mais para o apoio à operação regular de serviços de TI no ambiente das organizações. Nesse domínio observa-se uma grande variedade de ferramentas automatizadas disponíveis no mercado para apoio a esses processos, entre sistemas de gestão de relacionamento com clientes (CRM) adaptados à operação de centrais de atendimento (*Service*

Desks e *Call Centers*), a aplicações dedicadas à monitoração de disponibilidade de ativos de TI interligados em rede (inclusive apoiando as tarefas de inventário de equipamentos e licenciamento de software).

O primeiro dos processos, **DS1, *Definir e Gerenciar Níveis de Serviços***, se propõe a manter sob controle os níveis esperados de qualidade dos serviços de TI entregues aos usuários de cada um. As expectativas do cliente quanto ao desempenho de prestadores de serviço (internos ou externos) é fator crítico de sucesso em contratos, e a formalização de responsabilidades do fornecedor garante segurança ao cliente na contratação de um serviço. Os Acordos de Nível de Serviço (*Service Level Agreements, SLAs*) no mercado de TI são comumente definidos através de tempos de resposta para solução de solicitações demandadas, principalmente em situações de indisponibilidade de serviços críticos à operação da empresa, e a monitoração da conformidade do desempenho real ao planejado transmite uma maior imagem de valor do serviço coberto pelo SLA. Como equipes internas da empresa também podem estar vinculadas a trabalhar sob um SLA, o termo é aplicável por exemplo a um time de suporte a aplicações.

O processo seguinte trabalha de maneira associada ao gerenciamento de níveis de serviços. O **DS2, *Gerenciar Serviços Terceirizados***, coloca entre seus objetivos de controle a monitoração do desempenho de todos os fornecedores críticos para a operação e os projetos da organização, assim como a gestão do risco associado a esse nível de dependência externa, através de responsáveis pelos contratos relacionados. Estes objetivos demonstram a importância de um método de avaliação propriamente definido como indicadores de desempenho.

Quanto ao desempenho dos serviços de TI, o COBIT define no **DS3, *Gerenciar o Desempenho e a Capacidade***, princípios para sua monitoração quanto à demanda atual e capacidade futura, de forma a garantir que estejam sempre sendo analisados em conjunto para atender as necessidades de operação. Como aumentos de capacidade dos serviços implicam em revisão de orçamentos vinculados, este processo contribui com saídas (informações de mudanças necessárias) para planos de ação que consideram custos de infra-estrutura.

O processo seguinte, **DS4, *Assegurar a Continuidade dos Serviços***, trabalha pontos cruciais para o planejamento de médio e longo prazo da empresa, embora sejam freqüentemente negligenciados no cotidiano das operações. Neste tópico deve ser elaborada a relação de serviços de TI através dos quais atividades operacionais críticas da empresa são desempenhadas. O levantamento destes serviços (e os riscos que podem torná-los indisponíveis para os usuários) e o mapeamento de possíveis soluções de contorno para estes possíveis problemas compõem um plano de continuidade que intenciona mitigar, eliminar ou transferir riscos para minimizar impactos contra a organização. Até os riscos aceitos pela empresa (isto é, aqueles contra os quais a empresa decide não elaborar plano de resposta) compõem o plano, e formalizam o planejamento de contingência contra situações adversas no ambiente da empresa. Mesmo após elaborado, o plano de continuidade deve ser colocado em prática em simulações de risco real, para testar os procedimentos definidos para cada solução e periodicamente garantir a capacitação dos colaboradores responsáveis pela correção de cada risco. Novamente, estes objetivos de controle implicam em custos para a empresa (equipamentos de contingência, rotinas de *backup* periódico, etc.) que podem ser considerados justificáveis apenas após a ocorrência de um prejuízo real para a organização após a concretização de um risco previsto (mas não tratado). Portanto, a apresentação destas necessidades de investimento demanda da área de TI uma perfeita apresentação dos possíveis cenários de ocorrência e os benefícios de um modelo de prevenção.

