

**Universidade Federal de Santa Catarina
Departamento de Informática e Estatística
Curso de Ciência da Computação**

**Uma Análise Comparativa de Metodologias para
Governança de Tecnologia da Informação – ITIL e COBIT**

**MARÍLIA GABRIELA SODRÉ
SUZANA MARIA DE SOUZA**

Florianópolis – SC
Ano 2007 / 1

MARÍLIA GABRIELA SODRÉ
SUZANA MARIA DE SOUZA

**Uma Análise Comparativa de Metodologias para
Governança de Tecnologia da Informação – ITIL e COBIT**

Trabalho de conclusão de curso apresentado como parte dos requisitos para
obtenção do grau de Bacharel em Ciência da Computação

Orientadora: Profa. Dra. Eng. Maria Marta Leite

Banca Examinadora

Profa. Dra. Eng. Aline França de Abreu
Prof. Dr. Eng. João Bosco da Mota Alves
Prof. Dr. Eng. João Cândido Dovicchi

Resumo

A Governança de TI destaca-se no atual cenário dinâmico e competitivo dos negócios como um conjunto de mecanismos que permitem estabelecer objetivos, formular controles, executar estratégias e avaliar os resultados obtidos pela Tecnologia da Informação. A tecnologia deixou de ser apenas uma área de suporte para tornar-se um parceiro estratégico no alcance dos objetivos do negócio. As organizações que compreendem este conceito e conseguem incorporar os objetivos da governança em sua estrutura adquirem condições para aperfeiçoar o gerenciamento de sua infra-estrutura e serviços de TI.

Aprimorar controles e processos requer investimento e comprometimento das partes envolvidas, assim, é necessário que a organização avalie seus objetivos de acordo com quais resultados deverão ser alcançados e quais são as prioridades para o negócio. Para tal, estão disponíveis diversos modelos (*frameworks*) de melhores práticas consolidadas em diversas organizações. Tais práticas atuam como guias para o estabelecimento de controles e métricas que se alinham para o alcance da governança. Neste trabalho realiza-se uma revisão bibliográfica de dois modelos de destaque nessa área: o COBIT, como um *framework* de melhores práticas para governança e auditoria de TI, e o ITIL, um *framework* para gerência de serviços e infra-estrutura de TI. Individualmente ou integradas, essas ferramentas constituem um poderoso recurso para aderência aos objetivos da governança, aprimoramento dos controles internos e conformidade às práticas regulatórias, como a Lei Sarbanes-Oxley¹.

Palavras-chave: Tecnologia da Informação, Governança de TI, Alinhamento Estratégico, Gerência de TI, COBIT, ITIL, modelo de maturidade, melhores práticas, auditoria de sistemas, controle, conformidade, Sarbanes-Oxley, normas, padrões.

¹ Decreto para proteger os investidores e o público em geral de erros na contabilidade e práticas fraudulentas na organização (SOX, 2002 apud Holm; Kühn; Viborg, 2006, p. 3).

Abstract

In the current dynamic and competitive scene of the businesses, the IT Governance is distinguished as a set of mechanisms that allows establishing objectives, to formulate controls, to execute strategies and to evaluate the Information Technology's results. The technology isn't more only an area of support. Now, it's a strategical partner in the reach of the business's objectives. The organizations that understand this concept and obtain to incorporate the objectives of the governance in your structure, acquire conditions to perfect the management of your infrastructure and IT services.

Improving controls and processes requires investment and compromising of the involved parts. Thus, it's necessary that the organization evaluates its objectives in accordance with which results will have to be reached and which are the priorities for the business. For such, they are available diverse frameworks of better practical consolidated in diverse organizations. Such practices act as guides for the establishment of metrics and controls that are line up for the reach of the governance. In this work, a bibliographical revision of two models of prominence is become fulfilled: COBIT, as a framework of best practices for governance and IT audit, and ITIL, a framework for services management and IT infrastructure. Individually or integrated, these tools constitute a powerful resource for adhesion to the objectives of the governance, improvement of the internal controls and conformity to the regulator practices, as the Sarbanes-Oxley law.

Keywords: Information Technology, IT Governance, Strategical Alignment, IT Management, COBIT, ITIL, model of maturity, best practices, systems audit, control, conformity, Sarbanes-Oxley, norms, standards.

Sumário

1	INTRODUÇÃO	1
1.1	APRESENTAÇÃO	3
1.2	FORMULAÇÃO DO PROBLEMA	3
1.3	JUSTIFICATIVAS	4
1.4	OBJETIVOS	5
1.4.1	Objetivo Geral	6
1.4.2	Objetivos Específicos	6
1.5	DELIMITAÇÃO DO ESCOPO	6
1.6	METODOLOGIA DE DESENVOLVIMENTO	7
1.6.1	A Pesquisa e o Método	7
1.6.2	Caracterização da Pesquisa	8
1.7	ORGANIZAÇÃO DO TRABALHO	9
2	REFERENCIAL TEÓRICO	10
2.1	PLANEJAMENTO ESTRATÉGICO DOS NEGÓCIOS	10
2.2	PLANEJAMENTO ESTRATÉGICO DE TI	12
2.3	ALINHAMENTO ESTRATÉGICO DA TI	15
2.3.1	Alinhamento Estático e Alinhamento Dinâmico	25
2.3.2	Análise de Alinhamento	25
2.4	A LEI SARBANES – OXLEY	26
2.4.1	Implicações da SOX quanto à governança de TI	29
3	GOVERNANÇA EM TECNOLOGIA DE INFORMAÇÃO	33
3.1	INTRODUÇÃO	33
3.2	FATORES MOTIVADORES	38
3.3	OBJETIVOS DA GOVERNANÇA DE TI	40
3.4	FRAMEWORKS PARA GOVERNANÇA DE TI	41
4	O COBIT - VERSÃO 4.0	49
4.1	O CRIADOR	49
4.2	ORGANIZAÇÃO – OS SEIS COMPONENTES DO COBIT	50
4.3	RESUMO EXECUTIVO	50
4.4	O FRAMEWORK COBIT	58
4.4.1	Por que adotar um <i>framework</i>	58
4.4.2	A quem se destina o <i>framework</i>	61
4.4.3	Focado no Negócio	61
4.4.4	Baseado em Controles	65
4.4.5	Direcionado à Medição	67
4.5	A ESTRUTURA DO FRAMEWORK DO COBIT	72
4.6	OS DOMÍNIOS DO COBIT	75
4.7	ACEITABILIDADE DO COBIT	79
5	O ITIL	81
5.1	O CRIADOR	81
5.2	O FRAMEWORK ITIL	82
5.3	OS LIVROS DO ITIL - VERSÃO 2	86
5.3.1	Prestação de Serviço	89

5.3.1.1	Gerenciamento de Níveis de Serviço.....	90
5.3.1.2	Gerenciamento Financeiro para os Serviços de TI.....	91
5.3.1.3	Gerenciamento da Capacidade	94
5.3.1.4	Gerenciamento da Continuidade dos Serviços de TI.....	96
5.3.1.5	Gerenciamento da Disponibilidade	97
5.3.2	Suporte de Serviço.....	98
5.3.2.1	Serviço de Atendimento ao Cliente.....	99
5.3.2.2	Gerenciamento de Incidentes.....	100
5.3.2.3	Gerenciamento de Problemas	100
5.3.2.4	Gerenciamento de Mudanças.....	101
5.3.2.5	Gerenciamento de Versões.....	102
5.3.2.6	Gerenciamento de Configuração.....	102
5.3.2	perspectiva do negócio.....	103
5.3.3	Gerenciamento de Infra-Estrutura de TI - ICT	103
5.3.4	Gerenciamento das Aplicações.....	104
5.3.5	Gerenciamento e Organização.....	105
5.3.6	Planejamento e Implementação	105
5.3.7	Gerenciamento da Segurança.....	106
6	ANÁLISE DO <i>FRAMEWORK</i> COBIT	107
7	ANÁLISE DO <i>FRAMEWORK</i> ITIL.....	110
8	ANÁLISE COMPARATIVA DOS <i>FRAMEWORKS</i> COBIT E ITIL.....	113
9	INTEGRAÇÃO DAS METODOLOGIAS E PADRÕES PARA GOVERNANÇA E/OU GESTÃO DE TI	116
10	INTEGRAÇÃO DOS <i>FRAMEWORKS</i> COBIT E ITIL PARA UM PROCESSO DE IMPLANTAÇÃO DE GOVERNANÇA DE TI.....	120
11	CONCLUSÃO	125
11.1	CONSIDERAÇÕES FINAIS	125
11.2	QUANTO AOS OBJETIVOS ESPECÍFICOS	128
11.2.1	Objetivo Específico I.....	128
11.2.2	Objetivo Específico II.....	128
11.2.3	Objetivo Específico III.....	129
11.2.4	Objetivo Específico IV	130
11.2.5	Objetivo Específico V	131
11.2.6	Objetivo Específico VI	132
11.2.7	Objetivo Específico VII	132
11.3	QUANTO AO OBJETIVO GERAL	133
11.4	QUANTO ÀS PERSPECTIVAS DE CONTINUIDADE	133
11.5	LIMITAÇÕES DA PESQUISA	134
12	REFERÊNCIAS.....	135

Índice de Figuras

FIGURA 2.1 - ESTRUTURA PARA ALINHAMENTO DE ESTRATÉGIAS, PROCESSOS E TI.	16
FIGURA 2.2 - O ALINHAMENTO ESTRATÉGICO COMO PONTO DE PARTIDA PARA SE ALCANÇAR O MÁXIMO POTENCIAL DA TI.	17
FIGURA 2.3 - A CAPTURA DE VALOR NA OBTENÇÃO DE RESULTADOS CONCRETOS DAS INICIATIVAS DE TI.	18
FIGURA 2.4 - MODELO DE ROCKART & MORTON (1984).	18
FIGURA 2.5 - MODELO DE MACDONALD (1991).	19
FIGURA 2.6 - MODELO DE WALTON (1993).	20
FIGURA 2.7 - MODELO DE YETTON, JOHNSTON & CRAIG (1994).	21
FIGURA 2.8 - MODELO DE MCGEE & PRUSAK (1994).	21
FIGURA 2.9 - MODELO ADAPTADO DE CHAIN ET AL. (1997).	22
FIGURA 2.10 – MODELO DE REZENDE & ABREU (2000).	23
FIGURA 2.11 - MODELO DE HENDERSON & VENKATRAMAN (1993).	24
FIGURA 4.1 – GERENCIAMENTO DA INFORMAÇÃO	53
FIGURA 4.2 – ÁREAS FOCO DA GOVERNANÇA DE TI	55
FIGURA 4.3 – INTER-RELACIONAMENTO ENTRE OS COMPONENTES DO COBIT	57
FIGURA 4.4 – PRINCÍPIO BÁSICO DO COBIT	62
FIGURA 4.5 - REPRESENTAÇÃO GRÁFICA DO MODELO DE MATURIDADE	68
FIGURA 4.6 - RELACIONAMENTO ENTRE PROCESSOS, OBJETIVOS E MÉTRICAS.	72
FIGURA 4.7 – GERENCIAMENTO, CONTROLE, ALINHAMENTO E MONITORAMENTO DO COBIT	73
FIGURA 4.8 – O CUBO DO COBIT	74
FIGURA 4.9 – O FRAMEWORK DO MODELO COBIT	75
FIGURA 4.10 – DOMÍNIOS E PROCESSOS DO COBIT.....	79
FIGURA 5.1 – LIVROS DO ITIL.....	86
FIGURA 5.2 – DIAGRAMA DO ITIL.....	88
FIGURA 5.3 – ESTRUTURA DO FRAMEWORK ITIL.....	89
FIGURA 9.1 – RELACIONAMENTO ENTRE OS MODELOS, PADRÕES E SUAS ÁREAS DE ATUAÇÃO	119

Índice de Gráficos e Tabelas

TABELA 2.1 - IMPLICAÇÕES DA SOX PARA TI.....	30
TABELA 3.1 - CICLO DA GOVERNANÇA DE TI.....	34
TABELA 3.2 - OS COMPONENTES DA ETAPA ALINHAMENTO ESTRATÉGICO E COMPLIANCE..	35
TABELA 3.3 - OS COMPONENTES DA ETAPA DECISÃO, COMPROMISSO, PRIORIZAÇÃO E ALOCAÇÃO DE RECURSOS.....	37
TABELA 3.4 - OS COMPONENTES DA ETAPA ESTRUTURA, PROCESSOS, OPERAÇÕES E GESTÃO.....	37
TABELA 3.5 - OS COMPONENTES DA ETAPA DE MEDIÇÃO DO DESEMPENHO DA TI.	37
TABELA 3.6 - ALGUNS MODELOS APLICÁVEIS À GOVERNANÇA DE TI.....	47
TABELA 4.1 - FERRAMENTAS FORNECIDAS PELO COBIT PARA ALINHAMENTO AO NEGÓCIO	62
TABELA 4.2 - DOMÍNIOS DO COBIT	63
TABELA 4.3 - IMPACTOS DO SISTEMA DE CONTROLES INTERNOS DA ORGANIZAÇÃO NA TI .	66
TABELA 4.4 - MODELO GENÉRICO DE MATURIDADE.....	68
TABELA 4.5 - O COBIT E AS ÁREAS FOCO DA GOVERNANÇA DE TI.....	79
TABELA 9.1 - QUADRO COMPARATIVO DE MODELOS E SEUS OBJETIVOS.....	116
TABELA 10.1 - RELACIONAMENTO ENTRE OS LIVROS DO ITIL E OS OBJETIVOS DO COBIT PARA GOVERNANÇA DE TI.....	120
TABELA 10.2 - INTEGRAÇÃO DOS FRAMEWORKS COBIT E ITIL.....	121

Lista de Abreviaturas e Siglas

ABNT – Associação Brasileira de Normas Técnicas

ASL - *Application Services Library*

BS - British Standard

BSC – Balanced Scorecard

CCO – Ciências da Computação

CEO - *Chief Executive Officer*

CFO – *Chief Financial Officer*

CIO – *Chief Information Officer*

CMM: *Capability Maturity Model*

CMMI – *Capability Maturity Model Integration* (Modelo Integrado de Maturidade de Processos)

COBIT – *Control Objectives for Information and Related Technology* (Objetivos de Controle para Informação e Tecnologias Relacionadas)

COO – *Chief Operation Officer*

IEC - *International Electrotechnical Commission*

ISACA – *Information Systems Audit and Control Association*

ISO - *International Organization for Standardization*

IT – *Information Technology*

ITGI - *IT Governance Institute*

ITIL – *Information Technology Infrastructure Library* (Biblioteca de Infra-estrutura para Tecnologia da Informação)

ITSMF - IT Service Management

PMBok – *Project Management Body of Knowledge* (Corpo de Conhecimento de Gerenciamento de Projetos)

PRINCE2 – *Projects in Controlled Environments* (Projetos em ambientes controlados)

SAS70: *Statements on Auditing Standards for Service Organizations*

SOX - *Sarbanes-Oxley Act of 2002*

TI – Tecnologia da Informação

1 INTRODUÇÃO

No cenário atual das organizações, a Tecnologia da Informação (TI) tem, paulatinamente, deixado de ser uma área de suporte. Ela tem exercido cada vez mais papel fundamental para as estratégias de negócio das organizações. Com isso, as exigências quanto à organização e controle da área de TI também aumentaram dentro das empresas.

Visando suportar a estratégia definida e a demanda de serviços de Tecnologia da Informação (TI), as organizações buscam diversas alternativas para melhor planejar e direcionar seus projetos e investimentos em TI.

A administração eficaz dos recursos de TI tornou-se um fator impactante para o desenvolvimento, fortalecimento e sucesso de uma organização no mercado, considerando fatores como:

- o potencial de contribuição para as práticas do negócio, criando novas oportunidades e reduzindo custos;
- a dependência das informações e dos recursos tecnológicos, que pode ser crítica dependendo da natureza do negócio;
- a relação custo x benefício dos investimentos em TI;
- a segurança da informação e dos sistemas de informação.

As operações de TI envolvem altos riscos e demandam grandes investimentos. Alinhar os objetivos da TI ao negócio da empresa e gerenciá-los tornou-se uma tarefa complexa e, sem o auxílio de métodos confiáveis, é difícil garantir o atendimento das necessidades com eficiência, eficácia e cumprimento dos prazos.

Nesse contexto surge a necessidade da implantação da Governança de TI, objetivando o gerenciamento prudente dos recursos, o aprimoramento dos controles internos e a mitigação dos riscos envolvidos.

O processo de implantação da governança de TI em uma organização necessita de investimentos, estruturas e processos que garantam que a TI da

empresa suporte e contribua para os objetivos do negócio. Esse processo aborda, também, a institucionalização de boas práticas e métricas de controle e auditoria, que garantam que os objetivos estabelecidos estejam sendo cumpridos conforme especificado.

Os principais objetivos da Governança de TI são:

- alinhamento e entrega de valor por parte da área de TI para o negócio;
- correta alocação e medição dos recursos envolvidos;
- a mitigação dos riscos em TI;
- medição e avaliação do desempenho;
- alinhamento estratégico.

Para a implantação da governança é necessária a especificação de controles que descrevam os processos e seus responsáveis, os recursos envolvidos e formas de garantir os resultados esperados. Para auxiliar as empresas nesse processo estão disponíveis no mercado diversos modelos ou padrões que contribuem para a Governança em TI, dentre eles: COBIT (*Control Objectives for Information and Related Technology*), ITIL (*Information Technology Infrastructure Library*), CMMI (*Capability Maturity Model Integration*), PMBoK (*Project Management Body of Knowledge*) e padrões de segurança e melhores práticas como a ISO/IEC – 17799, ISO/IEC 20000 e BS 15000. Alguns desses modelos agregam, em estruturas denominadas *frameworks*, um conjunto de melhores práticas testadas com sucesso em várias empresas de grande, médio e pequeno porte, e servem como suporte para a definição dos caminhos a seguir no gerenciamento e no processo de governança de TI.

É proposta neste trabalho uma apresentação da Governança de TI, sua contextualização na governança corporativa, e como alcançá-la fazendo uso dos modelos acima descritos. Pretende-se realizar uma análise específica dos *frameworks* de melhores práticas de controle e gerência de TI, COBIT e ITIL, abordando suas aplicações para o alcance da governança de TI. Pretende-se, ainda, evidenciar casos de aplicação em empresas que tenham implantado as práticas propostas por essas metodologias na busca por melhores resultados.

Outro objetivo deste trabalho é apresentar outros modelos e padrões que facilitem o processo de governança, destacando os objetivos e estratégias de integração destes modelos com o COBIT e ITIL, visando seus escopos de aplicação.

1.1 APRESENTAÇÃO

Este trabalho teve início com uma pesquisa sobre ferramentas para auditoria dos controles no ambiente de TI, ferramentas para implantação da governança de TI e um posterior estudo dos modelos COBIT e ITIL. Observou-se a carência de material em português sobre estes modelos e a necessidade de informações mais detalhadas sobre seus escopos de aplicação. Através desta pesquisa inicial percebeu-se que muitas organizações reconhecem os benefícios que poderiam obter com a aplicação da governança de TI, porém verificou-se que estabelecer os critérios de implantação pode ser problemático.

Tendo sido levantada essa questão, a proposta foi estudar em detalhes o modelo COBIT (visto que ele oferece as ferramentas iniciais para avaliação e verificação da situação de um ambiente de TI) e o modelo ITIL (que oferece as diretrizes de gerenciamento para otimização dos serviços). Percebeu-se, porém, que estas ferramentas não cobririam todas as áreas da implantação de um processo de governança de TI e, como segundo foco, a apresentação de outras ferramentas deveria ser abordada.

1.2 FORMULAÇÃO DO PROBLEMA

Para muitas organizações a Tecnologia de Informação representa um recurso precioso e um fator crítico para o negócio. O setor de TI apresenta-se como um ambiente altamente competitivo e dinâmico. Além de ser requerida uma excelente habilidade gerencial e a redução de custos, é necessário que os controles da área garantam a continuidade dos negócios, suportem a estratégia da empresa e

atendam aos requisitos legais e auditorias. Balancear todas estas questões e colocá-las em prática é um grande desafio para os gestores de TI.

As etapas envolvidas na implantação de um processo de governança são problemáticas e envolvem a definição de controles em diversos níveis. Apenas os controles, contudo, não garantem resultados. É preciso garantir o comprometimento dos envolvidos e, em muitos casos, promover uma mudança na cultura da empresa.

Uma avaliação incorreta das práticas de controle e do impacto que suas aplicações podem causar na organização, pode levar a resultados indesejados, burocracia excessiva e inviabilidade de aplicação prática.

Diante do exposto, o problema que este trabalho busca solucionar reside no estudo e avaliação dos modelos de governança e gerência de TI e de como integrá-los em um processo de implantação da governança. Estudar as práticas através de seus documentos originais é um processo denso, assim, apresentaremos um resumo dos dois modelos mais aceitos (COBIT e ITIL), bem como, uma breve descrição de outros modelos e padrões auxiliares.

1.3 JUSTIFICATIVAS

A administração prudente de TI é um elemento essencial para o sucesso corporativo. A área de TI das empresas sofre grande pressão por resultados tangíveis, sustentáveis e seguros. Pretende-se com este trabalho, reunir informações sobre governança de TI e os modelos de melhores práticas, para apontar caminhos que possibilitem melhorar a tomada de decisão do profissional de TI e facilitar o alinhamento estratégico do negócio.

Embora qualquer modelo de governança de TI possa ser aplicado em uma empresa, ou ainda desenvolvido de acordo com suas necessidades, os padrões mais amplamente aceitos são COBIT e ITIL. Eles são mundialmente reconhecidos como guias das melhores práticas, utilizados para auditoria de sistemas, consultoria de TI e aplicáveis a processos de certificação legal, como a legislação SOX - Sarbanes – Oxley (todas as empresas que negociam ações nos

Estados Unidos precisam estar aderentes a esta legislação, que será oportunamente comentada) e a NBR ISO/IEC – 17799.

Um fator que motivou a escolha do ITIL, é que se trata de uma biblioteca de informações utilizada como auxílio à gerência da infra-estrutura e serviços de TI. A estrutura é composta por diretrizes, independente de qualquer aplicativo ou plataforma e, portanto, pode ser aplicada em qualquer empresa. O COBIT, criado em 1996, tornou-se praticamente padrão para auditores e para adequação à legislação SOX. O motivo de sua escolha foi a independência de plataforma de seus padrões. Há aproximadamente 300 objetivos genéricos no COBIT, agrupados em componentes. Este *framework* consiste de um conjunto de diretrizes, voltado para a mitigação de risco, integridade, confiabilidade e segurança dos processos internos.

Segundo Fagundes (2004), o COBIT é um guia para a gestão de TI recomendado pelo ISACF (*Information Systems Audit and Control Foundation*), que inclui recursos tais como sumário executivo, *framework* de objetivos de controle, guias de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento. As práticas de gestão do COBIT ajudam a otimizar os investimentos de TI e fornecem métricas para avaliação dos resultados.

Ampliar o conhecimento acerca das melhores práticas e esclarecer que a aplicação de controles, documentação e formalização de processos trazem benefícios reais para os administradores de TI, é o fator motivador deste estudo. Objetiva-se mostrar que a governança de TI permite que a empresa utilize suas informações para maximizar benefícios, capitalizar oportunidades e ganhar vantagens competitivas através do alinhamento estratégico.

1.4 OBJETIVOS

Este trabalho baseia-se em um objetivo principal e outros específicos, descritos a seguir.

1.4.1 OBJETIVO GERAL

O principal objetivo desse trabalho é realizar um estudo sobre a governança de TI e a relevância de sua aplicação nas organizações, apresentando uma análise detalhada dos dois modelos mais aceitos no mercado (COBIT e ITIL), aplicáveis em um processo de implantação da governança de TI.

1.4.2 OBJETIVOS ESPECÍFICOS

- i. Apresentar o conceito de governança em TI e a importância dos controles para a otimização dos processos de TI.
- ii. Apresentar detalhadamente a metodologia aplicável para alcance da governança de TI – COBIT.
- iii. Apresentar detalhadamente a metodologia aplicável para alcance da governança de TI – ITIL.
- iv. Apresentar outros modelos e padrões que possam ser integrados ao COBIT e ITIL, buscando cobrir áreas da governança de TI que não estejam contempladas nestes modelos.
- v. Apresentar uma análise comparativa, delimitando o escopo de aplicação dos modelos.
- vi. Citar casos de aplicação dos *frameworks* no mercado, evidenciando sua eficácia.
- vii. Apresentar a integração dos modelos com foco na implantação de um processo de governança de TI.

1.5 DELIMITAÇÃO DO ESCOPO

Pretende-se neste trabalho realizar um estudo teórico da governança de TI e dos modelos COBIT e ITIL, aplicáveis em um processo de implantação da governança. O objetivo é realizar uma análise detalhada de suas características,

similaridades e diferenças, buscando identificar os escopos genéricos de aplicação e um modelo de integração.

Este trabalho não contempla uma aplicação prática da integração proposta ou de um dos modelos isoladamente, o que se pretende é apresentar uma estrutura genérica dos modelos e um quadro de integração que possa ser compreendida e aplicada em empresas de qualquer porte, que busquem implantar governança de TI.

Sabendo-se que apenas COBIT e ITIL não cobrem todos os aspectos de um processo geral de implantação de governança, desenvolvimento de software ou gerência de projeto, por exemplo, pretende-se indicar outros modelos que possam ser utilizados em complemento, tais como: CMMI (*Capability Maturity Model Integrated*), ISO (*International Organization for Standardization*) 17799, 20000 e a família 27000, PMBoK (*Project Management Body of Knowledge*), entre outros. Ressalta-se que não pertence ao escopo deste trabalho um estudo detalhado destes modelos.

A opção pelos modelos COBIT e ITIL deve-se ao fato que essas metodologias vêm se consolidando como padrões de melhores práticas no mercado. Outro fator relevante na escolha foi que estas metodologias são independentes de plataforma, facilmente integráveis a outros padrões e aplicáveis à governança de TI de uma forma geral.

1.6 METODOLOGIA DE DESENVOLVIMENTO

Este trabalho será desenvolvido conforme apresentado nas próximas seções.

1.6.1 A PESQUISA E O MÉTODO

Segundo Leite (1978, p. 15), a pesquisa científica é um processo consciente e racional de aprendizagem destinado a promover a compreensão e explicação de determinados fenômenos de interesse coletivo com a finalidade de interpretação, previsão e controle. O autor defende que "o método científico difere do

método comum por utilizar processos sistemáticos de averiguação, análise e conclusão ao invés do processo aleatório e assistemático das observações, indagações e conclusões leigas".

Esta pesquisa está baseada na revisão bibliográfica. Portanto, pode-se dizer que a técnica de pesquisa utilizada é a **documentação indireta**, já que a documentação direta baseia-se em entrevistas ou questionários.

O método científico é um instrumento formado por um conjunto de procedimentos, mediante os quais os problemas são formulados e as hipóteses são examinadas (GALLIANO, 1979 *apud* PEREIRA et al., 'sem data'). Sabbatini & Cardoso (1998 *apud* PEREIRA et al., 'sem data') afirmam que método científico é um conjunto de abordagens, técnicas e processos utilizado pela Ciência para formular e resolver problemas de aquisição objetiva do conhecimento de uma maneira sistemática. Mas, segundo Galliano (1979 *apud* PEREIRA et al., 'sem data') o método científico não dá receitas infalíveis, não é um receituário nem é milagroso. Nader (1996 *apud* PEREIRA et al., 'sem data') diz que os métodos podem ser considerados como técnicas ou como orientação de pesquisa.

Quanto aos métodos de procedimento, este trabalho utiliza o **método comparativo**. O método comparativo visa explicar semelhanças e dessemelhanças através de observações de duas épocas, ou dois fatos (MEDEIROS, 1997). No caso deste trabalho, é feita a comparação entre duas metodologias para governança em tecnologia da informação, COBIT e ITIL, apontando suas diferenças e semelhanças, e identificando situações em que cada qual se sobressai.

1.6.2 CARACTERIZAÇÃO DA PESQUISA

Ao selecionar um assunto, o estudioso leva em consideração seu gosto pessoal, de valor relevante, teórico ou prático, para o grupo a que pertence (MEDEIROS, 1997). Medeiros diz ainda que "o assunto deverá estar de acordo com a formação intelectual do pesquisador". A introdução deste trabalho tenta explicar a relevância do assunto escolhido.

De modo geral, este trabalho pode ser classificado como uma pesquisa **aplicada**, já que se baseia na aplicação de teoria já elaborada, ou seja, não visa

descobrir teoria. Ele também pode ser considerado uma pesquisa **qualitativa**, pois não tem como interesse medir variáveis. Seu objetivo está relacionado com a compreensão e a interpretação do processo, não sendo necessário o uso da estatística.

Considerando seus objetivos, esta pesquisa é **explicativa**, pois visa registrar e analisar fatos, interpretando-os e identificando suas causas. Quanto à obtenção de dados, o trabalho caracteriza-se como uma pesquisa **bibliográfica**, já que tem como base, principalmente, a leitura e a análise de textos.

1.7 ORGANIZAÇÃO DO TRABALHO

Este item mostra o modo como o trabalho está organizado. Esta introdução apresenta o tema, os motivos que levaram à sua escolha e os objetivos do trabalho. O capítulo 2 traz informações sobre Planejamento e Alinhamento Estratégico, além de abordar a Lei Sarbanes-Oxley. O capítulo 3 trata da Governança de TI. Os capítulos 4 e 5, partes “vitais” deste trabalho, apresentam o COBIT e o ITIL, respectivamente. Nos capítulos 6 e 7, estão contidas as análises individuais dos Frameworks COBIT e ITIL. No capítulo 8 é feita uma análise comparativa desses frameworks. O capítulo 9 traz a integração das metodologias e padrões para governança de TI. O capítulo 10 apresenta a integração dos frameworks COBIT e ITIL para um processo de implantação de governança de TI.

No capítulo 11 estão as conclusões. Por fim, as referências utilizadas na pesquisa encontram-se no capítulo 12.

2 REFERENCIAL TEÓRICO

2.1 PLANEJAMENTO ESTRATÉGICO DOS NEGÓCIOS

Segundo Chiavenato (2003), o planejamento estratégico é a formulação de estratégias organizacionais, onde se busca a inserção da organização e de sua missão no ambiente em que ela está atuando. Oliveira (2001, p.46) conceitua o planejamento estratégico como “um processo gerencial que possibilita ao executivo estabelecer o rumo a ser seguido pela empresa, com vistas a obter um nível de otimização na relação da empresa com o seu ambiente”. Drucker (1997, p.77) define planejamento estratégico como

o processo contínuo de tomar decisões atuais que envolvam riscos, organizar sistematicamente as atividades necessárias à execução dessas decisões e através de um *feedback* organizado e sistemático, medir os resultados dessas decisões em confronto com as expectativas alimentadas.

A atividade de planejar está associada ao destino a ser dado para a organização e ao modo como se pretende atingi-lo. Além disso, é importante definir caminhos alternativos em caso de imprevistos, na tentativa de redirecionar as decisões e suportar os problemas (MONTANA; CHARNOV, 1999).

O planejamento é uma atividade extremamente complexa, composta por uma série de ações, as quais são executadas tendo em vista o alcance dos objetivos e metas definidos pela empresa (OLIVEIRA, 2001). Neste sentido, Stoner e Freeman (1995) colocam que o planejamento estratégico é o “processo de estabelecer os objetivos e as linhas de ação adequadas para alcançá-los”.

Através do planejamento estratégico, segundo Oliveira (2001, p.46), a empresa espera:

- conhecer e melhor utilizar seus pontos fortes;
- conhecer e eliminar ou adequar seus pontos fracos;
- conhecer e usufruir das oportunidades externas;

- conhecer e evitar as ameaças externas;
- obter um efetivo plano de trabalho estabelecendo as premissas básicas, as expectativas e os caminhos desejados pela empresa.

Cobra (1992) coloca que tudo começa com a auto avaliação acerca do negócio da organização, observando-se o ponto em que o negócio está e em qual deveria estar. O estabelecimento dos objetivos a serem alcançados é o ponto de partida do planejamento. Uma vez alcançados os objetivos, estes passam a ser realidade (CHIAVENATO, 1993).

Segundo Oliveira (2001, p.43) a estrutura das organizações subdivide-se em três categorias de decisões que formam o planejamento empresarial. Essas decisões ocorrem em nível estratégico, nível tático e nível operacional. O planejamento estratégico abrange a empresa como um todo, enquanto os planejamentos tático e operacional se preocupam com as metas restritas a determinada área da empresa. Cada tipo de planejamento possui um escopo distinto, porém as decisões definidas são complementares e interdependentes.

Uma das características principais é a preocupação em analisar o ambiente externo e harmonizar as estratégias da empresa com a realidade do mercado.

Resumidamente Oliveira (2001) define que:

- Planejamento estratégico é um processo gerencial de responsabilidade dos níveis mais altos da empresa. Possibilita ao executivo estabelecer o rumo a ser seguido pela empresa, com objetivo de estabelecer um nível de otimização da organização como seu meio ambiente. O planejamento estratégico tem uma visão de longo prazo para a empresa como um todo.
- Planejamento tático, desenvolvido pelas gerências de nível médio, vislumbra um período mais curto do que o planejamento estratégico e trabalha com a decomposição do estratégico, examinando o que é específico de cada área de atuação.

- Planejamento operacional, de responsabilidade das lideranças dos níveis mais baixos de cada área, consiste na definição dos planos de ação de curto prazo: mensais, semanais e diários.

Referente a importância da aplicação do Planejamento Estratégico nas empresas, Oliveira (2001) coloca que o exercício contínuo do planejamento proporciona o desenvolvimento de processos, técnicas e atitudes administrativas que tendem a reduzir a incerteza envolvida no processo decisório.

[...] os gestores deveriam entender que é primordial as empresas obterem um planejamento estratégico estruturado, pois só assim poderiam delinear um futuro esperado para suas empresas e maneiras de alcançar ou se aproximar o mais possível desse futuro desejado. Inclusive, se uma maneira não deu certo, o gestor sabe como direcionar para outra opção no momento certo e de forma adequada". (OLIVEIRA, 2001)

O objetivo do Planejamento Estratégico é prover direção, concentração de esforço, constância de propósito, e flexibilidade, como um negócio continuamente empenhado em impor sua posição em todas as áreas estratégicas (BOAR, 1994).

Na literatura estão disponíveis diversos modelos para desenvolvimento de um Planejamento Estratégico, cada empresa necessita avaliar o que melhor se enquadra a sua realidade. Além dos fatores internos, é preciso considerar as condições externas que rodeiam a empresa e que lhe impõem desafios e oportunidades, como explica Chiavenato (1993).

2.2 PLANEJAMENTO ESTRATÉGICO DE TI

A combinação dos objetivos estratégicos e a seleção de capacidades de negócio utilizadas para atingir os objetivos é o que constitui a estratégia da empresa. As empresas, de modo geral, procuram desenvolver um conjunto de capacidades de negócio para atingir seus objetivos estratégicos. Estes, suportados por investimentos necessários nas capacidades de TI, podem levar a empresa ao sucesso em seus negócios. (MARCHAND; KETTINGER; ROLLINS, 2001 *apud* GARCIA, 2005).

Marchand; Kettinger; Rollins (2001 *apud* GARCIA, 2005) classificam os objetivos estratégicos em quatro categorias de prioridades estratégicas: criação de

novas oportunidades de negócios, encantar os clientes, minimizar riscos e reduzir custos. Eles também identificaram cinco capacidades chave dos negócios: estrutura organizacional, processos, pessoas, relacionamento externo e capacidades de informação. As capacidades de informação são: importância e utilização da informação, práticas de gerenciamento da informação e práticas de TI. Para eles o gerenciamento efetivo de cada uma das três capacidades de informação, maximiza os resultados obtidos através da TI, contribuindo significativamente para a melhoria da performance dos negócios.

O Planejamento Estratégico da Tecnologia da Informação (PETI) é um processo dinâmico e interativo que visa estruturar estratégica, tática e operacionalmente as informações organizacionais, a TI, os sistemas de informação (estratégicos, gerenciais e operacionais), as pessoas envolvidas e a infra-estrutura necessária para o atendimento de todas as decisões, ações e respectivos processos da organização (PREMKUMAR; KING, 1992; BOAR, 1993; TURBAN; MCLEAN; WETHERBE, 1996; STAIR, 1996; KEARNS; LEDERER, 1997; REZENDE; ABREU, 2000 *apud* REZENDE; ABREU, 2001).

Mañas (1999 *apud* GARCIA, 2005) afirma que o PETI, para ser totalmente eficaz, deve ser coerente com o Plano Estratégico da empresa. Segundo Fernandes; Abreu (2006), no processo de PETI a TI participa na definição dos objetivos e estratégias da empresa, sugerindo novas oportunidades de negócio com o uso da TI ou apoiando os demais objetivos e estratégias. Para os autores, o PETI não deve servir apenas para eliminar um ponto da auditoria, e sim ser um elemento de apoio à gestão do CIO e dos demais gerentes, em toda a operação.

Analogamente, Spohr; Sauv  (2003) afirmam que o processo de Planejamento Estrat gico de TI procura avaliar as necessidades da empresa baseando-se no conhecimento de sua estrutura de TI e sugerindo op es para a melhor estrat gia de seus neg cios com o uso, reestrutura o, aquisi o, implanta o, ou melhoria dos processos de TI.

Para Amaral; Varaj o (2000 *apud* GARCIA, 2005), o processo de PETI tem sofrido diversas evolu es quanto  s suas finalidades e   sua inser o na atividade organizacional. Segundo os autores, o processo de PETI   visto como um

processo dedicado à construção de diversas arquiteturas que permitam suportar a estratégia organizacional. O principal foco de atenção é o desenho das arquiteturas, especialmente a da Informação, procurando simultaneamente um melhor alinhamento entre os requisitos da organização e a aplicação da TI, a integração dos sistemas existentes e a identificação e priorização dos projetos de desenvolvimento.

O processo de PETI, segundo Boar (2002), é composto pelas seguintes etapas:

- Avaliação - é a atividade de desenvolver um conhecimento claro e profundo da situação do negócio. Culmina na identificação de conclusões que localizam os aspectos que exigem uma atenção estratégica. Duas etapas principais são usadas para gerar as conclusões: posicionamento e análise da situação. A etapa de posicionamento oferece um modo gráfico de entender a posição ou o estado da tecnologia da informação em todas as áreas estratégicas relevantes. A etapa de análise da situação usa vários métodos analíticos para interpretar os dados sobre a organização e seu ambiente.
- Estratégia - consiste em identificar os objetivos específicos a serem alcançados e as mudanças estratégicas necessárias para se perceber os futuros estados e objetivos. Para dar suporte à realização dos objetivos, também são desenvolvidos um plano de comprometimento, para focalizar a tensão da organização aos objetivos e um plano de gerenciamento de mudança, para antecipar e reduzir a resistência às mudanças.
- Execução - coloca o plano em movimento. Transforma a intenção em realidade. As estratégias tornam-se operacionais por meio de programas de implementação que são particionados em vários projetos. Uma etapa de monitoração e controle do processo é usada para ajustar e sintonizar os projetos, oferecer *feedback* de aprendizado a partir das experiências do projeto, observar o ambiente quanto a situações adicionais que exijam resposta estratégica.

Pode-se dizer que o planejamento estará completo quando estiver formado o *Portfólio* de TI Aprovado, ou seja, quando estiverem decididas as prioridades de investimentos e manutenção de itens de custeio. O *Portfólio* Aprovado deverá ser executado e guiará a organização de TI (FERNANDES; ABREU, 2006).

2.3 ALINHAMENTO ESTRATÉGICO DA TI

Segundo Fernandes e Abreu (2006), alinhamento estratégico é a transformação da estratégia do negócio em estratégias e ações de TI que garantam o apoio dos objetivos de negócio. Para Pinho (2005), alinhamento estratégico de TI sintetiza o propósito de tornar a Tecnologia da Informação um fator crítico na modelagem da estratégia organizacional. Segundo o autor existe a abordagem de conceitos, estratégias, políticas públicas e tecnologias, para demonstrar que a TI se configura como um forte instrumento para consolidar e viabilizar os objetivos institucionais das esferas públicas, bem como as vantagens competitivas das empresas modernas.

De acordo com Boar (2002), a organização da TI existe a fim de haver competitividade para o restante da empresa. A direção precisa estar alinhada com as necessidades e os requisitos da empresa maior.

Como explanam Fernandes e Abreu (2006), o mercado de cada empresa define a estrutura do negócio, criando elementos competitivos. Esses elementos têm impacto na forma como a empresa descobre novas oportunidades de negócio, desenvolve produtos e serviços, realiza as suas vendas e aquisições de insumos e recursos e, também, como ela os transforma em produtos e serviços, e assim sucessivamente.

Além de definir a estrutura do negócio, o mercado também fornece informações sobre possíveis ameaças a ele (o negócio). Assim, como afirmam Fernandes e Abreu (2006), as linhas de produtos e serviços da empresa podem pedir o uso simultâneo de várias estratégias, que, por sua vez, podem requerer processos de negócio distintos, do ponto de vista operacional e da gestão. Isso

constitui um impacto significativo na definição da arquitetura e da infra-estrutura de TI, visando obter o máximo de compartilhamento de recursos.