Para fins de segurança do ambiente de TI, o modelo COBIT consolida no processo **DS5** (***Garantir a Segurança dos Sistemas***) diferentes objetivos de controle, tendo como um princípio a gestão de identidades para acesso aos serviços. Os indivíduos devem receber mecanismos de autenticação validados por colaboradores em diferentes pontos do fluxo de autorização (entre seus gestores diretos que solicitam o acesso e os gestores dos sistemas que os permitem), de forma a garantir apenas os acessos necessários ao desempenho de suas funções e a rastreabilidade das ações dentro de cada sistema corporativo (quando o mesmo é planejado seguindo as melhores práticas de mercado). Em organizações de maior porte, equipes de trabalho podem estar dedicadas exclusivamente para a gestão da segurança de rede, monitorando possíveis falhas e incidentes, propondo melhorias para o controle de vulnerabilidades, e definindo políticas para tratamento de questões da TI como ferramentas antivírus, criptografia, regras para acesso a Internet e controle de mensagens *spam*. Fundamental nesse tópico é também o controle do tráfego de informações entre os ambientes

interno e externo da organização, principalmente quando a empresa se julga vulnerável ao vazamento de informações privilegiadas.

Fazendo a ponte entre diferentes processos de múltiplos domínios, está o **DS6** (***Identificar e Alocar Custos***) que defende o rastreamento de todos os custos vinculados aos serviços de TI e seu respectivo rateio entre os diferentes centros de custo da organização de forma que as áreas de negócio tenham visibilidade do perfil de consumo dos recursos vinculados. Sugere-se neste processo utilizar para a TI os mesmos critérios de rateio, quando houverem, aplicados a outros recursos compartilhados da organização. Esta proposição pode permitir um modelo de bilhetagem mesmo internamente à organização que, ao exibir indicadores mensuráveis e previsíveis, permita também o uso apropriado dos recursos disponíveis (por exemplo, através do controle mais restrito de conteúdos específicos no acesso à Internet quando o orçamento de telecomunicações já se encontra no limite máximo tolerável pela alta direção). O controle destes custos também representa uma importante ferramenta gerencial quando confronta custos e despesas de TI previstos com os realizados (entre pessoal, materiais e serviços), demonstrando a precisão dos métodos de previsão estabelecidos.

Outro processo destinado a treinamento e capacitação de colaboradores é o **DS7, *Educar e Treinar os Usuários***, que diferente do **AI4** (***Habilitar Operação e Uso***), objetiva manter um programa regular de treinamento para os colaboradores da organização, e não apenas na adoção ou atualização de novas tecnologias. O planejamento deste programa tem por fundamento a detecção das necessidades de treinamento de cada equipe-alvo, a identificação dos colaboradores da empresa com o perfil de multiplicadores do conhecimento, e a avaliação de pré-requisitos e resultados de cada treinamento ministrado. O foco do processo é garantir a produtividade na operação de cada tecnologia, tanto pelo uso pleno de todas as funcionalidades das ferramentas de TI quanto pela redução de erros e retrabalho no desempenho das atividades suportadas pela TI.

Para a área de maior visibilidade da operação de TI, o atendimento e suporte técnico aos usuários dos serviços de TI, o COBIT estabeleceu um processo principal denominado **DS8, *Gerenciar a Central de Serviço e os Incidentes***, no qual diversas melhores práticas de mercado (propostas inclusive em metodologias afins como o *ITIL*) estão previstas para implantação. Fundamental neste processo é o primeiro objetivo de controle, o estabelecimento