A figura 2.1 mostra uma estrutura para alinhamento de estratégias, processos e TI, apresentada por Spohr & Sauv  (2003).

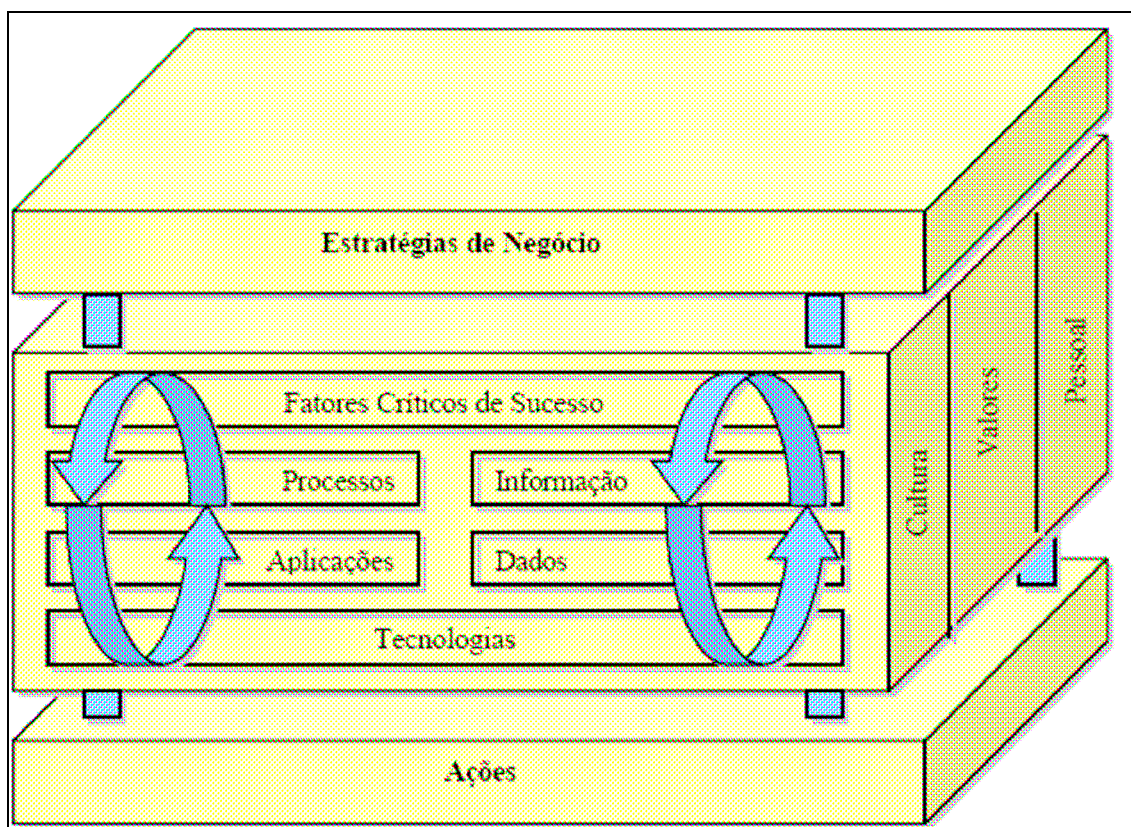


Figura 2.1 - Estrutura para alinhamento de estrat gias, processos e TI (SPOHR; SAUV , 2003).

Segundo Ramirez; Sender (2003), o objetivo do alinhamento de TI   extrair o m ximo da estrat gia e da arquitetura de TI. Os riscos da m  aplica o da TI devem ser reduzidos ou eliminados. Projetos de TI abortados antes do seu t rmino e iniciativas implementadas e nunca utilizadas tamb m s o fatores de risco. Entretanto, o principal risco do n o alinhamento   o alto n vel de insatisfa o entre os diretores corporativos e superintendentes de neg cios, com servi os e produtos de TI.

O alinhamento da estratégia de TI com a estratégia da empresa, continuam os autores, é o ponto de partida para se alcançar o máximo potencial dessa área, como mostra a figura 2.2.



Figura 2.2 - O alinhamento estratégico como ponto de partida para se alcançar o máximo potencial da TI (SPOHR; SAUVÉ, 2003).

Para Ramirez; Sender (2003), o alinhamento de TI à estratégia permite uma ação pró-ativa com a direção da área de TI, na identificação de oportunidades nessa área, como mostra a figura 2.3. Essas oportunidades podem ser provenientes de mudanças no mercado, na regulamentação e da propriedade. Outros fatores externos também podem gerar a necessidade de rever a estratégia de TI.

Atualmente, o alinhamento estratégico é bidirecional, ou seja, da estratégia do negócio para a estratégia de TI e vice-versa, pois a TI pode potencializar estratégias de negócio que seriam impossíveis de serem implantadas sem o auxílio da tecnologia da informação. (FERNANDES; ABREU, 2006, p.35)

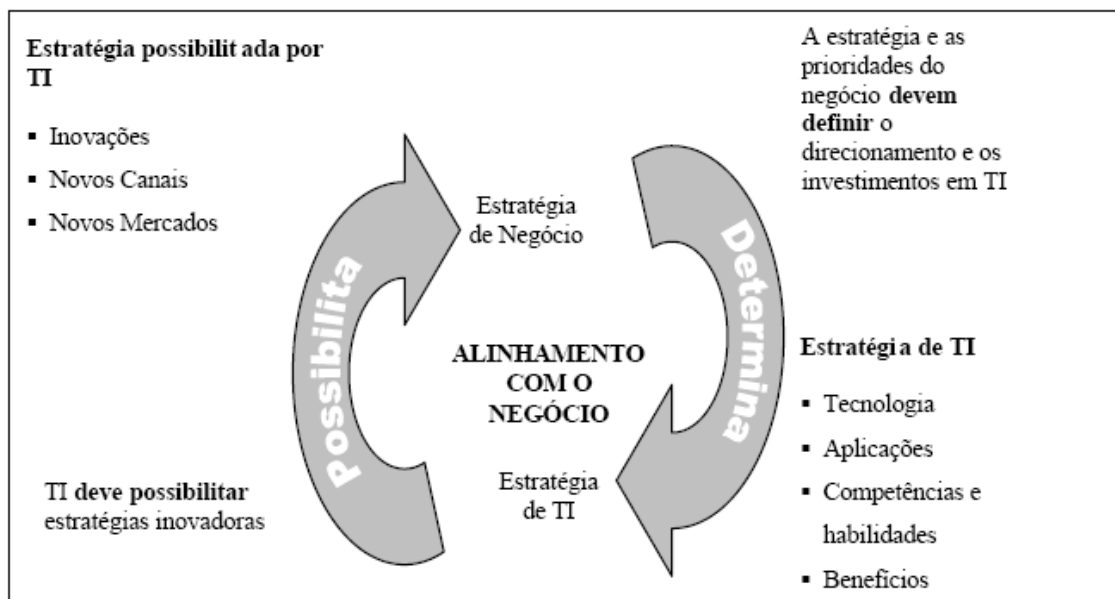


Figura 2.3 - A captura de valor na obtenção de resultados concretos das iniciativas de TI (RAMIREZ; SENDER, 2003).

A seguir, da figura 2.4 à figura 2.11, estão apresentados os esquemas de alguns modelos de alinhamento estratégico de TI, apresentados por Rezende (2002).

□ Modelo de Rockart & Morton (1984)

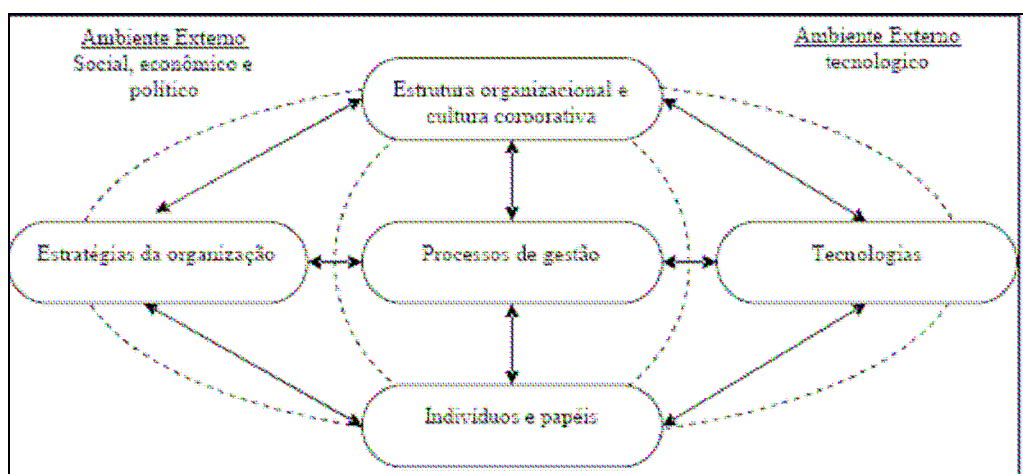


Figura 2.4 - Modelo de Rockart & Morton (1984) (REZENDE, 2002).

O modelo de Rockart e Morton é baseado em cinco elementos do funcionamento corporativo: estratégias da organização, tecnologias, estrutura organizacional e cultura corporativa, processos de gestão (planejamento, orçamentos e recompensas), e indivíduos e papéis. Esses cinco elementos são circundados pela fronteira da organização, em forma de diamante. Nesse modelo está implícita a adequação tecnológica, objetivando o alinhamento dos negócios da organização por meio da TI. O esquema da TI para contribuir nesse modelo e beneficiar a organização, é formado por computadores, tecnologia de comunicações, estações de trabalho, robótica e codificação inteligente em chips (MORTON, 1988 *apud* RAMIREZ, 2007).

□ Modelo de MacDonal (1991)

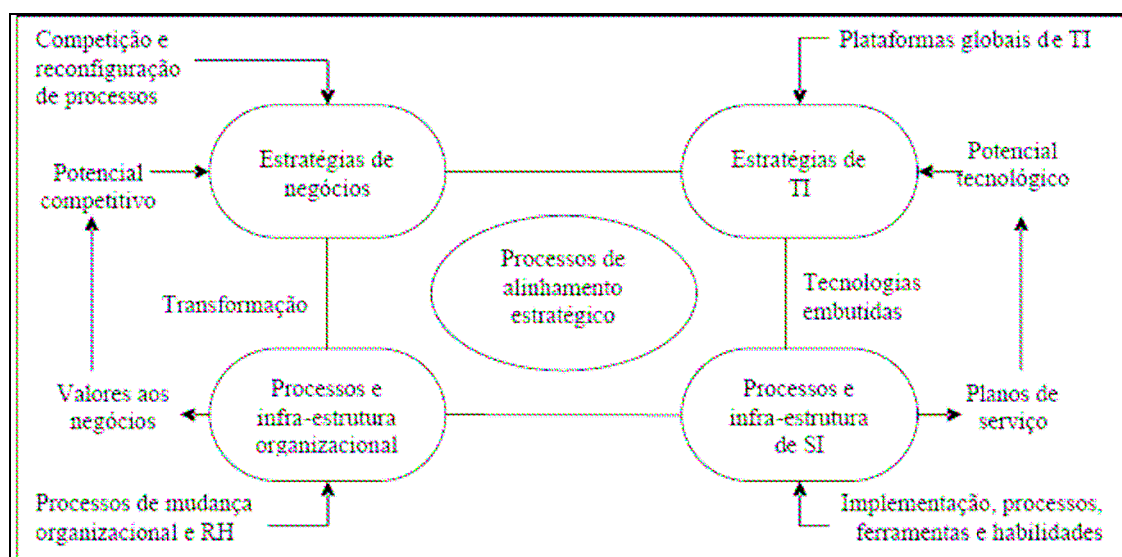


Figura 2.5 - Modelo de Macdonald (1991) (REZENDE, 2002).

O modelo de Macdonald (1991) transforma o modelo teórico de alinhamento estratégico de Rockart e Morton (1984) com o objetivo de explorar resultados organizacionais. O processo estabelece o co-alinhamento transversal da estratégia de negócios com os processos e infra-estrutura de SI, da estratégia de TI com a organização e gestão dos processos e infra-estrutura organizacional, e entre esses dois eixos. O co-alinhamento acontece a partir das considerações das operações internas e externas à organização, das relações entre competidores, das necessidades dos consumidores, das oportunidades dos fornecedores, das

tendências do segmento do negócio, entre outras operações (VENKATRAMAN, 1989 *apud* RAMIREZ, 2007).

□ **Modelo de Walton (1993)**

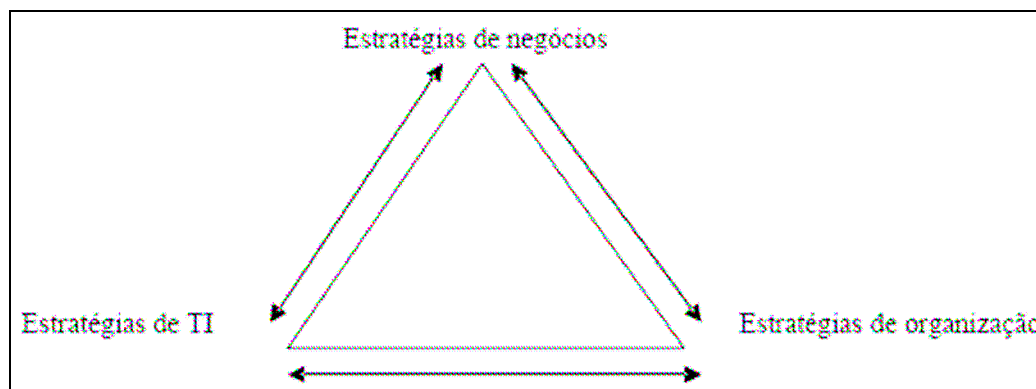


Figura 2.6 - Modelo de Walton (1993) (REZENDE, 2002).

A proposta de Walton (1993) para o alinhamento do PETI ao PEE é o triângulo estratégico. Esse triângulo visa a criação da visão estratégica como uma ampla concepção dos aspectos-chave para a organização no futuro. Essa visão deve abranger a estratégia competitiva (PORTER, 1990 *apud* RAMIREZ, 2007) e os modelos organizacionais que poderão direcionar ou serem direcionados pelos sistemas de TI, que devem abranger os três ângulos do triângulo. As empresas orientadas para o comprometimento mercadológico devem estar fundamentadas na capacitação tecnológica (ZUBOFF, 1988 *apud* RAMIREZ, 2007) e na estratégia de organização (CHANDLER, 1962 *apud* WALTON, 1993 *apud* RAMIREZ, 2007) onde a estrutura organizacional, os SI e as habilidades pessoais podem contribuir ou restringir o alinhamento estratégico de negócios (MILES; SNOW, 1978 *apud* RAMIREZ, 2007).

□ **Modelo de Yetton, Johnston & Craig (1994)**

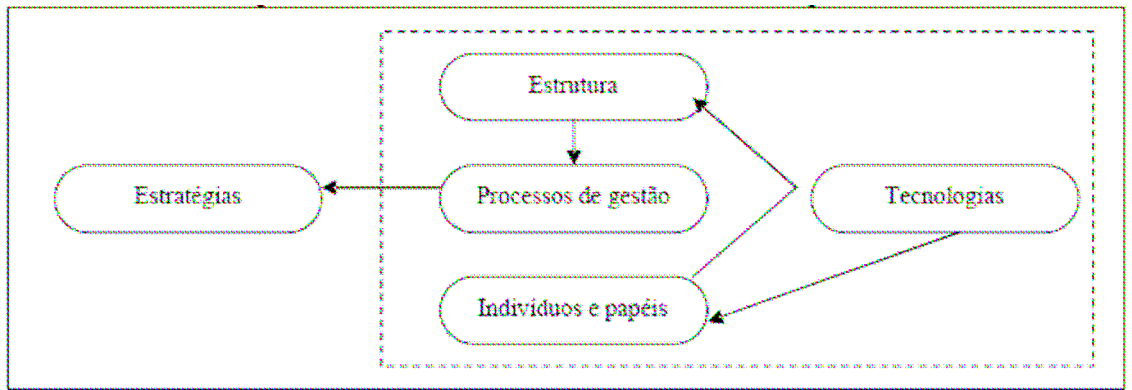


Figura 2.7 - Modelo de Yetton, Johnston & Craig (1994) (REZENDE, 2002).

O modelo de Yetton, Johnston e Craig (1994) é uma adaptação do modelo de Rockart e Morton (1984) a partir da análise dos resultados obtidos num estudo de caso em uma empresa australiana, que mostra a TI como impulsionadora da mudança e alinhamento estratégico por meio da alteração das responsabilidades dos papéis e habilidades individuais, de processos de gestão, da estrutura organizacional e das estratégias do negócio. Esse caminho de alinhamento dinâmico é mais precisamente representado com a intervenção do nível de tecnologia, seguido da transformação dos papéis e das habilidades individuais, da mudança na estrutura e, subsequente, alinhamento e integração nos processos de gestão (REZENDE, 2002).

□ Modelo de McGee & Prusak (1994)

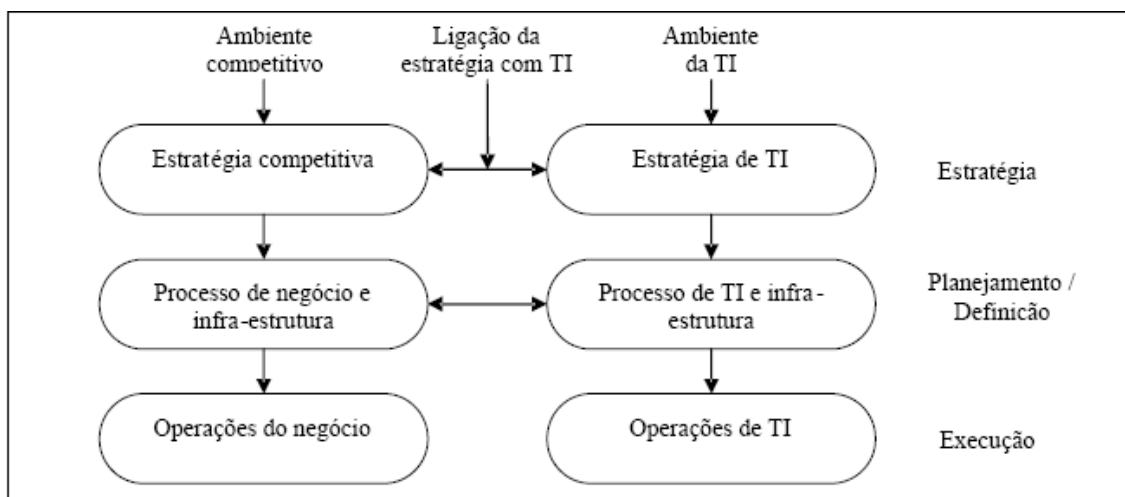


Figura 2.8 - Modelo de McGee & Prusak (1994) (REZENDE, 2002).

As variáveis informação e TI devem ser consideradas relevantes e críticas potenciais dentro do processo de definição de estratégias. No modelo de alinhamento estratégico de Mcgee e Prusak (1994) as alternativas de negócio são definidas em paralelo com as alternativas de TI, mantendo um fluxo contínuo de interação e troca de informações. O alinhamento das estratégias de negócios e as de TI procura evidenciar as potencialidades da TI, considerando-a como um recurso a ser observado durante o processo de definição ou de redesenho de estratégias (EVANS; WURSTER, 1997 *apud* REZENDE, 2002).

□ **Modelo de Chan, Huff, Barclay e Copeland (1997)**

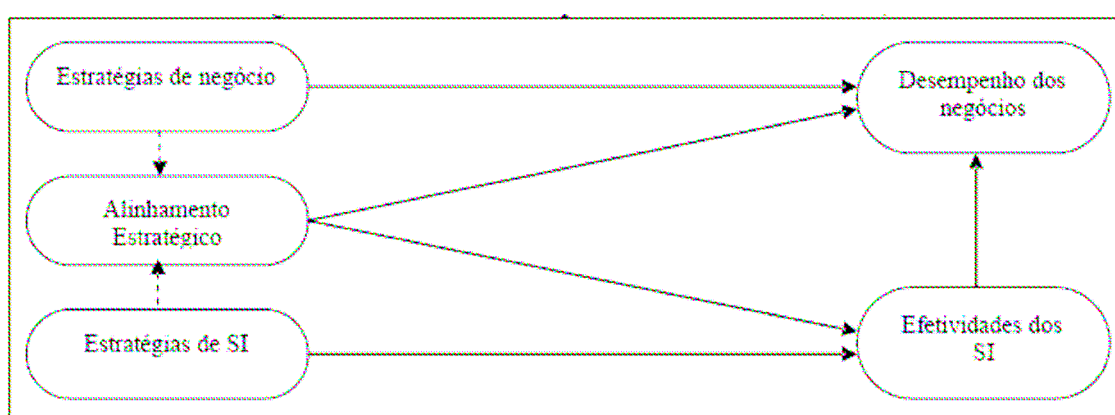


Figura 2.9 - Modelo adaptado de Chan et al. (1997) (REZENDE, 2002).

O modelo de Chan, Huff, Barclay e Copeland é voltado para a obtenção de resultados. Nesse modelo as estratégias de negócios e de SI são alinhadas para proporcionar a efetividade dos SI, gerando o desempenho dos negócios organizacionais. Esse modelo é uma extensão dos trabalhos de outros pesquisadores precursores (COPELAND; MCKENNEY, 1988; HENDERSON; VENKATRAMAN, 1993; LUFTMAN; LEWIS; OLDACH, 1993; CHAN; HUFF, 1993 *apud* RAMIREZ, 2007).

□ **Modelo de Rezende e Abreu (2000)**

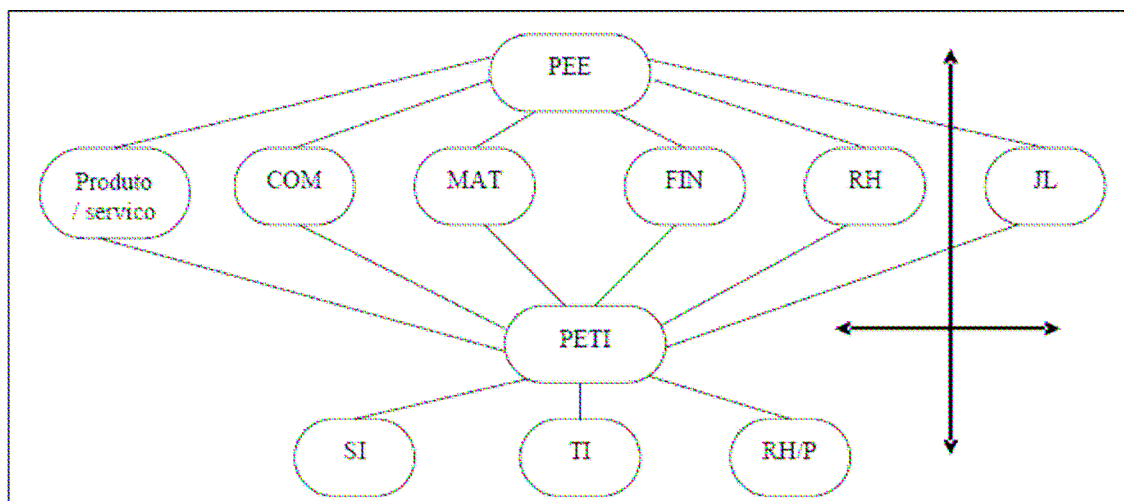


Figura 2.10 – Modelo de Rezende & Abreu (2000) (REZENDE, 2002).

A integração dos negócios ou funções empresariais estratégicas com a TI abrange outras variáveis no modelo de alinhamento de Rezende e Abreu (2000). Nesse modelo, o alinhamento acontece pela coerência vertical e horizontal (representada pela cruz) entre o PEE e o PETI, onde o PEE está integrado ao planejamento estratégico dos negócios ou das funções empresariais e aos respectivos planos dos Sistemas de Informação, Tecnologia da Informação e Recursos Humanos ou Pessoas (RH/P). Nesse modelo de alinhamento os objetivos do PEE com o uso da TI são: investigar as oportunidades de ganho e as vantagens competitivas por meio do melhor uso de tecnologias, estabelecer objetivos e fatores críticos de sucesso para a empresa, facilitar a consecução dos objetivos empresariais mediante a análise de seus fatores críticos de sucesso, determinar quais informações podem auxiliar a gestão na melhor realização do seu trabalho, priorizar o uso da TI em função das necessidades da empresa, criar um modelo funcional e de dados do negócio, de modo que permita à alta administração visualizar o negócio em termos dos objetivos, funções, informações, fatores críticos de sucesso e estrutura organizacional (REZENDE, 2002).

□ **Modelo de Henderson & Venkatraman (1993)**

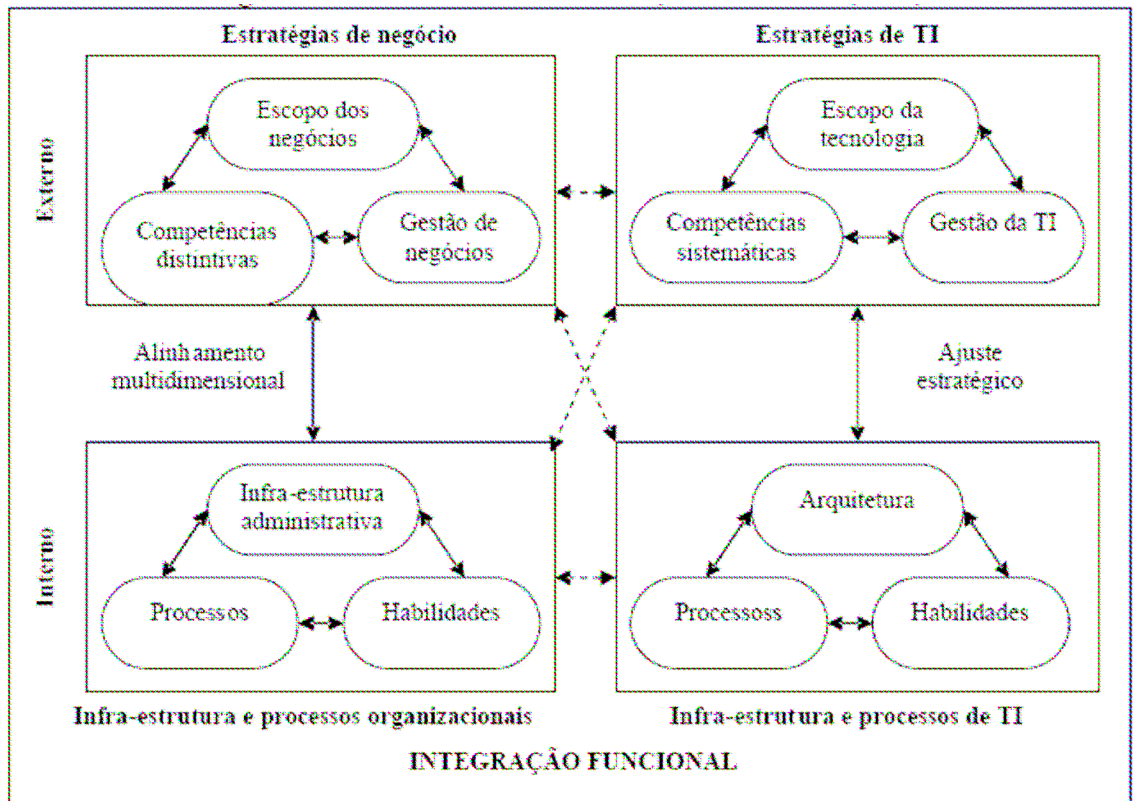


Figura 2.11 - Modelo de Henderson & Venkatraman (1993) (REZENDE, 2002).

O modelo proposto por Henderson & Venkatraman (1993), como comentam Fernandes; Abreu (2006), mostra que a estratégia de TI influencia e é influenciada pela estratégia de negócio, interagindo bidirecionalmente com a infraestrutura e os processos organizacionais e de TI.

O alinhamento estratégico ocorre em vários momentos na vida da empresa. Um momento é quando o "board" da organização se reúne para definir objetivos de negócio de médio e longo prazo e estabelece estratégias para atingir esses objetivos. [...]

Outros momentos acontecem quando este mesmo "board" redefine aleatoriamente o seu plano de negócios em função de novas oportunidades ou cenários macroeconômicos e microeconômicos de negócios.

Por fim, esse alinhamento ocorre no dia-a-dia, quando os clientes de TI demandam soluções novas que mudam os requisitos do negócio estabelecidos no alinhamento estático, quando foi feito o plano de tecnologia. Neste caso a TI tem que ser bastante flexível. (FERNANDES; ABREU, 2006, p.37)

2.3.1 ALINHAMENTO ESTÁTICO E ALINHAMENTO DINÂMICO

Alinhamento estático é a derivação da estratégia de TI a partir do Plano Estratégico da empresa. Já o alinhamento dinâmico, é a alteração da estratégia de TI em função da mudança aleatória da estratégia de negócios da empresa. Para ser efetivo e robusto, um modelo de Governança de TI deve contemplar esses dois alinhamentos (FERANDES; ABREU, 2006).

Como acreditam os autores, inicialmente, o Plano de Tecnologia provém do alinhamento estático. Durante a implantação das estratégias de negócio, ocorrem mudanças no cenário do mercado, da economia ou da política, fazendo com que as estratégias originais sofram modificações. As novas estratégias precisarão de um novo alinhamento da TI, o alinhamento dinâmico.

2.3.2 ANÁLISE DE ALINHAMENTO

Segundo Boar (2002), a situação ideal de planejamento estratégico exige simultaneidade e entrelaçamento entre as atividades de planejamento estratégico da empresa e da organização de TI. Assim, o planejamento de TI deve acontecer em paralelo com o planejamento da empresa, que precisa da participação ativa do CIO. De acordo com o autor, nessa situação, o grau de colaboração, coordenação, comunicação e alinhamento é maximizado, mas, geralmente, falta uma estratégia formal da empresa para oferecer as diretrizes e hipóteses necessárias. Esse problema pode ser minimizado através de uma análise de alinhamento. Como coloca Boar (2002), a análise de alinhamento, envolve quatro conceitos:

- Impulsionadores da empresa – Forças externas à empresa, que precisa responder criativa e agressivamente a elas. Exemplos: regulamentação, globalização, advento de novos canais de distribuição.
- Impulsionadores da tecnologia – Forças do setor de TI, que precisam ser respondidas criativa e agressivamente pelas organizações de TI. Exemplos: Internet, terceirização seletiva, padrões de tecnologia.

- Principais iniciativas da empresa – Classes de respostas para os impulsionadores da empresa. Exemplos: oferecer cuidado inicial com o cliente, simplificar os processos comerciais, atender a um cliente global.
- Requisitos de TI – Impacto das iniciativas da empresa ou dos impulsionadores da tecnologia na organização de TI. Exemplos: oferecer uma visão única do cliente, atualizar o treinamento da força de trabalho, equilibrar a criação e a compra de novos sistemas de *software*.

De acordo com a conclusão de Boar (2002), a lógica do alinhamento é a seguinte: devido aos impulsionadores da empresa, é necessário que ela tome iniciativas de negócios importantes. Para executá-las, alguns requisitos de TI precisam ser atendidos, possibilitando também a reação criativa aos impulsionadores da tecnologia, que criam oportunidades nessa área para a organização e/ou tornam obsoletos os investimentos existentes.

2.4 A LEI SARBANES – OXLEY

Em 2001, grandes empresas, como Enron, Tyco, Worldcom e MCI, envolveram-se em escândalos corporativos. Esses escândalos tiveram graves impactos financeiros, impactando a confiança dos investidores e, coseqüentemente, derrubando os preços das ações no mundo todo, principalmente nos Estados Unidos. Como medida preventiva para tais irregularidades, o congresso estadunidense decretou o Ato Sarbanes-Oxley (SOX) em agosto de 2002.

Para Mendes (2006), o SOX representou a maior reforma sobre a regulamentação das empresas depois do New Deal, nome dado a um conjunto de medidas elaboradas nos anos 30 para tentar sanar a situação financeira dos Estados Unidos após a quebra da bolsa em 1929.

O SOX está relacionado com a forma como as empresas de capital aberto relatam suas finanças. De acordo com Ramos (2004 *apud* FERNANDES, ABREU, 2006, p. 22): O termo 'controle interno sobre relatórios financeiros' é definido como o processo projetado por, ou sob a supervisão do principal executivo e do principal responsável por finanças do emitente, ou pessoas que desempenham funções similares, efetivado pelo comitê de diretores do emitente, pela gerência ou outras pessoas, para prover garantia razoável relacionada à confiabilidade de emissão de relatórios financeiros e a preparação de relatórios de resultados financeiros para propósitos externos, de acordo com princípios de contabilidade geralmente aceitos.

Tais controles incluem políticas e procedimentos para:

- Manter registros que, em razoável detalhe, com exatidão e de forma correta, reflitam as transações e disposições dos ativos do emitente;
- prover garantia de que as transações sejam registradas quando necessário para permitir a preparação de declarações de resultados financeiros de acordo com os princípios contábeis geralmente aceitos, e que as receitas e despesas do emitente sejam feitas somente de acordo com autorizações da gerência e diretores do emitente;
- prover garantia relacionada à prevenção ou detecção, no momento preciso, de aquisições não autorizadas, uso ou disposição dos ativos do emitente que possam ter um efeito material nas declarações dos resultados financeiros”.

A conformidade Sarbanes-Oxley requer documentação e estabelecimento de controles financeiros e avaliação da infra-estrutura. Os onze títulos que compõem a SOX são:

- Título I: *Public Company Accounting Oversight Board* – ONG responsável por registrar as auditorias e estabelecer os padrões relativos aos controles financeiros das empresas abertas;
- Título II: *Auditor Independence* – auditores independentes e rotatividade entre empresas de auditoria;
- Título III: *Corporate Responsibility* – responsabilidades corporativas;

- Título IV: *Enhanced Financial Disclosures* – novas regras para a elaboração e publicação de resultados financeiros;
- Título V: *Analyst Conflicts of Interest* – regras preventivas contra conflitos de interesse entre analistas de corretoras de valores ou de administração de fundos;
- Título VI: *Commission Resources and Authority* – regras para a autorização de fundos para a *Stock Exchange Commission* (SEC), e autoridade da SEC para suspender empresas e auditores;
- Título VII: *Studies and Reports* – autoridade da SEC para realizar estudos e relatórios;
- Título VIII: *Corporate and Criminal Fraud Accountability* – regras e penalidades para a destruição de registros corporativos, alteração de dados e falsificações;
- Título IX: *White-Collar Crime Penalty Enhancements* – penalidades para crimes de colarinho branco;
- Título X: *Corporate Tax Returns* – o CEO (*Chief Executive Officer*) é obrigado a assinar o imposto de renda de pessoa jurídica;
- Título XI: *Corporate Fraud Accountability* – responsabilidade corporativa através da comunicação de informações financeiras de resultados fraudulentos.

Em relação à TI, segundo Charley Luz (2006), as seguintes adequações são necessárias à lei: proteções técnicas apropriadas que obriguem a organização ao cumprimento de políticas e controles (*workflows*); proteção da integridade do ambiente de informação, armazenamento e retenção de dados; facilitar a demonstração de controles que possam aumentar a integridade e auditoria dos processos de TI e sistemas (registro do processo de produção de TI - gerenciamento de projetos); reforçar o bloqueio de acesso de perfis não autorizados aos sistemas financeiros e negócios (segurança da informação).

As seções 302 e 404 da SOX estão diretamente relacionadas à TI. Suas implicações estão descritas a seguir.

2.4.1 IMPLICAÇÕES DA SOX QUANTO À GOVERNANÇA DE TI

As seções 302 e 404 da SOX especificam controles que envolvem impacto (direta ou indiretamente) relacionado à área de TI. Segundo Fernandes e Abreu (2006), a seção 302 especifica que:

- o CEO e o CFO devem revisar os relatórios financeiros;
- os relatórios não contêm nenhuma declaração falsa de um fato material ou omissão;
- outras informações financeiras incluídas representam corretamente a condição financeira, resultados de operações e fluxos de caixa nos períodos representados pelos relatórios;
- o CEO e o CFO são responsáveis por manter e estabelecer controles e procedimentos sobre a emissão de relatórios financeiros e controles internos sobre tais relatórios;
- os sistemas de controle interno sobre a emissão de relatórios financeiros devem ser projetados sob a supervisão do CEO e do CFO, incluindo as subsidiárias;
- os sistemas de controle interno sobre relatórios financeiros também devem ser projetados sob a supervisão do CEO e do CFO;
- deve ser avaliada a efetividade do sistema de controle sobre a emissão de relatórios financeiros;
- devem ser comunicadas mudanças nos controles internos sobre relatórios financeiros, considerando o último ano fiscal;
- devem ser comunicadas as deficiências dos sistemas de controle interno que possam afetar a habilidade da empresa em registrar, processar, sumarizar e comunicar informações financeiras;
- deve ser comunicada qualquer fraude que envolva a gerência ou outros empregados que tenham um papel significativo nos registros do controle interno sobre relatórios financeiros.

A seção 404 especifica que:

- a administração tem a responsabilidade de estabelecer e manter uma estrutura adequada de controle interno e procedimentos para relatórios financeiros;
- a administração deve avaliar a efetividade do sistema de controle interno sobre relatórios financeiros;
- deve ser realizada uma auditoria externa específica sobre a avaliação interna da efetividade do sistema de controle interno feita pela administração.

De acordo com Fernandes e Abreu (2006), num sistema de controle interno, os riscos são identificados e mitigados, os controles são estabelecidos e executados, os registros e sistemas de controle são desenvolvidos e mantidos e toda a sistemática é monitorada. Os autores afirmam ainda, que a Tecnologia da Informação é uma fonte de risco para a continuidade do negócio e para o atendimento ao Ato Sarbanes-Oxley.

A Tabela 2.1 apresenta algumas implicações da SOX em relação à TI, como apresentado em Fernandes; Abreu (2006, p. 27).

Tabela 2.1 - Implicações da SOX para TI

Requisitos de qualidade da informação	Implicações do SOX
O conteúdo da informação deve ser apropriado.	<p>Processo de desenvolvimento de requisitos de software;</p> <p>Processo de gerenciamento de requisitos de software;</p> <p>Métodos de engenharia de software;</p> <p>Processos de verificação (teste);</p> <p>Processos de validação (aceitação pelos usuários);</p> <p>Processos de segurança da informação empregados nos aplicativos;</p> <p>Processos de aceitação de produtos de terceiros;</p>

	Processo de gestão da mudança e da configuração.
A informação deve estar disponível no momento em que for necessária.	Disponibilidade de aplicativos; Disponibilidade de infra-estrutura; Gerenciamento de incidentes e problemas no ambiente de produção; Suporte aos usuários; Gestão de aplicativos e de ativos de TI; Processos de gerenciamento da infra-estrutura; Segurança da infra-estrutura; Gerenciamento da contingência; Gerenciamento de disponibilidade e desempenho.
A informação é atual ou pelo menos é a última disponível.	Processos de gerenciamento de dados; Planejamento e gerenciamento da contingência e de desastres; Segurança da informação na infra-estrutura.
Os dados e as informações estão corretas.	Segurança da informação em aplicativos; Segurança da infra-estrutura de TI; Teste de software; Controle da mudança e da configuração; Gerenciamento de dados; Gerenciamento de requisitos.
A informação é acessível aos usuários interessados.	Segurança da informação referente a controle de acessos e privilégios; Controle de autorizações.
Há um sistema de controle interno sobre relatórios financeiros.	Avaliação de riscos de TI; Gestão de qualidade; Planos de desastres e recuperação;

Fonte: FERNANDES; ABREU (2006, p. 27)

Resumidamente, a criação de novas aplicações e funcionalidades, melhoria dos processos de TI para mitigar riscos, criação de novos processos de TI, desenvolvimento de novos indicadores de desempenho e monitoração constante dos riscos de TI, são alguns dos impactos do Ato Sarbanes-Oxley na governança de TI.

Os requisitos do Ato Sarbanes-Oxley de 2002 não diminuem com base no tamanho ou receita de uma empresa. Empresas com departamento de TI de tamanho pequeno a médio enfrentarão desafios únicos, tanto orçamentários quanto com pessoal, em seus esforços para corresponder ao Ato Sarbanes-Oxley.(Lahti, Peterson, 2006 p.26).

3 GOVERNANÇA EM TECNOLOGIA DE INFORMAÇÃO

3.1 INTRODUÇÃO

Segundo o dicionário da língua portuguesa Aurélio (1999), governança é o ato de governar(-se). A governança de TI provém da governança corporativa, que passou a ter destaque depois dos escândalos financeiros de diversas empresas, em meados de 2002.

Governança corporativa é o sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade (Instituto Brasileiro de Governança Corporativa – IBCG).

A governança corporativa é um elemento crucial no aumento da eficiência econômica. Ela proporciona a estrutura que define os objetivos da empresa, bem como a maneira de atingi-los e fiscalizar o desempenho. A boa governança corporativa deve estimular o conselho de administração e a diretoria, para que os objetivos da empresa e dos acionistas sejam perseguidos, e para facilitar a fiscalização, incentivando o uso dos recursos de maneira mais eficiente (OCDE, 1999).

De acordo com o *IT Governance Institute* (2005 apud Fernandes; Abreu, 2006, p.11), “a governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização.”

Já para Weill; Ross (2006), Governança de TI é “a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização da TI”.