da função de *Service Desk* (Central de Serviços), uma equipe dedicada a realizar o contato direto com os usuários dos serviços de TI, registrando, analisando e direcionando para resolução todas as solicitações encaminhadas pelos clientes. Esta equipe é a responsável pela monitoração constante dos atendimentos em andamento de forma a garantir o cumprimento dos *SLAs* acordados em cada demanda (através de procedimentos padronizados de priorização e escalonamento). Observa-se no mercado que a função do *Service Desk* é adotada em larga escala mesmo fora do ambiente de TI, quando centrais de atendimento de operadoras de telefonia ou cartões de crédito, por exemplo, trabalham sob os mesmos conceitos (registro de todas as solicitações através de números de protocolo, resolução de atendimentos em 1º nível, encaminhamento de atendimentos mais elaborados para equipes especialistas, etc.). A implantação de ferramentas específicas para esta função inclusive permite a automatização dos fluxos de trabalho e a geração de estatísticas de atendimentos demonstrando a demanda pelos usuários e a produtividade das equipes atendentes. A centralização das tarefas de registro de solicitações, monitoração constante de seu status e informe aos clientes do andamento de cada registro estabelece outro termo técnico de mercado para a Central de Serviços: Ponto Único de Contato (*Single Point of Contact*). Para o COBIT, a Central de Serviços deve gerenciar os *incidentes* propriamente ditos (que correspondem às interrupções ou perdas de qualidade nos serviços), assim como também as *solicitações de informação* e as *solicitações de serviço padrão* (estas últimas não significando necessariamente uma falha do serviço em questão).

Para fins de controle de configuração, isto é, o registro correto de todas as características de um equipamento ou sistema de TI, o processo **DS9, *Gerenciar a Configuração***, estabelece objetivos de controle para o gerenciamento destas informações. O processo recomenda o uso de ferramenta própria para repositório destes dados, capaz de estabelecer uma linha de base (baseline) para a configuração padrão do recurso; isto garante a disponibilidade da informação necessária para recuperação de um serviço em caso de alterações do perfil do recurso (exemplos: *Que configurações deste modelo de equipamento são necessárias para executar tal sistema? Quais características do sistema precisam estar conformes para o serviço estar disponível aos clientes?*). O gerenciamento destas informações de configuração é um processo dinâmico e condicionado às alterações do ambiente controladas através dos processos de gerenciamento de mudanças (**AI6** e **AI7**). Ainda, através do objetivo de controle **DS9.3, *Revisar Integridade de Configuração***, é proposto o controle periódico de *software* instalado

indevidamente no parque de equipamentos da organização, de forma a regular uso dos mesmos para fins particulares e detectar licenças de programas instaladas acima das quantidades contratadas (o que expõe a empresa a riscos financeiros e legais).

Outro conceito estabelecido no mercado de TI é associado à gerência de incidentes (discutida no **DS8**): a gerência de problemas. O processo dedicado a esse tópico (**DS10, *Gerenciar Problemas***) parte da mesma definição estabelecida em normas como a ISO 20.000, em que problema é "a causa desconhecida de um ou mais incidentes". Na prática, a gerência de problemas é responsabilidade de um time de especialistas designados pela organização para resolução de ocorrências de maior gravidade no ambiente de TI que requerem conhecimento aprofundado da infra-estrutura e das aplicações que suportam os serviços. Ao elaborar soluções de contorno ou definitivas para as falhas do ambiente, a gerência de problemas maximiza disponibilidades dos serviços, garantindo a manutenção de *SLAs*, e contribui portanto para o aumento de satisfação do usuário final destes serviços. A ideal interação entre a Central de Serviços e a gerência de problemas permite a triagem das ocorrências mais simples pela primeira (poupando o tempo dos profissionais especialistas da segunda) e a montagem de uma base de conhecimento que integre soluções para os erros conhecidos do ambiente da organização. De forma geral, os processos do domínio ***Entregar e Suportar*** trabalham de forma bastante integrada (entre si e com processos de outros domínios), pois uma causa-raiz de diversos incidentes, gerenciados pela Central de Serviços (**DS8**), após rastreada pela gerência de problemas (**DS10**), pode ser identificada em determinado componente da infra-estrutura (**DS9**) e motivar uma mudança em um sistema a ser controlada pela gerência de mudanças (**AI6/AI7**).