A Governança de TI, para Fernandes; Abreu (2006), busca o compartilhamento das decisões de TI com outros dirigentes da organização, além de instituir as regras, a organização e os processos necessários para dirigir o uso da tecnologia da informação pelos usuários, departamentos, divisões, negócios da organização, fornecedores e clientes, e também determinar de que forma a TI deve prover os serviços para a empresa.

A OCDE (Organização para a Cooperação e Desenvolvimento Econômico) (2000 apud WEILL; ROSS, 2006) articulou dois lados complementares da governança: o comportamental e o normativo. O lado comportamental da governança de TI, segundo Weill; Ross (2006), define os relacionamentos formais e informais, conferindo direitos decisórios a indivíduos ou grupos de indivíduos. Já o lado normativo define mecanismos, formalizando os relacionamentos e estabelecendo regras para assegurar que os objetivos sejam atingidos.

Fernandes e Abreu (2006) sugerem o “Ciclo da Governança de TI”, composto por quatro etapas, conforme apresentado na Tabela 3.1.

Tabela 3.1 - Ciclo da Governança de TI

	Etapas	Descrição
1	Alinhamento estratégico e compliance	Refere-se ao planejamento estratégico de TI, que considera as estratégias da empresa para seus produtos e segmentos de atuação, bem como os requisitos de compliance externos, como o ato Sarbanes-Oxley.
2	Decisão, compromisso, priorização e alocação de recursos	Refere-se às responsabilidades pelas decisões relativas à TI, bem como à definição dos mecanismos de decisão.
3	Estrutura, processos, operações e gestão	Refere-se à estrutura organizacional e funcional de TI,

		aos processos de gestão e operação dos produtos e serviços de TI, alinhados com as necessidades estratégicas e operacionais da empresa.
4	Medição do desempenho da TI	Refere-se à determinação, coleta e geração de indicadores de resultados dos processos, produtos e serviços de TI e à sua contribuição para as estratégias e objetivos do negócio.

Cada etapa do “Ciclo da Governança de TI” engloba componentes que, segundo Fernandes e Abreu (2006), permitem o desdobramento da estratégia de TI até a operação dos produtos e serviços correlatos.

De acordo com os autores, a etapa de **Alinhamento estratégico e compliance** possui doze componentes apresentados na Tabela 3.2.

Tabela 3.2 - Os componentes da etapa Alinhamento Estratégico e Compliance.

Componentes	Descrição
Alinhamento estratégico	Determina qual deve ser o alinhamento da TI, com relação à arquitetura, à infra-estrutura, às aplicações, aos processos e à organização, com as necessidades presentes e futuras do negócio.
Princípios de TI	São regras que auxiliam tomadas de decisão acerca da arquitetura e infra-estrutura de TI, aquisição e desenvolvimento de aplicações, entre outros.
Necessidades de aplicações	Dizem respeito às aplicações de TI que são necessárias para atender à continuidade e às estratégias do negócio, determinando quais aplicações devem ser mantidas, melhoradas, substituídas e implantadas.
Arquitetura de TI	“É a organização lógica dos dados, aplicações e infra-estruturas, definida a partir de um conjunto de políticas,

	relacionamentos e opções técnicas adotadas para obter a padronização e a integração técnicas e de negócio desejadas.” (WEILL; ROSS, 2006, p. 32)
Infra-estrutura de TI	“É a base da capacidade planejada de TI (tanto técnica como humana) disponível em todo o negócio, na forma de serviços compartilhados e confiáveis, e utilizada por aplicações múltiplas.” (WEILL; ROSS, 2006, p.37)
Objetivos de desempenho	Direcionam a administração de TI para atingir metas de desempenho compatíveis com os objetivos traçados para a prestação de serviços.
Capacidade de atendimento da TI	Define a quantidade de recursos computacionais e humanos necessários para atender à demanda por sistemas e serviços, indicando se a infra-estrutura atual tem condições de atendê-la.
Estratégia de <i>outsourcing</i>	Deve decidir, por exemplo, como fazer o <i>outsourcing</i> , o que será feito por ele e como gerenciá-lo. “O <i>Outsourcing</i> é um acordo para contratar outras partes para desempenhar funções ou serviços que antes eram feitos internamente[...]” (MIRANDA; REIS, 2007, p. 75)
Segurança da informação	Determinação de diretrizes e ações referentes à segurança dos aplicativos, da infra-estrutura, dos dados, das pessoas e das organizações.
Competências	Habilidades e conhecimentos necessários para o desenvolvimento e implantação das iniciativas de TI.
Processos e organização	Determinam a forma como os serviços e produtos de TI serão desenvolvidos, gerenciados e entregues aos usuários e clientes.
Plano de TI	É o principal produto do alinhamento estratégico. Contém informações sobre todos os outros componentes dessa etapa.

A etapa de **Decisão, compromisso, priorização e alocação de recursos** possui dois componentes, apresentados na tabela 3.3.

Tabela 3.3 - Os componentes da etapa Decisão, Compromisso, Priorização e Alocação de Recursos.

Componentes	Descrição
Mecanismos de decisão	Definem quem toma quais decisões em relação à TI dentro da organização.
Portfólio de TI	Metodologia para a priorização dos investimentos de TI. É baseada no retorno de projetos e ativos para a organização, e no seu alinhamento com os objetivos estratégicos do negócio. O portfólio de projetos permite que a organização saiba onde deve investir.

A etapa de Estrutura, processos, operações e gestão possui três componentes, como mostra a tabela 3.4.

Tabela 3.4 - Os componentes da etapa Estrutura, Processos, Operações e Gestão.

Componentes	Descrição
Operações de serviços	Locais onde geralmente ocorre o atendimento de serviços de TI. Podem ser, por exemplo, operações de sistemas, de suporte técnico, de infra-estrutura etc.
Relacionamento com o cliente	Diz respeito à relação dos usuários internos ou externos com a área de TI. Abrange processos que definem, por exemplo, a capacidade da TI para atender aos usuários.
Relacionamento com os fornecedores	Diz respeito à relação dos fornecedores com a área de TI. Trata, entre outros aspectos, da forma como as solicitações são encaminhadas para os fornecedores.

A etapa de **Medição do desempenho da TI** possui um componente, apresentado na tabela 3.5.

Tabela 3.5 - Os componentes da etapa de Medição do Desempenho da TI.

Componentes	Descrição
Gestão do desempenho da TI	Monitoramento dos objetivos de desempenho das operações de serviços.

3.2 FATORES MOTIVADORES

Os fatores motivadores da governança de TI podem ser divididos em internos e externos. As motivações internas são:

- os investimentos em TI aumentam progressivamente;
- integração da área de TI com os demais setores da empresa, aumentando o risco que a TI representa para o negócio;
- importância cada vez maior da segurança da informação para a empresa, devido, por exemplo, a ataques e vírus;
- os clientes estão cada vez mais exigentes em relação aos produtos e serviços;
- a vida dos produtos e dos serviços está cada vez mais curta;
- a transparência nos negócios é cada vez mais exigida.

Por trás da aplicação de recursos financeiros em TI, está a preocupação das empresas em melhorar seus processos operacionais, reduzir custos, aumentar a eficiência dos funcionários, aperfeiçoar a relação com fornecedores, parceiros e clientes. As organizações de TI encontram dificuldades para manter os custos operacionais sob controle devido, entre outros fatores, à elevada complexidade de gerenciamento. Isso acaba forçando as organizações a aumentar o orçamento e as equipes. Na verdade, são poucas as empresas que sabem, efetivamente, o retorno que os investimentos em TI trazem. A implantação da governança de TI busca criar formas de controlar e quantificar os resultados das otimizações (Esmeraldo, 2006).

Como motivações externas podem ser citadas:

- garantia de ética na organização;
- criação e proteção de benefícios para os acionistas;
- adequação ao Ato Sarbanes-Oxley (SOX), que apesar de representar restrições ao negócio, atrai geração de lucros. O SOX tem artigos diretamente relacionados com a área de TI.

Segundo o ITGI, a TI tem potencial para ser a principal motivadora da riqueza econômica no século XXI. Se hoje a TI já é um fator crítico para o sucesso da empresa, fornecendo oportunidades para obter vantagem competitiva e aumentar a produtividade, no futuro ela será ainda mais importante.

De acordo com estudos feitos por Weill; Ross (2006), empresas com fins lucrativos que seguem uma estratégia específica e apresentam um desempenho acima da média na Governança de TI, têm lucros superiores em relação às demais.

Com o aumento da importância da Tecnologia da Informação, continuam os autores, as equipes de alta gerência vêm-se cada vez mais desafiadas a controlá-la e geri-la a fim de garantir que ela gere valor. Por essa razão, muitas empresas vêm criando ou refinando estruturas de Governança de TI. Com isso, elas pretendem direcionar melhor os gastos com Tecnologia da Informação. Segundo Weill; Ross (2006), a TI é pervasiva, ou seja, ela está presente em todas as áreas da empresa, mais um motivo para não deixar de dar a devida importância à governança de TI.

Outro fator relevante é a rápida introdução de novas tecnologias, que vem gerando ameaças e oportunidades estratégicas. Os autores alertam para a previdência em estabelecer a infra-estrutura correta na hora certa, permitindo a rápida implementação de novas iniciativas comerciais com base eletrônica, e a consolidação e redução de custos de processos comerciais correntes. Essa previdência torna-se mais provável se existirem processos de governança formalizados para harmonizar os comportamentos desejáveis e os princípios de TI. “A incapacidade de reagir a mudanças de mercado tecnologicamente induzidas pode ameaçar a sobrevivência de uma empresa” (WEILL; ROSS, 2006, p.16).

Ainda seguindo o raciocínio de Weill; Ross (2006), uma governança eficaz permite às empresas o debate do valor potencial e a formalização do aprendizado. Formalizando processos de exceção, as empresas podem aprender muito, quando abordagens que não são consideradas padrão são usadas por boas razões. “Uma governança eficaz deixa explícito o aprendizado pelas exceções e difunde por toda a empresa quaisquer novas práticas sempre que apropriado” (WEILL; ROSS, 2006, p.17).

Os papéis dos tecnólogos e dos líderes de negócio estão num processo progressivo de interligação. A tomada de decisões de TI transforma-se numa tomada de decisão conjunta. Além de tomar boas decisões de TI, empresas de sucesso envolvem as pessoas certas no processo. Isso proporciona maiores números de aplicações estratégicas e índices de adesão. Uma governança de TI cuidadosamente planejada torna o processo decisório claro e transparente, condizente com a visão da alta gerência e, ao mesmo tempo, estimulante para a criatividade geral. Isso é importante, já que a alta gerência não tem como atender todas as requisições relativas à TI. (WEILL; ROSS, 2006)

3.3 OBJETIVOS DA GOVERNANÇA DE TI

O principal objetivo da Governança de TI é o alinhamento da TI aos requisitos do negócio, que se baseia na continuidade do negócio e no atendimento às suas estratégias e aos marcos de regulação externos.

Fernandes e Abreu (2006), desdobraram esse objetivo principal em outros seis objetivos:

- permitir à TI um posicionamento mais claro e consistente em relação às outras áreas da empresa;
- alinhar e priorizar as iniciativas de TI com a estratégia do negócio;
- alinhar a arquitetura e a infra-estrutura de TI às necessidades do negócio, pensando não só no presente, mas também no futuro;
- munir a TI com processos operacionais e de gestão, necessários para atender os serviços de TI, conforme padrões que atendam às exigências do negócio;
- garantir à TI uma estrutura de processos que possibilite a gestão do seu risco para a continuidade operacional da empresa;
- prover regras claras para as responsabilidades sobre decisões e ações relativas à TI, no âmbito da empresa.

3.4 FRAMEWORKS PARA GOVERNANÇA DE TI

Atualmente, existem vários modelos de melhores práticas para TI. Eles auxiliam na implantação da governança de TI. Holm; Kühn; Viborg (2006, p. 1-5) apresentam dezessete desses modelos:

- **ITIL** (*Information Technology Infrastructure Library*) - É o padrão mundial em Gerência de Serviço (Behr et al., 2004 apud Holm; Kühn; Viborg, 2006, p. 2). ITIL estabelece melhores práticas compreensivas e consistentes, baseadas na experiência coletiva de milhares de profissionais de TI. (Niessink; van Vliet, 2001 apud Holm; Kühn; Viborg, 2006, p. 2). ITIL está focado em processos críticos de negócio e disciplinas necessárias para que se tenha serviços de alta qualidade. Fora do *framework* ITIL, surgiu o *British Standard* BS15000, o primeiro padrão do mundo para gerenciamento de serviços de TI. Toda atividade é classificada em dois grupos: Gerência de Serviço e Prestação de Serviço. Isso define qualidade de TI como o nível de alinhamento entre serviços de TI e as efetivas necessidades de negócio (Niessink; van Vliet, 2000 apud Holm; Kühn; Viborg, 2006, p. 2). Como resultado, as organizações podem amadurecer suas melhores práticas sem ter que levar em consideração tecnologias específicas.
- **COBIT** (*Control Objectives for Information and Related Technology*) - Foi desenvolvido como um padrão genericamente aplicável para boas práticas de segurança e controle de TI (Lainhart, 2000 apud Holm; Kühn; Viborg, 2006, p.2). As ferramentas incluem: elementos de medição de desempenho; uma lista de Fatores Críticos de Sucesso (FCS); modelos de Maturidade para auxiliar nos testes de desempenho e na tomada de decisões.
- **ASL** (*Application Services Library*) - É uma coleção de melhores práticas para gerenciar o desenvolvimento e a manutenção de aplicações. É o padrão de domínio público para o gerenciamento de aplicações, diferente do ITIL, mas ligado a ele em termos de aderência

para padrões de gerenciamento de processos e provimento de um coerente, rigoroso e de domínio público conjunto de orientações. (Bastiens, 2004; van der Pols, 2004 apud Holm; Kühn; Viborg, 2006, p. 3). ASL é uma parte do *IT Service Management (ITSM) Library*. ASL reconhece três tipos de controle: funcional, aplicação e técnico. Enquanto o ITIL é um padrão geralmente aceito para organizar o gerenciamento técnico, o ASL oferece um *framework* para a organização do gerenciamento de aplicação (Meijer, 2003 apud Holm; Kühn; Viborg, 2006, p. 3).

- **Seis Sigma** - Essa metodologia provê as técnicas e ferramentas para melhorar a capacidade e reduzir os defeitos em qualquer processo. Ela aperfeiçoa qualquer processo de negócio através de constante revisão (Hammer, 2002 apud Holm; Kühn; Viborg, 2006, p. 3). Para isso, a Seis Sigma usa uma metodologia conhecida por DMAIC (Definir oportunidades, Medir desempenho, Analisar oportunidades, Melhorar desempenho, Controlar desempenho) (Puzdek, 2003 apud Holm; Kühn; Viborg, 2006, p. 3). Estes são os principais elementos do Processo de Aperfeiçoamento Seis Sigma: requerimentos do consumidor, qualidade do projeto, métricas e medidas, envolvimento do empregado e aperfeiçoamento contínuo.
- **CMM/CMMI** (*Capability Maturity Model/ Capability Maturity Model Integrated*) - Metodologia utilizada para desenvolver e refinar um processo de desenvolvimento de software da organização. O modelo descreve um caminho evolutivo de cinco níveis de crescimento organizado e sistematicamente processos mais maduros. CMM foi desenvolvido pelo *Software Engineering Institute* (SEI), um centro de pesquisa e desenvolvimento patrocinado pelo *U.S. Department of Defense* (DoD). Os cinco níveis sugeridos pelo CMM são: o inicial, o repetitivo, o definido, o gerenciado e o otimizado (Mathieassen e Sørensen, 1996 apud Holm; Kühn; Viborg, 2006, p. 3). O CMM é baseado no modelo clássico de cascata. Já o CMMI baseia-se no desenvolvimento iterativo e é mais orientado aos resultados.

- **IT Service CMM** - É um modelo de crescimento de maturidade focado nos provedores de serviços de TI (Niessink, 2003 apud Holm; Kühn; Viborg, 2006, p. 3). É uma evolução do CMM para desenvolvimento de software e incorpora estágios de maturidade similares. Origina-se dos esforços para desenvolver um *framework* de aperfeiçoamento de qualidade para empresas de serviços (Niessink; van Vliet, 1998 apud Holm; Kühn; Viborg, 2006, p. 3). O modelo não mede a maturidade serviços, projetos ou unidades da organização individualmente. Ele mede a maturidade de toda a organização, cobrindo o processo de prestação do serviço (Niessink et al., 2005 apud Holm; Kühn; Viborg, 2006, p. 3). Esse modelo é delimitado pelo cobrimento do desenvolvimento de novos serviços.
- **SAS70** (*Statements on Auditing Standards, No. 70 for Service Organizations*) - É um padrão de auditoria projetado para permitir que um auditor independente avalie e opine nos controles de uma organização de serviços. Desenvolvido pelo *American Institute of Certified Public Accountants* (AICPA), é internacionalmente reconhecido. Uma auditoria SAS70 é altamente reconhecida, porque representa que a empresa foi exposta a uma auditoria profunda, por uma firma independente de contabilidade e auditoria, das atividades de controle, as quais geralmente incluem controles sobre TI e seus processos. As organizações devem demonstrar que possuem controles adequados quando armazenam ou processam dados dos seus consumidores. Objetivos e atividades de controle deveriam também ser organizados de maneira a permitir ao usuário auditor e à organização identificar quais controles suportam as informações dos relatórios financeiros.
- **ISO 17799** - Padrão para segurança da informação que inclui um conjunto compreensível de controles e melhores práticas. O padrão pretende servir como um ponto de referência para identificar o conjunto de controles necessários para a maioria das situações onde os sistemas de informações são usados na indústria e no comércio. A

aderência ao padrão garante que a organização tem estabelecido um determinado nível de concordância para cada uma das dez categorias cobertas (Ma; Pearson, 2005 apud Holm; Kühn; Viborg, 2006, p. 3): política de segurança, organização da segurança, classificação e controle de valor, segurança de pessoal, segurança física e ambiental, gerenciamento de comunicações e operações, controle de acesso, desenvolvimento e manutenção de sistemas, gerenciamento de continuidade de negócio, e concordância (ISO 2000, BS 2002).

- **SOX** (Sarbanes-Oxley Act of 2002) - Decreto para proteger os investidores e o público em geral de erros na contabilidade e práticas fraudulentas na organização (SOX, 2002 apud Holm; Kühn; Viborg, 2006, p. 3). Essa lei não afeta só o lado financeiro da corporação, mas também o departamento de TI, cuja função é armazenar os registros eletrônicos da corporação. O SOX define que todos os registros do negócio, incluindo registros e mensagens eletrônicas, devem ser salvos por pelo menos cinco anos (Alles et al., 2004 apud Holm; Kühn; Viborg, 2006, p. 3-4). As conseqüências do não cumprimento são multas, prisão ou ambos. A concordância ao SOX traz implicações significantes para a função de TI (Moore; Swartz, 2003 apud Holm; Kühn; Viborg, 2006, p. 4). Os requerimentos do SOX estão cada vez mais integrados às iniciativas de gerenciamento de riscos (Beasley et al., 2004; Sammer, 2004 apud Holm; Kühn; Viborg, 2006, p. 4).
- **SysTrust** - Serviço de garantia desenvolvido pelo *American Institute of Certified Public Accountants* (AICPA) em conjunto com o *Canadian Institute of Chartered Accountants* (CICA). É projetado para aumentar o conforto da gerência, dos clientes e dos parceiros de negócio com sistemas que suportam um negócio ou atividade particular (Pacini et al., 2000 apud Holm; Kühn; Viborg, 2006, p. 4). Numa implantação SysTrust, o participante avalia e testa se um sistema específico é confiável quando medido sob três princípios essenciais: disponibilidade, segurança e integridade (McPhie, 2000 apud Holm; Kühn; Viborg, 2006, p. 4).

- **PRINCE2** (*Projects IN Controlled Environments*) - PRINCE é um método de gerenciamento de projetos que cobre a organização, o gerenciamento e o controle dos projetos. A princípio, ele foi desenvolvido como um padrão do governo britânico. Desde então, o PRINCE tem sido largamente utilizado nos setores público e privado e, agora, é um padrão *de facto* no Reino Unido. PRINCE foi desenvolvido inicialmente para projetos de TI, mas é usado também em muitos projetos que não são de TI. O PRINCE2, a última versão dessa metodologia, foi desenvolvido para incorporar requerimentos de usuários existentes e melhorar o método em direção a uma abordagem genérica de melhores práticas para a gerência de todos os tipos de projetos (OGC, 2005 apud Holm; Kühn; Viborg, 2006, p. 4).
- **IT Audit** - Uma revisão de TI deveria focar em três principais áreas: tecnologia, organização de TI e processos de TI (Cisco, 2002 apud Holm; Kühn; Viborg, 2006, p. 4). Como a organização tecnológica possui muitas partes funcionais, uma quantificação da estrutura organizacional de TI incluirá: infraestrutura (redes) e aplicações de negócio (pesquisa & desenvolvimento e suporte) (Cisco, 2002 apud Holm; Kühn; Viborg, 2006, p. 4).
- **IT Due Diligence** - Cisco (2002b apud Holm; Kühn; Viborg, 2006, p. 4) estabelece que o objetivo do plano de continuidade precisa estar claramente definido. Para isso, sugere que ele seja quebrado em sete partes: operação corrente de TI, planos de riscos e contingência, plano financeiro, requerimentos de investimento de capital, planos de oportunidades de inovação e recomendações, plano de transição e relatório de continuidade.
- **IT Governance Review** - Contém as seguintes atividades: mapear a governança atual das organizações com ferramentas de um *Governance Design Framework* (GDF) e de uma *Governance Arrangements Matrix* (GAM), comparar o GDF e a GAM, realizar auditoria em mecanismos de governança de TI, projetar a estrutura da futura governança de TI, transformar a versão futura do GDF e da GAM

da organização, e focar em comunicar, ensinar, convencer, refinar e medir o sucesso da governança de TI (Weill; Ross, 2006).

- **IT Governance Assessment** - é um framework para avaliar o desempenho da governança de TI. A performance da governança deve ser avaliada para analisar quão bem as suas estruturas encorajam comportamentos desejáveis (Weill; Ross, 2006). Por essa razão, o framework propõe que a governança de TI deve abordar cinco fatores importantes, que são: a configuração da empresa, as estruturas da governança, o desempenho da governança, e o desempenho financeiro.
- **IT Governance Checklist** - Damianides (2005 apud Holm; Kühn; Viborg, 2006, p. 4) sugere um checklist para governança de TI, contendo um conjunto de 44 questões de diagnóstico. Para cada uma das questões existe uma extensão para: valor da prestação de TI, alinhamento estratégico de TI, gerenciamento de risco e/ou desempenho. O questionário contém três subgrupos: assuntos de TI, relação da gerência com assuntos de TI e auto-avaliação da prática de governança de TI com relação à diretoria e gerência.
- **IT Governance Assessment Process (ITGAP) Model** - Peterson (2004 apud Holm; Kühn; Viborg, 2006, p. 4-5) sugere um processo de quatro estágios para avaliar governança de TI. Os estágios são: descrição e avaliação dos valores impulsionadores da governança de TI, descrição e avaliação da diferenciação da autoridade de tomada de decisão de TI para o *portfólio* de atividades de TI, descrição e avaliação das capacidades de governança de TI e descrição e avaliação da realização de valor de TI.

Além dos modelos apresentados acima, existem outros padrões como o **BS** (British Standard) **7799** e o **ISO/IEC 27001**, relativos à segurança da informação, o **PMBOK** (*Project Management Body of Knowledge*) – base de conhecimento em gestão de projeto, o **Balanced Scorecard** (BSC) – relativo ao planejamento e à gestão da estratégia, o **ISO/IEC 9001** e o conjunto de normas **ISO/IEC 27000**. Os

objetivos de cada um desses modelos, com base na obra de Fernandes; Abreu (2006) e no Instituto de Educação Tecnológica (IETEC) estão apresentados na tabela 3.6 a seguir:

Tabela 3.6 - Alguns modelos aplicáveis à Governança de TI

Modelo	Descrição
PMBOK	<p>Objetiva identificar o subconjunto do conjunto de conhecimentos em gerenciamento de projetos (PMI, 2004 apud Fernandes, Abreu, 2006, p.205);</p> <p>Fornecer uma visão geral do conjunto de conhecimentos (PMI, 2004 apud Fernandes, Abreu, 2006, p.205);</p> <p>Não é uma ferramenta de gerenciamento de projetos.</p>
BS 7799	<p>A sua primeira parte deu origem à ISO/IEC 17799</p> <p>A sua segunda parte deu origem à ISO/IEC 27001</p>
ISO/IEC 17799	<p>Estabelece diretrizes para iniciar, manter e melhorar a gestão da segurança da informação em uma organização;</p> <p>Visa atender aos requisitos identificados através da análise de risco;</p> <p>Serve como guia para desenvolver procedimentos de segurança da informação e práticas eficientes de gestão da segurança para a organização.</p>
ISO/IEC 27001	<p>Norma criada para estabelecer, implantar, operar, monitorar, rever, manter e melhorar um Sistema de Gestão da Segurança da Informação (ISMS);</p> <p>Pode ser usada visando a avaliação da conformidade por partes interessadas</p>

	internas e externas.
Balanced Scorecard (BSC)	<p>É um sistema de gestão estratégica;</p> <p>Traduz a estratégia da empresa em termos operacionais;</p> <p>Alinha a organização à estratégia;</p> <p>Transforma a estratégia em tarefas de todos;</p> <p>Converte a estratégia em processo contínuo;</p> <p>Mobiliza a mudança por meio da liderança executiva.</p>
ISO/IEC 9001	<p>Especifica requisitos para um sistema de gestão de qualidade;</p> <p>Todos os seus requisitos são genéricos;</p> <p>Pode ser combinada com outros modelos.</p>
BS 15000	Deu origem à ISO/IEC 20000
ISO/IEC 20000	<p>Apresenta um conjunto de requisitos certificáveis para a gestão de serviços em TI;</p> <p>Está alinhada às recomendações previstas pelo ITIL;</p> <p>Foi publicada em duas partes. A primeira trata das especificações e a segunda aborda o código de boas práticas para a gestão de serviços em TI.</p>

Dentre os modelos apresentados, dois serão apresentados com detalhes nos próximos capítulos: o ITIL e o COBIT.

4 O COBIT - VERSÃO 4.0 ²

Este capítulo apresenta o modelo COBIT – *Control Objectives for Information and Related Technology* – um padrão internacional aberto, cuja proposta é reunir as melhores práticas para Governança, Segurança e Controle de TI. Sua estrutura proporciona uma verificação dos processos de TI através da empresa, podendo ser utilizado internamente e por auditorias internas e externas.

Este capítulo não contém referências, trata-se de um resumo do documento COBIT 4.0 disponibilizado pelo ITGI (*IT Governance Institute*) em 2005.

4.1 O CRIADOR

O *IT Governance Institute* (ITGI) foi estabelecido em 1998 com o objetivo de avançar os padrões internacionais sobre gestão e controle da Tecnologia de Informação de um empreendimento.

O ITGI (“proprietário” do COBIT) projetou e criou a publicação COBIT® 4.0, principalmente como um recurso educacional para profissionais da área de TI, administradores, diretores e profissionais que atuam com o controle de TI. O objetivo era demonstrar a efetividade da governança de TI e como ela atua no suporte ao negócio, aperfeiçoa o investimento empresarial na TI e administra adequadamente riscos e oportunidades relacionadas à TI.

O material não faz referência a nenhum tipo de teste e seu autor não garante um resultado próspero referente à aplicação da metodologia, salienta ainda, que a aplicação deve considerar o juízo do profissional de controle em avaliar as particularidades do sistema ou ambiente de tecnologia em questão.

² Este capítulo é um resumo do documento COBIT 4.0 disponibilizado pelo ITGI, 2005.

4.2 ORGANIZAÇÃO – OS SEIS COMPONENTES DO COBIT

O COBIT está organizado em seis componentes:

- **Resumo executivo:** Apresenta os conceitos e princípios chaves.
- **Estrutura:** Base para a abordagem e para os elementos do *framework* COBIT. Apresenta o modelo do processo e seus quatro domínios.
- **Planejamento e organização:** domínio do COBIT onde são definidos o plano estratégico, a arquitetura das informações e a estrutura de TI.
- **Aquisição e implementação:** domínio do COBIT onde ocorre a aquisição de softwares aplicativos, infra-estrutura tecnológica e recursos de TI.
- **Distribuição e suporte:** domínio do COBIT onde são gerenciados: níveis de serviço, serviços de terceiros, desempenho e capacidade, atendimento aos clientes, problemas e incidentes, configurações e dados.
- **Monitoração e avaliação:** domínio do COBIT onde são monitorados e avaliados o desempenho e os controles internos da TI.

4.3 RESUMO EXECUTIVO

Segundo o *IT Governance Institute* (ITGI, 2005), para diversas organizações, a tecnologia de informação representa seu mais valioso, mas freqüentemente menos compreendido recurso.

Empreendimentos de sucesso reconhecem os benefícios de tecnologia de informação e usam isto para dirigir seus negócios. Estas empresas também entendem e administram os riscos associados à TI, como a crescente necessidade

de medidas regulatórias e de conformidade e a dependência crítica de muitos processos em relação à TI.

A necessidade de garantia sobre o valor da TI, a administração dos riscos com ela relacionados e as exigências crescentes de práticas de controle sobre a informação, são atualmente compreendidas como elementos-chaves de governança empresarial. Valor, risco e controle constituem o núcleo da governança de TI.

Governança de TI é responsabilidade dos executivos e diretores, necessitando de liderança, estrutura organizacional e processos que garantam que a TI da organização suporte as estratégias organizacionais e objetivos.

O objetivo da governança de TI é integrar e institucionalizar as práticas que garantam que a empresa suporte os objetivos do negócio.

A governança da TI habilita a empresa a obter o máximo dos benefícios de suas informações, criando oportunidades e ganhando vantagem competitiva. Para atingir estes objetivos é necessário um *framework* para controlar a TI, que satisfaça e suporte o *Committee of Sponsoring Organisations of the Treadway Commission (COSO) Internal Control – Integrated Framework*, o mais amplamente aceito *framework* de controle para governança empresarial e gerenciamento de risco.

Organizações necessitam satisfazer os requisitos de qualidade, confiança e segurança de suas informações. O gerenciamento pode otimizar o uso dos recursos de TI disponíveis, incluindo aplicações, informações, infra-estrutura e pessoal. Para atingir estes objetivos, o gerenciamento ajuda a compreender a arquitetura da empresa e como a governança e o controle podem contribuir para a TI.

O *Control Objectives for Information and related Technology (COBIT®)* provê um conjunto de boas práticas através de um *framework* composto de domínios e processos, apresentando atividades dispostas em uma estrutura manejável e lógica. O COBIT provê um modelo de processo genérico que representa todos os processos freqüentemente encontrados nas atividades de TI, disponibilizando um modelo de referência compreensível para gerentes operacionais de TI e de negócios. As boas práticas do COBIT representam o consenso de peritos.

O *framework* é fortemente focado em controle e menos em execução. Suas práticas ajudam a aperfeiçoar os investimentos em TI, assegurar a prestação de serviços e prover uma medida para avaliar quando algo não está sendo feito como deveria. Para obter êxito em suas metas e estar de acordo com as exigências empresariais, a administração necessita adotar um sistema de controle interno ou *framework* para TI.

O *framework* de controle COBIT contribui para estas necessidades fornecendo:

- Um mecanismo para alinhar a TI com os objetivos do negócio.
- Organizar as atividades da TI em um modelo de processo amplamente aceito.
- Identificar os melhores investimentos em recursos de TI.
- Definir os objetivos de controle que a administração deve considerar.

A orientação empresarial do COBIT consiste em unir os objetivos do negócio (metas da empresa) com os objetivos da TI e provê métricas e modelos de maturidade para avaliar a satisfação o cumprimento de tais objetivos, identificando as responsabilidades associadas aos processos.

A estrutura do COBIT é organizada em um modelo de processo que subdivide a TI em 34 processos alinhados com a responsabilidade das áreas de planejamento, construção, execução e monitoramento (auditoria), provendo uma visão fim-a-fim da TI.

Em resumo, para prover a informação que a empresa precisa para atingir seus objetivos, os recursos de TI precisam ser administrados por um conjunto de processos naturalmente agrupados.

A questão é como uma empresa aplica um controle rigoroso sobre sua TI e ainda garante a prestação de serviços e cumprimento dos prazos que o empreendimento requer? Como gerenciar os riscos e a segurança da TI? Como assegurar que a TI alcança seus objetivos e apóia o negócio?

Inicialmente, a administração precisa de objetivos de controle que definam como metas a implementação de políticas, procedimentos, práticas e estruturas organizacionais que ofereçam uma garantia razoável de:

- que os objetivos do negócio estão sendo satisfeitos;
- que eventos indesejados (sinistros) estão sendo prevenidos, detectados e corrigidos com eficiência e eficácia.

Posteriormente, diante da complexidade dos ambientes atuais, a gerência busca continuamente por informação condensada e oportuna, que possibilite a tomada rápida de decisões difíceis, que envolvam risco, e controlar situações inesperadas com sucesso. O que necessita ser avaliado e como? As empresas necessitam de uma forma de avaliar seu estado atual e quais os objetivos a serem alcançados. Necessitam ainda, implementar uma ferramenta de gerenciamento para monitorar as melhorias pretendidas.

A Figura 4.1 mostra algumas questões tradicionais e as ferramentas de informação utilizadas para respondê-las, mas para isso é necessário que seja feito um levantamento, utilizando indicadores e medidas de comparação.

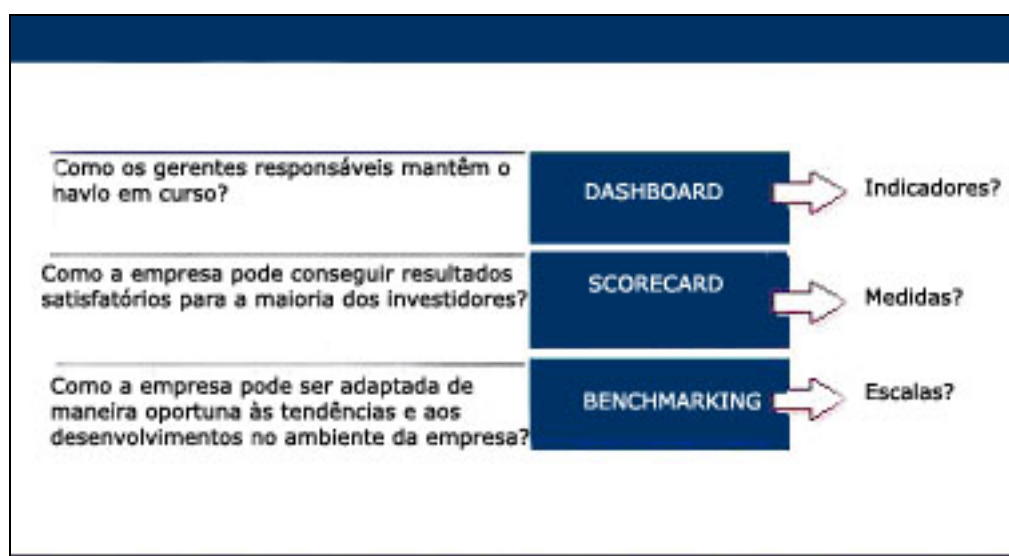


Figura 4.1 – Gerenciamento da Informação (Adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

Uma resposta para estas exigências de determinar e monitorar os controles apropriados de TI e níveis de desempenho são as definições específicas do COBIT para:

- *Benchmarking* da capacidade dos processos de TI, expressos como modelos de maturidade, derivados do *Software Engineering Institute's Capability Maturity Model (CMMI)*.
- Metas e métricas para os processos de TI, para definir e medir o resultado e o desempenho, baseados nos princípios de Robert Kaplan e David Norton *balanced business scorecard*.
- Metas das atividades para manter estes processos sob controle, baseadas nos objetivos de controle detalhados do COBIT.

A avaliação dos processos baseada no modelo de maturidade do COBIT é parte fundamental na implantação da governança de TI. Depois de identificados os processos e controles críticos, é possível através de uma análise de *gap*, demonstrar os níveis de maturidade desejados e identifica-los para posterior gerenciamento. Em uma próxima etapa, podem ser desenvolvidos planos de ação para trazer estes processos até o nível de maturidade desejado.

Assim, o COBIT apóia a governança de TI, provendo um *framework* que assegura que:

- a TI esteja alinhada ao negócio;
- a TI contribui para o negócio e maximiza benefícios;
- os recursos da TI são utilizados com responsabilidade;
- os riscos envolvidos na TI são administrados adequadamente.

A medida de desempenho é essencial para a governança de TI. Ela é suportada pelo COBIT, que inclui ainda ferramentas para monitorar os objetivos de controle, apontando o que os processos de TI devem entregar (produto final dos processos) e como estes serviços estão sendo entregues (maturidade dos processos e desempenho).

Muitas pesquisas identificaram que a falta de transparência dos custos da TI, de seu valor e de seus riscos são um dos grandes objetivos da governança de TI. A transparência é alcançada principalmente pela medida de desempenho. A Figura 4.2 destaca as áreas foco da governança de TI.

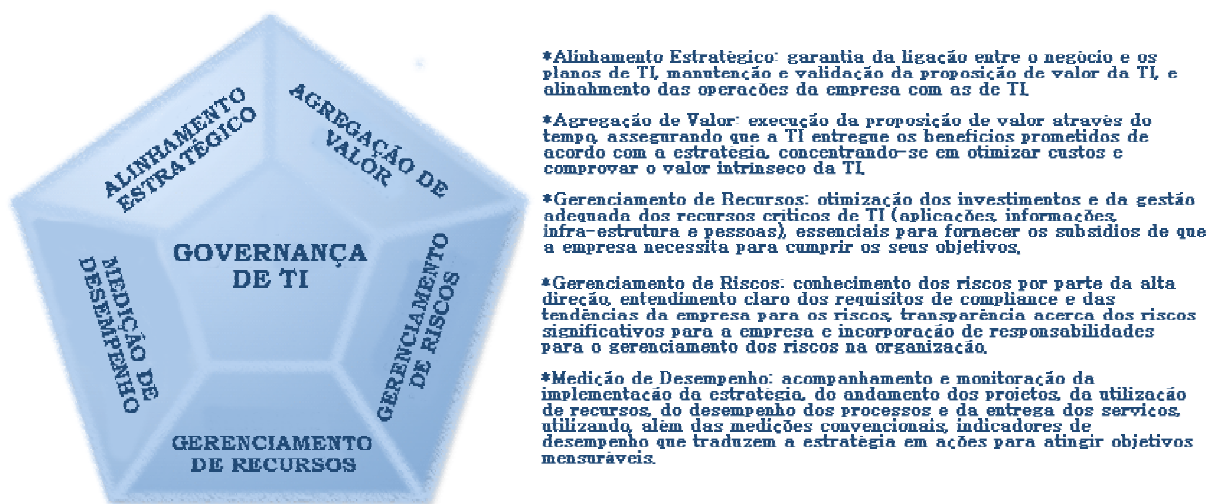


Figura 4.2 – Áreas foco da governança de TI (Adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

Estas áreas focadas pela governança de TI, descrevem os tópicos que a gerência executiva precisa dirigir para governar a TI em sua empresa.

A gerência operacional usa processos para organizar e administrar as atividades da TI continuamente. O COBIT provê um modelo genérico que representa todos os processos normalmente encontrados na TI e funciona como um modelo de referência comum, compreensível para gerentes operacionais de TI e gerentes de negócio. O modelo de processos do COBIT foi mapeado para as áreas-foco da governança de TI, provendo uma ponte entre o que os gerentes operacionais precisam executar e o que os executivos desejam governar.

Para alcançar a governança efetivamente, os executivos esperam controles que possam ser implementados por gerentes operacionais dentro de um *framework* de controle definido para todos os processos de TI. Os objetivos de controle do COBIT são organizados por processos da TI; então, o *framework* provê

uma relação entre as exigências da governança de TI, os processos da TI e os controles da TI.

O enfoque do COBIT é no que é exigido alcançar uma administração adequada e um controle satisfatório para o ambiente de TI; e é posicionado em um alto nível. O COBIT tem sido alinhado e utilizado com outros *frameworks* e guias mais detalhados de melhores práticas de TI. O COBIT atua como um integrador destes guias diferenciados, sintetizando objetivos-chave que unem governança e as exigências do negócio.

O COSO (e *frameworks* semelhantes) geralmente é aceito como o *frameworks* de controle interno para as organizações. O COBIT é *framework* mais aceito de controle interno para TI.

Os componentes do COBIT foram organizados em três níveis, destinados para apoiar:

- A gerência executiva.
- O gerenciamento do negócio e da TI.
- A governança, confiabilidade e profissionais de controle, auditoria e segurança.

O principal interesse dos executivos é entender porque a governança de TI é importante, quais são seus principais tópicos e qual a responsabilidade envolvida em administrá-la. O principal interesse dos responsáveis em gerenciar o negócio e a TI é satisfeito pelas Diretrizes de Gerenciamento (*Management Guidelines*), que foi integrado à quarta versão do livro do COBIT. Trata-se de uma ferramenta para auxiliar nas definições de responsabilidades, avaliação de desempenho e *benchmarks* para verificação do nível de maturidade dos processos. As diretrizes ajudam a prover respostas para as questões típicas de administração: Quanto devemos nos aprofundar nos controles de TI e o benefício justifica o custo? Quais são os indicadores de bom desempenho? Quais são as práticas chaves de administração que devemos aplicar? Como outras organizações lidam com isso? Como medir e comparar?