De maneira associada ao **DS5**, o processo **DS11** (***Gerenciar os Dados***) propõe o estabelecimento de garantias para processamento, armazenamento e descarte de informações (e das mídias que as suportam) de maneira a atender os requisitos de negócio da organização. Para fins de segurança e conformidade com obrigações legais, contratuais ou regulatórias, a organização deve garantir por exemplo que cópias de segurança dos sistemas corporativos sejam arquivadas de maneira segura (em ambientes adequados) e por períodos mínimos (em caso de necessidade de recuperação). Este objetivo de controle em particular (**DS11.5, *Backup e Restauração***) está fortemente associado ao plano de continuidade previsto no processo **DS4**. Também deve estar implementada uma política de descarte seguro de mídias

ou equipamentos de forma a assegurar que informações críticas da organização não sejam distribuídas indevidamente ou criem complicações legais. Até o descarte consciente de resíduos eletrônicos pode ser incorporado ao processo, tendo em vista a atenção corrente da mídia com o tema.

O processo seguinte, **DS12, *Gerenciar o Ambiente Físico***, também está vinculado ao planejamento para contingências ao promover recomendações para a administração dos espaços críticos que hospedam os principais equipamentos da TI. Atualmente há um nicho específico no mercado de TI para hospedagem de serviços em ambientes de alto controle (*datacenters*), com salvaguardas, por exemplo, contra interrupções de alimentação elétrica e climatização constante de forma a manter sistemas em alta disponibilidade. Estes espaços de hospedagem, de acesso restrito, são selecionados por empresas que desejam confiar seus recursos mais críticos a ambientes com monitoração em regime constante (24 horas x 7 dias/semana x 365 dias/ano). O investimento correspondente a esse tipo de serviço é percebido nessas situações como justificável em vista da segurança trazida pelos recursos disponíveis.

O último dos processos do domínio *Entregar e Suportar*, **DS13, *Gerenciar as Operações***, engloba as demandas de rotina como o processamento de dados nos sistemas corporativos em caráter regular pelas equipes de TI, a monitoração de disponibilidade e capacidade de sistemas através de processos padrão, assim como a manutenção preventiva de equipamentos. A padronização destas rotinas é aplicada idealmente em operações onde turnos de trabalho se sucedem, e relatórios de acompanhamento são passados entre as equipes para continuidade de serviços de uma escala para outra. Neste processo como em poucos outros é fundamental a documentação abrangente e precisa das tarefas, pois a aderência a procedimentos padronizados facilita a previsibilidade das ações a serem executadas, que por sua vez garante a produtividade no desempenho de cada uma.

4.4. Processos do Domínio *Monitorar & Avaliar*

Os processos subordinados ao domínio *Monitorar & Avaliar* estão explicitamente voltados para verificação de desempenho e resultado de outras ações de TI no ambiente organizacional.

Tendo isto em vista, torna-se recomendável instituir como responsáveis pela análise crítica das evidências enumeradas para cada um destes monitoramentos e avaliações colaboradores isentos de opinião pré-formada sobre o escopo de cada análise.

O primeiro destes processos, **ME1, *Monitorar e Avaliar o Desempenho de TI***, estabelece princípios para definição e coleta dos dados que informam desempenho e resultados das atividades de TI, assim como para o estabelecimento dos indicadores e metas contra os quais os dados serão comparados. O processo propõe também que os indicadores medidos sejam adequados a um método (se possível, inseridos no próprio modelo maior de avaliação de desempenho da organização, quando houver, como por exemplo o *Balanced Scorecard*), e que quaisquer desvios detectados sejam tratados através de planos de ação correspondentes. Além do acompanhamento destas correções até a sua resolução, o processo também recomenda a consolidação de todas essas informações (atividades, resultados, planos de ação e resoluções) em relatórios regulares para a alta direção, como forma de prestação de contas e transparência quanto às realizações da TI em contribuição à organização.