O principal interesse para a governança, confiabilidade e profissionais de controle, segurança e auditoria concentram-se no *framework* (como o COBIT organiza os objetivos da governança de TI e melhores práticas em domínios e processos, estabelecendo vínculos com as exigências empresariais), nos objetivos de controle e no modelo de maturidade.

Todos os componentes do COBIT se relacionam e provêm apoio à governança, administração, controle e auditoria, que segundo os autores constituem o público alvo da metodologia, como apresentado na Figura 4.3.

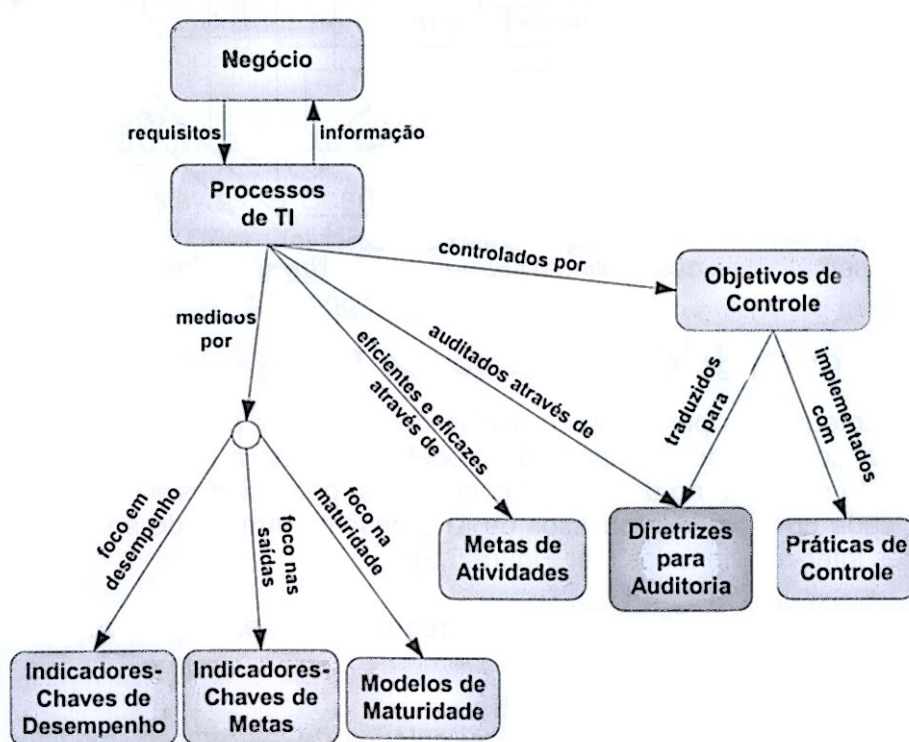


Figura 4.3 – Inter-relacionamento entre os componentes do COBIT (Adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

O COBIT é um *framework* que disponibiliza aos gerentes um guia para administrar as exigências de controle, os assuntos técnicos e os riscos empresariais e ainda reportar estes níveis de controle aos interessados (investidores, diretores e afins). O COBIT habilita o desenvolvimento de uma política clara e boas práticas para TI compatível com outros padrões.

Conseqüentemente, o COBIT se tornou o integrador das melhores práticas para governança de TI, ajudando a entender e administrar os riscos e benefícios associados à TI. A estrutura de processos do COBIT e seu alto-nível orientado ao negócio, provêem uma visão fim-a-fim da TI.

Os benefícios de implementar o COBIT como um *framework* de governança de TI incluem:

- Melhor alinhamento, baseado em um enfoque empresarial.
- Uma visão, compreensível para a administração, do que a TI faz.
- Esclarecimento das definições de responsabilidades, baseado em orientação a processo.
- Bom nível de aceitabilidade entre órgãos reguladores.
- Fornecimento de informação em linguagem clara para os investidores.
- Satisfação das exigências do COSO para os controles no ambiente de TI.

4.4 O FRAMEWORK COBIT

4.4.1 POR QUE ADOTAR UM FRAMEWORK

Crescentemente, os administradores estão observando o impacto significativo que a informação pode causar no sucesso do empreendimento.

É importante para a administração das empresas compreender como a TI está sendo gerenciada e como obter vantagens competitivas sobre seus recursos tecnológicos. Em particular, a alta administração precisa saber se a TI está sendo administrada de forma que:

- Contribua para os objetivos da empresa.

- Evolua e adapte-se às necessidades da organização.
- Os riscos enfrentados sejam criteriosamente gerenciados.
- Oportunidades sejam identificadas e aproveitadas.

Empreendimentos prósperos entendem os riscos e exploram os benefícios da TI, encontrando modos para:

- Alinhar a estratégia da TI com a estratégia empresarial.
- Prover estruturas organizacionais que facilitem a implementação de estratégias e metas da empresa.
- Criar relações construtivas e comunicação efetiva entre o negócio, a TI e sócios externos.
- Medir o desempenho da TI.

Os autores do ITGI afirmam que as empresas não podem lidar efetivamente com os requisitos de governança corporativa sem adotar e implementar um *framework* de governança para a TI que:

- Faça um vínculo com as exigências empresariais.
- Faça o desempenho diante destas exigências ser transparente.
- Organize suas atividades em um modelo de processo largamente aceito.
- Identifique os principais recursos a serem empregados.
- Defina os objetivos de controle gerenciais a serem considerados.

Além disso, os *frameworks* de governança e controle estão se tornando parte importante das melhores práticas de gerenciamento de TI e são facilitadores da consolidação da governança de TI e do atendimento das crescentes exigências dos órgãos reguladores e de controle.

As melhores práticas de TI ganharam significativa importância devido a vários fatores:

- Gerentes de negócio esperam melhores retornos dos investimentos em TI e garantias de que a TI atende às exigências do negócio.
- O nível crescente do custo de investimentos em TI revela-se um fator importante a ser considerado.
- A necessidade de satisfazer as exigências dos órgãos reguladores para os controles no ambiente de TI, principalmente em questões como sigilo e relatórios financeiros (por exemplo, as leis Sarbanes-Oxley e Basileia II³ e órgãos fiscalizadores como o Banco Central e a Controladoria Geral da União no Brasil).
- A seleção de fornecedores de serviço e a administração da terceirização de serviço e aquisição de produtos.
- O crescente risco relacionado com a TI como segurança em redes.
- As iniciativas de governança de TI, que incluem a adoção de *frameworks* de controle e melhores práticas para ajudar a monitorar e melhorar as atividades críticas da TI e aumentar o valor dos investimentos, reduzindo os riscos.
- A necessidade de reduzir os custos aplicando, quando possível, práticas já testadas e adotadas com sucesso em outras organizações.
- A maturidade crescente e aceitação conseqüente de *frameworks* mundialmente aceitos como COBIT, ITIL, ISO 17799, ISO 9001, CMM e PMBok.
- A necessidade de compreender como a empresa se comporta diante dos padrões geralmente aceitos e diante de seus próprios padrões já estabelecidos (*benchmarking*)

³ Acordo que estipula requisitos de capital mínimo para as instituições financeiras.

4.4.2 A QUEM SE DESTINA O FRAMEWORK

Um *framework* de controle e governança de TI, segundo o ITGI, destina-se à investidores internos e externos e a todos os profissionais envolvidos com questões como:

- Obter o máximo retorno sobre os investimentos em TI: profissionais que tomam decisões sobre os investimentos, que decidem sobre os requisitos, que utilizam os serviços da TI.
- Disponibilização de serviços: profissionais que gerenciam a organização e os processos da TI, desenvolvedores e operadores de serviço.
- Responsabilidade de controle dos riscos: profissionais com responsabilidades sobre sigilo, segurança e/ou risco, que executam atividades de *compliance* ou ainda que utilizam ou disponibilizam serviços que requerem alto grau de confiabilidade.

4.4.3 FOCADO NO NEGÓCIO

Para satisfazer as necessidades descritas anteriormente, o COBIT foi elaborado de forma a ser focado ao negócio, orientado ao processo, baseado em controles e direcionado à medição.

O enfoque no negócio é o principal tema do COBIT, pois foi projetado para ser utilizado em qualquer organização e não somente por fornecedores, usuários e auditores de TI. O COBIT é baseado no princípio de prover a informação que a empresa requer para alcançar seus objetivos, e na necessidade da empresa em gerenciar e controlar os recursos de TI usando um conjunto estruturado de processos para prestar os serviços de informação requeridos. Na Figura 4.4 podem-se observar os princípios básicos do COBIT.



Figura 4.4 – Princípio básico do COBIT (Adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

O COBIT fornece ferramentas para auxiliar o alinhamento às necessidades do negócio, conforme pode ser observado na Tabela 4.1.

Tabela 4.1 - Ferramentas fornecidas pelo COBIT para alinhamento ao negócio

Ferramenta do COBIT	Descrição
Critérios de Informação	<ul style="list-style-type: none"> • Para satisfazer os objetivos do negócio, as informações precisam de critérios de controle, aos quais o COBIT se refere como requerimentos do negócio relativos à informação. Baseados em requerimentos de segurança, qualidade e confiabilidade, são sete os critérios de informação: Efetividade, Eficiência, Confidencialidade, Integridade, Disponibilidade, <i>Conformidade</i> e Confiabilidade. • Fornece um método genérico para definir os requisitos do negócio.
Objetivos de Negócio e TI	<ul style="list-style-type: none"> • Provê uma base mais relacionada ao negócio e mais refinada para estabelecer os requerimentos do negócio e desenvolver as métricas que permitem avaliar o alcance dos objetivos. • Muitas empresas utilizam a TI para viabilizar o alcance de suas metas e isto pode ser representado como os objetivos da TI, os quais devem direcionar a arquitetura de TI da empresa. O COBIT disponibiliza em sua 4ª edição disponibiliza uma matriz de objetivos genéricos do negócio e da TI e o relacionamento

	<p>destes com os critérios de informação.</p> <ul style="list-style-type: none"> • A Figura 4.6 ilustra o relacionamento entre os objetivos do negócio e da TI.
Recursos de TI	<ul style="list-style-type: none"> • Para responder às exigências do negócio para a TI, a empresa necessita investir nos recursos requeridos para criar uma potencialidade técnica adequada para suportar uma potencialidade do negócio, com o objetivo de alcançar o resultado desejado. • Os recursos identificados no COBIT são: Aplicações, Informação, Infra-estrutura e Pessoal.

O COBIT define as atividades de TI em um modelo genérico de processo, composto de quatro domínios: Planejamento e Organização (PO), Aquisição e Implementação (AI), Prestação e Suporte (DS), e Monitoramento e Avaliação (ME). Estes domínios estão detalhados na Tabela 4.2 e podem ser mapeados respectivamente para as tradicionais áreas de responsabilidade de TI: Planejamento, Construção, Execução e Monitoramento. Incorporar um modelo operacional e uma linguagem comum para todas as partes do negócio envolvidas com a TI, é uma das etapas mais importantes para atingir a boa governança.

Tabela 4.2 - Domínios do COBIT

Domínio	Descrição
Planejamento e Organização (PO)	<ul style="list-style-type: none"> • Cobre aspectos estratégicos e táticos organizacionais; • Identifica a melhor forma através da qual a TI possa contribuir para o alcance dos objetivos do negócio; • A realização da visão estratégica precisa ser planejada, comunicada e gerenciada por diferentes perspectivas; • Este domínio preocupa-se com questões de gerenciamento como: • A TI e o negócio estão estrategicamente alinhados? A empresa está maximizando o uso de seus recursos? As pessoas compreendem os objetivos da TI? Os riscos são compreendidos e gerenciados de forma apropriada? A qualidade dos sistemas está de acordo com a necessidade dos

	negócios?
Aquisição e Implementação (AI)	<ul style="list-style-type: none"> • Para realizar a estratégia da TI, soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, como também implementadas e integradas ao processo do negócio; • Modificações e manutenção de sistemas existentes são cobertas neste domínio, para que continuem alinhados aos objetivos do negócio. • Este domínio preocupa-se com questões de gerenciamento como: • Os novos projetos estão aptos à prover as soluções que o negócio requer no prazo e sem falhas? Os novos sistemas implementados estão operando apropriadamente quando implementados?
Prestação e Suporte (DS)	<ul style="list-style-type: none"> • Focado na prestação dos serviços requeridos, incluindo: prestação do serviço, gerenciamento de segurança e continuidade do negócio, suporte aos usuários, e gerenciamento de dados e estruturas operacionais. • Este domínio preocupa-se com questões de gerenciamento como: • Os serviços de TI estão sendo entregues de acordo com as prioridades do negócio? Os custos da TI estão otimizados? A mão-de-obra está apta a utilizar os sistemas produtivamente e com segurança? A integridade, confidencialidade e disponibilidade dos dados está de acordo?
Monitoramento e Avaliação (ME)	<ul style="list-style-type: none"> • Os processos de TI precisam ser regularmente testados para garantir sua qualidade e conformidade com os requerimentos de controle. Este domínio trata do gerenciamento de desempenho, monitoramento de controles internos, conformidade com as regulamentações e provimento de governança em TI. • Este domínio preocupa-se com questões de gerenciamento como: • A TI está preparada para identificar os problemas em tempo hábil? O gerenciamento assegura que os controles internos

	são efetivos e eficientes? O risco, controle, conformidade e performance são monitorados e reportados?
--	--

4.4.5 BASEADO EM CONTROLES

O controle é definido como sendo políticas, procedimentos, práticas e estruturas organizacionais projetadas para prover uma seguridade razoável de que os objetivos de negócio serão alcançados e que eventos indesejáveis serão prevenidos ou detectados e corrigidos de forma adequada.

Um objetivo de controle de TI é uma frase que representa o desejo de um resultado ou propósito que se espera atingir através da implementação dos procedimentos de controle em uma atividade particular de TI. Os objetivos de controle de TI do COBIT são o mínimo requerido para um controle efetivo de cada processo de TI.

O COBIT apresenta um modelo de processo genérico que representa todos os processos normalmente encontrados em funções de TI, provendo um modelo de referência comum compreensível por gerentes operacionais de TI e de negócio. O COBIT organiza os controles de TI em processos e o *framework* permite uma ligação direta entre os requerimentos de governança de TI, os processos de TI e os controles de TI. Cada processo de TI possui um objetivo de controle de alto nível e um número de objetivos de controle detalhados. Como um todo, representam as características de um processo bem gerenciado.

Cada processo do COBIT possui requerimentos de controle genéricos, tais como: proprietário do processo, repetitividade, metas e objetivos, papéis e responsabilidades, desempenho do processo, e políticas, planos e procedimentos.

Controles efetivos reduzem o risco e aumentam a eficiência dos processos, pois haverão menos erros e um gerenciamento mais consistente.

Além disso, o COBIT apresenta exemplos ilustrativos de entradas e saídas genéricas dos processos, atividades e guia em papéis e responsabilidades através de um gráfico RACI (que estabelece quem é o responsável, quem autoriza e

direciona e quem deve ser informado e consultado em cada processo) metas chave das atividades e métricas.

O sistema de controles internos da organização impacta a TI em três níveis, conforme demonstrado na Tabela 4.3.

Tabela 4.3 - Impactos do Sistema de Controles Internos da Organização na TI

Nível	Descrição
Gerência Executiva	<ul style="list-style-type: none"> • Objetivos de negócio são definidos, políticas são estabelecidas e decisões são tomadas de como implantar e gerenciar os recursos da empresa para executar sua estratégia; • A abordagem geral, de governança e de controle, é estabelecida pela diretoria e informada para a empresa; • O ambiente de controle da TI é dirigido por este conjunto de objetivos e políticas de alto nível.
Nível de Processos do Negócio	<ul style="list-style-type: none"> • Controles aplicados à atividades específicas de negócio; • Maior parte dos controles e aplicações deste nível são automatizados; • Os controles são conhecidos como controles de aplicação e alguns, como autorização de transações, permanecem manuais; • Os controles neste nível são uma combinação de controles manuais, de negócio e automatizados por aplicações e existe responsabilidade do negócio em definir e gerenciar os controles. Os controles de aplicações requerem o suporte da TI para projeto e desenvolvimento.
Suporte de Processos de Negócio	<ul style="list-style-type: none"> • Para suportar os processos do negócio a TI provê os serviços de TI, usualmente como serviços compartilhados por vários processos de negócio; • Os controles aplicados para todos os serviços de TI são conhecidos como controles gerais de TI e a operação confiável desses controles gerais é necessária para a dependência ser colocada nos controles de aplicação.

Controles gerais são controles aplicados aos processos e serviços de TI, tais como: desenvolvimento de aplicação, gerenciamento de mudanças, segurança e

operação de computadores. Existem ainda, os controles de aplicação como: completitude, exatidão, validade, autorização e segregação de funções.

O COBIT assume como responsabilidade da TI projetar e implementar controles de aplicação automatizados, sendo cobertos no domínio de Aquisição e Implementação. O gerenciamento operacional e o controle são tarefas do responsável pelo processo. O COBIT trata de controles gerais de TI, uma vez que controles de aplicação são integrados aos processos do negócio.

Alguns objetivos de controle de aplicação recomendados são: origem de dados e controles de autorização, controles da entrada de dados, controles do processamento de dados, controles da saída de dados e controles de segurança de dados.

4.4.6 DIRECIONADO À MEDIÇÃO

Uma necessidade básica para qualquer empresa é compreender e posicionar-se sobre seus sistemas de TI e decidir qual nível de gerenciamento e controle aplicar. Para decidir o nível de maturidade em que se encontram seus processos de TI, os gerentes precisam avaliar quanto de controle necessitam aplicar e se o benefício obtido justifica os custos. O COBIT provê três ferramentas para auxiliar neste processo de análise: **modelos de maturidade, metas de desempenho e métricas para o processo de TI, e metas de atividades.**

Partindo dos processos do COBIT e dos objetivos de controle de alto nível, o responsável por um processo deve poder aperfeiçoá-lo, de forma a alcançar o controle pretendido. Os modelos de maturidade o auxiliam em três questões básicas: definir o estado atual do processo, definir de forma eficiente onde pretende-se chegar e uma forma de medir o progresso em busca deste objetivo.

Os modelos de maturidade e controle sobre os processos de TI são baseados em um método de avaliar a organização, desde o nível de não existência (0) até otimizado (5). O objetivo dessas avaliações é verificar onde se encontram os

problemas e definir as prioridades para aperfeiçoamento. O propósito não é avaliar o nível de aderência aos objetivos de controle.

Os níveis de maturidade foram projetados como perfis de processos de TI, onde a empresa reconheceria como descrições de possíveis estados atuais e futuros. Não é um modelo de limiares, onde devem ser cumpridos todos os requisitos de um nível inferior para se poderem cumprir os do nível superior. Usando o modelo de maturidade desenvolvido para os 34 processos de TI, a gerência pode identificar: o desempenho atual, o status atual do cenário (comparação) e o alvo da empresa para aperfeiçoamento. O ranking utilizado nesta avaliação está apresentado na Figura 4.5.

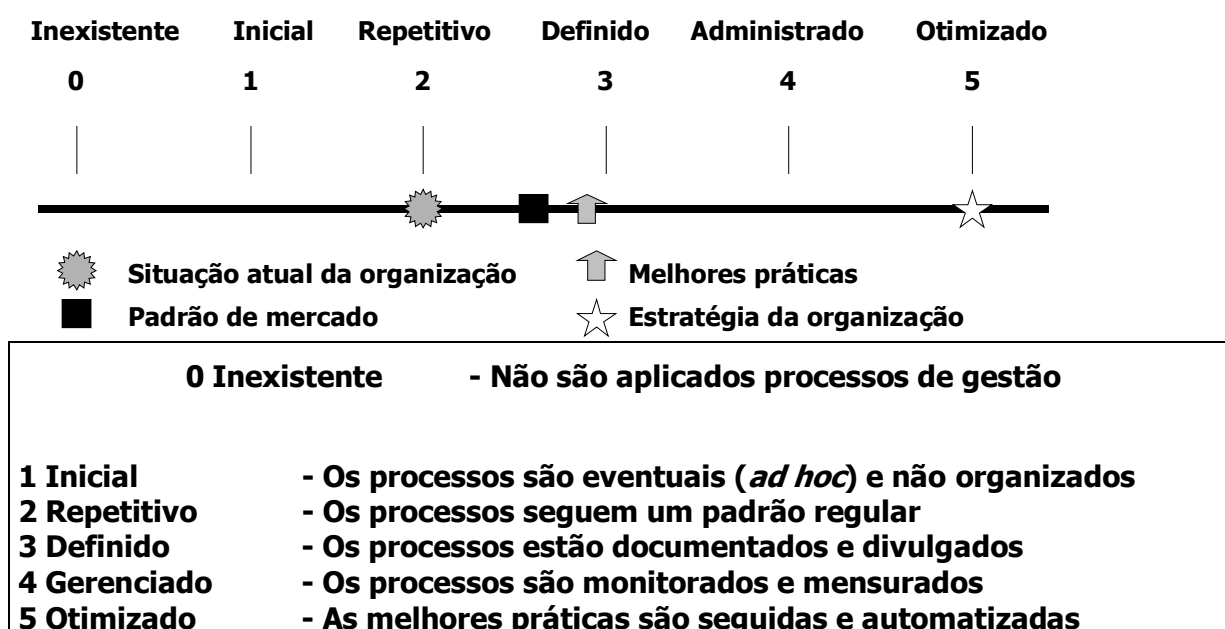


Figura 4.5 - Representação Gráfica do Modelo de Maturidade. (Adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

O desenvolvimento dos níveis de cada processo foi baseado em um modelo de maturidade genérico, como apresentado na Tabela 4.4.