Para um outro nível de monitoração, o processo **ME2 (*Monitorar e Avaliar os Controles Internos*)** propõe ações de controle gerencial de forma a mitigar desvios na operação da TI que possam impactar o negócio. O processo sugere a supervisão e revisão constante dos processos (inclusive através de auto-avaliação) de forma a garantir eficácia e eficiência no desempenho das atividades de TI, e o rastreamento para prevenção de reincidência da causa-raiz de desvios conhecidos. Como a revisão destes processos é válida também pela ação de agentes externos, as auditorias de qualidade sobre toda a organização constituem oportunidades de melhoria quando há detecção de pontos fracos na operação interna. Considerando a criticidade do negócio ou de contratos específicos, há margem inclusive para avaliação de conformidade de parceiros de negócio da organização (principalmente em situações onde empresas associam-se em projetos comuns sob acordos de confidencialidade).

De maior relevância no cenário recente de TI é o processo **ME3, *Assegurar a Conformidade com Requisitos Externos***, tendo em mente que no mercado brasileiro um crescente número de empresas busca mecanismos de certificação de sua conformidade a padrões normativos (compulsórios ou não). Como exemplo mais evidente desta tendência, destaca-se a **Lei Sarbanes-Oxley** (2002), originária dos Estados Unidos, que impõe requisitos para empresas

com títulos negociados em mercados financeiros norte-americanos (por exemplo *ADRs*, *American Depositary Receipts*, negociadas na *NYSE*), inclusive as que forem de origem estrangeira. A proposta desta regulamentação é garantir segurança a investidores através de mecanismos rigorosos de auditoria e controle, e coincidentemente o *framework* COBIT é o modelo de referência no mercado para que os requisitos da lei voltados à TI estejam em conformidade (em especial na seção 404, que dispõe sobre controles e procedimentos internos para emissão de relatórios financeiros). Entre as empresas brasileiras que atualmente estão sob obrigatoriedade destes requisitos relacionam-se:

- *Petrobras*
- *GOL Linhas Aéreas*
- *Sabesp*
- *TAM Linhas Aéreas*
- *Brasil Telecom*
- *Ultrapar (Ultragaz)*
- *Grupo Pão de Açúcar*
- *Banco Itaú*
- *Telemig Celular*
- *Eletrobrás*

Por fim, o processo final do COBIT, **ME4, *Prover Governança de TI***, faz o fechamento de todas as ações de Governança de TI que devem estar implementadas para a melhor gestão das responsabilidades afins. Entre estas ações está a instituição de um modelo interno de governança de TI que incorpore em suas políticas e processos internos os cinco pilares (áreas de foco) propostos pelo COBIT como fundamentais para sucesso: **alinhamento estratégico** com os objetivos de negócio da organização; **entrega de valor** correspondente aos investimentos realizados nos projetos de TI; **gerenciamento de recursos** eficaz e eficiente de TI (infra-estrutura, aplicações, pessoas e informações); **gestão de riscos** condizente com a tolerância da organização aos mesmos; e **medição de desempenho** que garanta a transparência dos resultados alcançados pela TI à alta direção. O processo também retorna ao tema de garantia por parte independente (interna ou externa) da conformidade das ações da TI à requisitos legais/regulatórios, às melhores práticas de mercado, aos princípios de eficácia e eficiência, e aos princípios internos da organização quanto a políticas e procedimentos corporativos.

5. CONCLUSÃO

Sumarizando os assuntos e considerações apresentados no decorrer deste trabalho, esta conclusão visa ratificar a relevância do tema de Governança de Tecnologia da Informação no contexto atual de mercado, onde serviços de TI encontram-se posicionados de forma crucial no desempenho de praticamente toda cadeia de valor de uma organização.

A abordagem selecionada por cada empresa para tratamento desse tema é fator determinante para a competitividade de cada uma, indiscutivelmente no desempenho de seus processos internos e freqüentemente nos resultados de suas próprias áreas de atuação no mercado. A TI se encontra atualmente em um nível de integração com as áreas de negócio que garante que seu pleno uso seja um fator de qualificação de concorrentes e de fracasso para as organizações que não acompanharem o ritmo de evolução cada vez mais acelerado.

A Governança de TI representa inclusive uma face importante do tópico de Governança Corporativa no seu âmbito mais abrangente, pois além de apoiar os princípios de controles internos, também apóia a operação das demais áreas e departamentos das organizações que devem também seguir os fundamentos da Governança Corporativa. Dentre estes destacam-se os princípios de prestação de contas e alinhamento estratégico, que comumente são deixados em segundo plano quando a TI não é regida por uma metodologia estabelecida de governança.

A utilização do COBIT como um *framework* padrão consagrou-se no mercado pela abrangência de escopo que o modelo propõe (desde o suporte a usuários de serviços ao desenvolvimento de novos sistemas, passando pelo modelo optado de *outsourcing* de serviços de TI e pela capacitação dos recursos humanos da área), ganhando força como referência em auditorias de conformidade como a Lei Sarbanes-Oxley e diferentes normas ISO. Tanto o fato de que este framework engloba outras metodologias de TI específicas a segmentos de atuação (como ITIL e CMMI) quanto a possibilidade de se adaptar os processos propostos ao contexto de cada organização contribuem para sua adoção em larga escala.

A abrangência e a extensão do material de referência do modelo COBIT, ao definirem diferentes fundamentos e múltiplos processos para gerenciar projetos e operações de TI, permitem mesmo para as organizações que não possuem estrutura alguma implementada um

caminho através do qual podem perseguir um processo de melhoria contínua, partindo de políticas de alto nível até as melhores práticas de nível operacional. O modelo permite a implementação gradual dos processos conforme cada organização priorizar suas necessidades, facilita a comunicação entre TI e áreas de negócio através de uma linguagem comum, e sugere métricas para acompanhamento de desempenho que são conceitos maiores da prática de gestão empresarial.

A maturidade estabelecida para cada processo de TI pode refletir a estratégia corporativa no âmbito interno da organização, mostrando o perfil de tolerância a risco e pioneirismo da empresa na seleção de tecnologias emergentes, assim como no apoio às operações internas das diferentes áreas de negócio, sendo cada processo representativo da prioridade da alocação de recursos definida pela alta direção. Principalmente no que diz respeito à vulnerabilidade aos riscos internos e externos, a prioridade com a qual o corpo executivo trata toda a TI dá transparência de sua maturidade como gestores.

6. REFERÊNCIAS BIBLIOGRÁFICAS

CARVALHO, T.C.M.B. (coord.) *TI – Tempo de Inovação: um estudo de caso de planejamento estratégico colaborativo*. São Paulo, M.Books, 2010.

FERNANDES, A.A. *Implantando a governança de TI: da estratégia a gestão dos processos e serviços*. Rio de Janeiro, Brasport, 2008.

FOINA, P.R. *Tecnologia de informação: planejamento e gestão*. São Paulo, Atlas, 2009.

ITGI (IT Governance Institute). *COBIT 4.1*, Rolling Meadows, 2007.

____ . *COBIT Control Practices, 2nd Ed*, Rolling Meadows, 2007.

____ . *Board Briefing on IT Governance, 2nd Ed*, Rolling Meadows, 2003.

LAHTI, C.B. *Sarbanes-Oxley Conformidade TI usando COBIT e ferramentas open source*. Rio de Janeiro, Alta Books, 2006.

MAGALHÃES, I.L. *Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL*. São Paulo, Novatec, 2007.