Tabela 4.4 - Modelo Genérico de Maturidade

Nível	Descrição
0 Não Existente	<ul style="list-style-type: none"> • Completa falta de qualquer processo reconhecível; • A empresa nem reconheceu que existe a necessidade de se gerenciar tal processo.

1 Inicial	<ul style="list-style-type: none"> • Existe evidência de que a empresa reconheceu a necessidade de gerenciamento do processo; • Entretanto, não existem ainda processos padronizados, e somente, abordagens <i>ad hoc</i> estão sendo aplicadas em casos individuais; • No geral, a abordagem de gerenciamento está desorganizada.
2 Repetitivo	<ul style="list-style-type: none"> • Procedimentos similares são seguidos por diferentes pessoas para a execução de uma mesma tarefa; • Não há treinamento formal ou procedimentos formalizados de comunicação, a responsabilidade é individual; • Existe grande dependência dos conhecimentos individuais e, logo, erros são comuns.
3 Definido	<ul style="list-style-type: none"> • Procedimentos são padronizados e documentados, e comunicados através de treinamento; • É deixado para as pessoas seguirem esses processos, tornando difícil detectar os desvios; • Os procedimentos não são sofisticados, mas a formalização refere-se à práticas existentes.
4 Gerenciado	<ul style="list-style-type: none"> • É possível monitorar e medir a concordância com os procedimentos e tomar medidas prudentes quando os processos parecem não estar trabalhando efetivamente; • Processos estão em constante melhoramento e provêm boas práticas; • Automação e ferramentas são usadas de forma limitada ou fragmentada.
5 Otimizado	<ul style="list-style-type: none"> • Os processos foram refinados a um nível de melhores práticas, baseados em resultados de melhoramento contínuo e modelagem de maturidade com outras empresas, • A TI é usada de forma integrada para automatizar o fluxo de trabalho, provendo ferramentas para melhorar a qualidade e efetividade, tornando a empresa rápida em adaptações.

A vantagem de uma abordagem de modelo de maturidade é que se torna relativamente fácil para a gerência localizar o status atual na escala e avaliar os

recursos envolvidos, caso determinado melhoramento de desempenho seja requerido. A escala de zero a cinco é usada para mostrar como um processo pode evoluir da inexistência até a otimização.

O gerenciamento da capacidade de um processo não é o mesmo que o desempenho do processo. A capacidade requerida, como determinada pelas metas do negócio e TI, pode não ser necessariamente aplicada no mesmo nível em todo o ambiente de TI da organização. A avaliação de desempenho é essencial para determinar qual o desempenho atual da organização em seus processos de TI. Enquanto uma capacidade propriamente aplicada reduz os riscos, a empresa ainda precisa os controles necessários para garantir que os riscos são mitigados e o valor é obtido, alinhado com as necessidades do negócio.

Capacidade, desempenho e controle são as dimensões da maturidade de um processo. O modelo de maturidade é uma forma de mensurar quão bem desenvolvidos os processos estão, mas quanto ainda precisam ser desenvolvidos depende da estratégia da empresa e das necessidades do negócio.

O modelo do COBIT foca em capacidades, e não necessariamente em desempenho. Os níveis foram projetados para serem sempre aplicáveis, provendo uma descrição onde uma empresa pode reconhecer como melhor se adequariam aos seus processos. O nível correto se define devido ao tipo de empresa, seu ambiente e sua estratégia. O desempenho, ou como uma capacidade é usada e implantada, é baseado em decisões de custo-benefício. Quanto maior o nível de maturidade, maior o controle sobre o processo. Os mecanismos de controle são baseados nos objetivos de controle do COBIT e focados no que deve ser realizado no processo, enquanto o modelo de maturidade se preocupa mais em quão bem o processo é gerenciado. Um ambiente de controle propriamente implementado é alcançado quando os três aspectos da maturidade (capacidade, desempenho e controle) são mapeados. Melhorar a maturidade reduz riscos e melhora a eficiência, leva a menos erros, processos mais previsíveis e ao uso dos recursos de forma mais eficiente em relação ao custo. **As metas e métricas de performance** são definidas pelo COBIT em três níveis: métricas e objetivos da TI (definem as expectativas do negócio em relação a TI), metas e métricas de processo (definem que serviços os

processos de TI devem prover para suportar os objetivos da TI) e métricas de desempenho (para medir o quão bem os processos são executados).

O COBIT utiliza dois tipos de métricas: indicadores de metas e de desempenho. Indicadores de metas de um nível inferior se tornam indicadores de desempenho em um nível superior. Os *Key Goal Indicators* (KGI) – ou Indicadores de metas chave - definem medidas para avaliar o processo quanto ao alcance dos seus requerimentos do negócio, sendo expressos usualmente em termos de critérios de informação como: disponibilidade de informação, controle dos riscos de integridade e sigilo, custo e eficiência dos processos e operações, efetividade e conformidade.

Os indicadores de desempenho chave definem métricas para se medir quão bem um processo está sendo executado para viabilizar o alcance de uma meta.

A Figura 4.6 ilustra o relacionamento entre processos, objetivos da TI e do negócio e métricas. As metas são definidas de cima para baixo, naqueles objetivos de negócio que determinarão um certo número de objetivos de TI para suportá-los. Os objetivos da TI decidirão os diferentes objetivos de processos necessários e cada objetivo de processo demandará certos objetivos de atividades. O alcance de objetivos é medido por metas chamadas *key goal indicators* ou *KGIs*, que direcionam os objetivos de nível superior. A performance é verificada pelas métricas chamadas *key performance indicators* (KPI). As métricas permitem à gerência corrigir o desempenho e o realinhamento do processo com os objetivos.

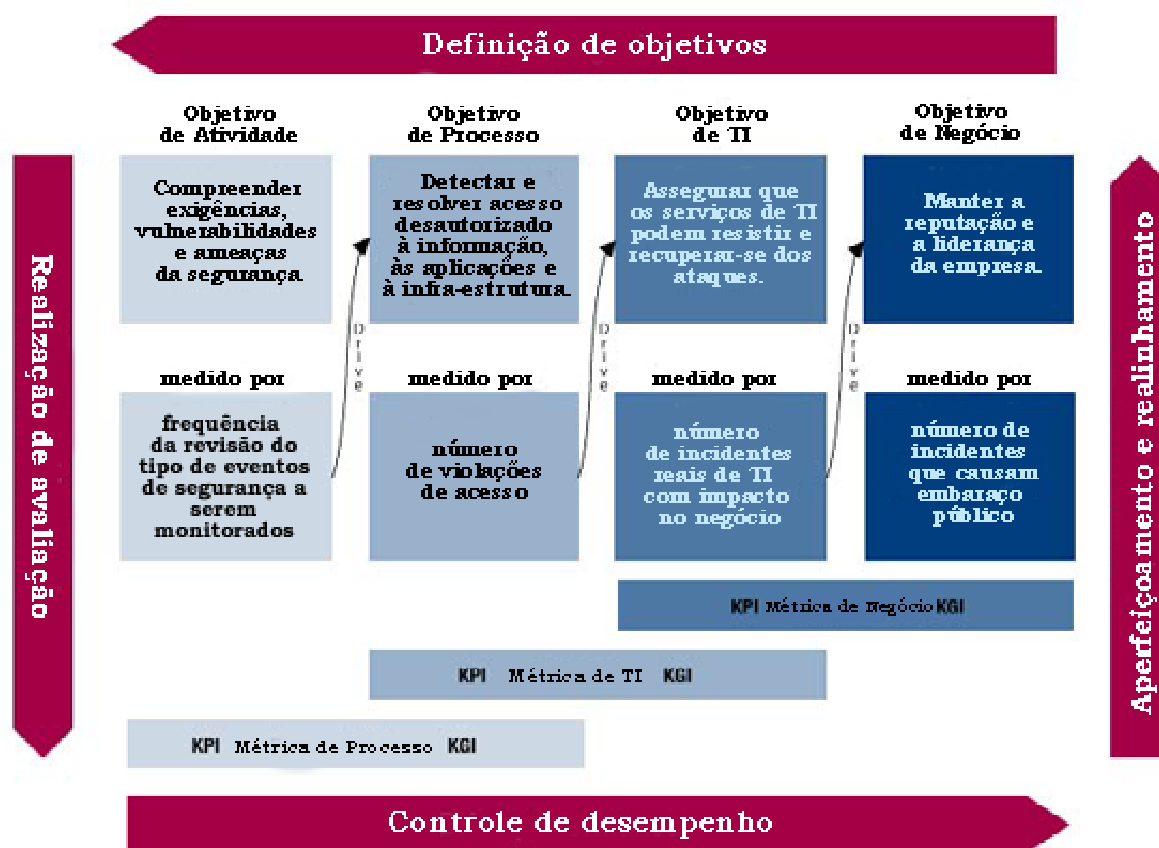


Figura 4.6 - Relacionamento entre processos, objetivos e métricas (adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

4.5 A ESTRUTURA DO FRAMEWORK DO COBIT

O *framework* do COBIT une os requerimentos do negócio por informação e governança com os objetivos das funções de TI. O modelo de processo permite que atividades de TI e os recursos que as suportam sejam propriamente gerenciados e controlados baseado nos objetivos de controle do COBIT, e alinhadas e monitoradas usando as métricas KGI e KPI, conforme ilustrado na Figura 4.7.

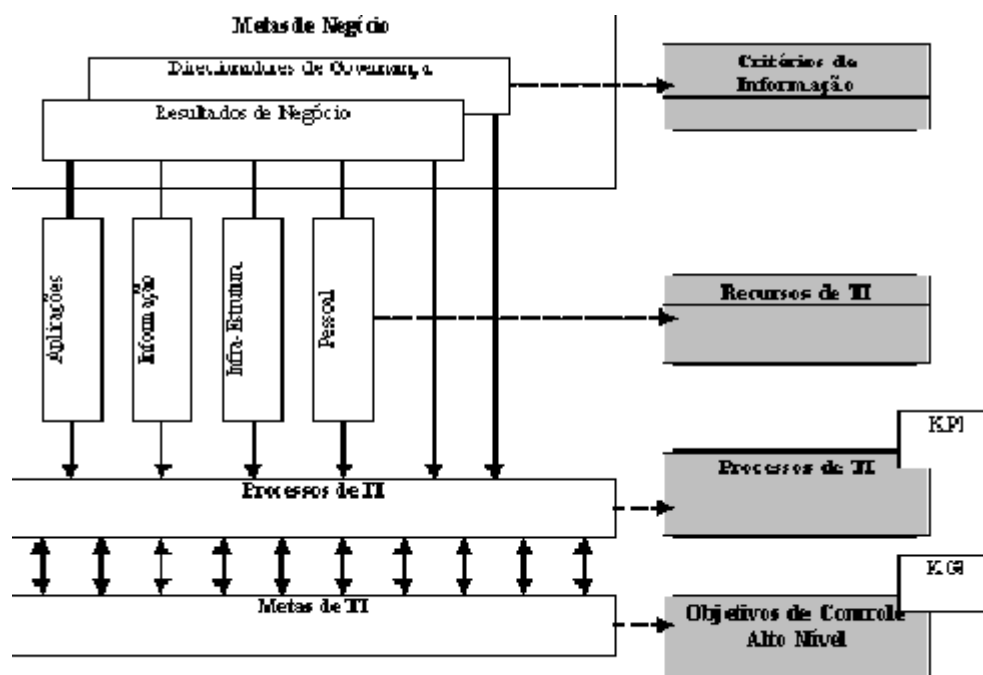


Figura 4.7 – Gerenciamento, Controle, Alinhamento e Monitoramento do COBIT (Adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

Resumindo, os recursos de TI são gerenciados por processos de TI para alcançarem metas de TI que respondam aos objetivos do negócio. Este é o princípio básico do *framework* COBIT, que é representado pelo cubo COBIT, como mostrado na Figura 4.8.

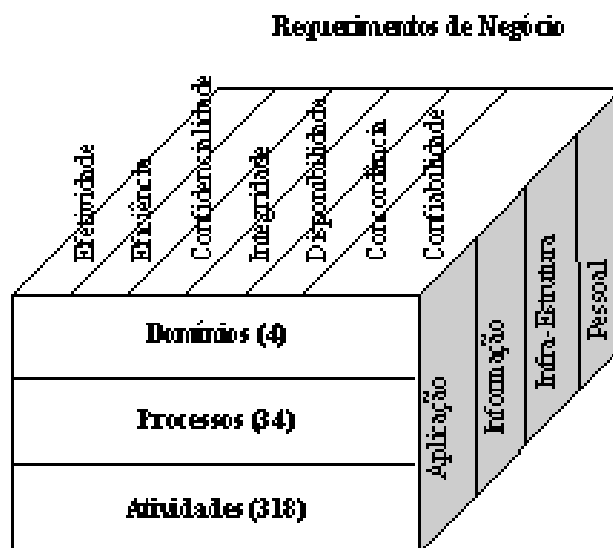


Figura 4.8 – O Cubo do COBIT (Adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

Em detalhes, o COBIT pode ser demonstrado graficamente como na Figura 4.9, com um modelo de processo composto de 4 domínios, contendo 34 processos genéricos, gerenciando os recursos de TI para prestar informação ao negócio, de acordo com os requerimentos de governança e com as necessidades do negócio.

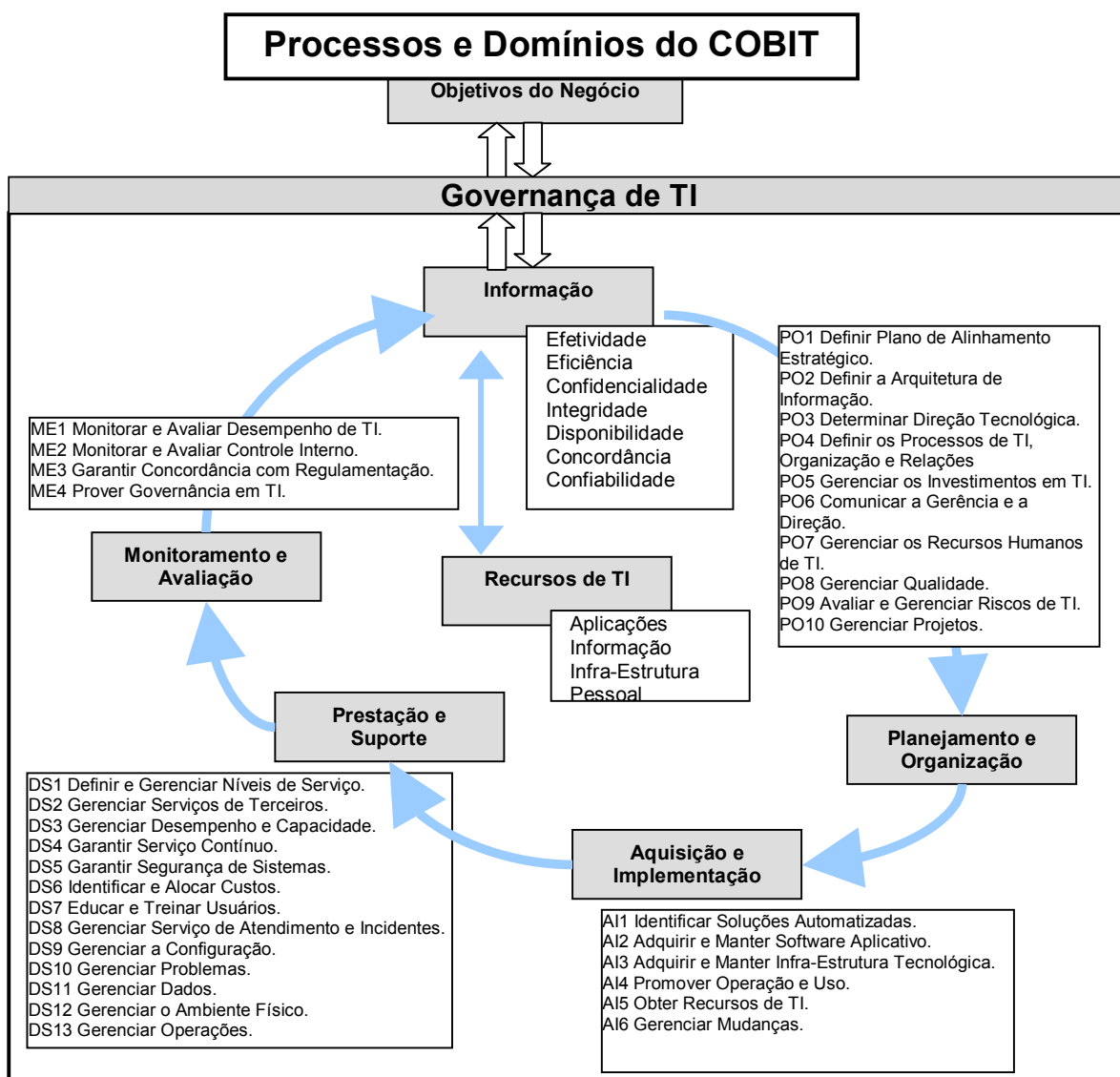


Figura 4.9 – O Framework do Modelo COBIT (Adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

4.6 OS DOMÍNIOS DO COBIT

Os quatro domínios do COBIT, descritos na Tabela 4.2, abordam dimensões detalhadas em 34 processos (objetivos de controle de alto nível) e estes, possuem 318 objetivos de controle que permitem uma visão ampla sobre o que é requerido da área de TI em suas atividades para suportar os objetivos do negócio e mitigar os riscos, fazendo uso adequado dos recursos de TI. Cada domínio e seus

respectivos processos atingem, de forma primária ou secundária, os critérios de informação e utilizam determinados recursos, conforme descrito na Figura 4.10.

Para cada um dos 34 processos o COBIT fornece, além dos objetivos de controle, os fatores críticos de sucesso, os indicadores de resultado e os indicadores de performance, permitindo uma abordagem ampla sobre o que se espera do processo, como se medem os resultados esperados e como se avalia a performance.

Domínio	Processo	Critérios de Informação Envolvidos							Recursos de TI Envolvidos				
		Efetividade	Eficiência	Confidencialidade	Integridade	Disponibilidade	Conformidade	Confiabilidade	Pessoas	Aplicações	Infra-estrutura de TI	Informações	
Planejamento e Organização	PO1	Definir um plano estratégico de TI	P	S						X	X	X	X
	PO2	Definir a arquitetura das informações	P	S	S	S					X		X
	PO3	Determinar a direção tecnológica	P	S						X			
	PO4	Definir a estrutura e o relacionamento de TI	P	S						X			
	PO5	Gerenciar o investimento em TI	P	P					S	X	X	X	
	PO6	Divulgar os objetivos e a orientação da gerência	P					S		X			
	PO7	Gerenciar os recursos humanos	P	P						X			

	PO8	Gerenciar qualidade	P					P	S	X	X		X
	PO9	Avaliar os riscos	P	S	P	P	P	S	S	X	X	X	X
	PO 10	Gerenciar os projetos	P	P						X	X	X	
	PO 11	Gerenciar a qualidade	P	P		P			S	X	X	X	
Aquisição e Implementação	AI1	Identificar soluções automatizadas	P	S								X	X
	AI2	Adquirir e prestar manutenção em softwares aplicativos	P	P		S		S	S			X	
	AI3	Adquirir e realizar manutenção na infraestrutura tecnológica	P	P		S							X
	AI4	Documentar e informar sobre uso e operação dos sistemas	P	P		S		S	S	X	X	X	
	AI5	Aquisição de recursos de TI	P			S	S			X	X	X	X
	AI6	Gerenciar alterações	P	P		P	P			X	X	X	X
	AI7	Instalar e certificar soluções e mudanças	P	S		S	S			X	X	X	X
Distribuição e Suporte	DS1	Definir e gerenciar níveis de serviços	P	P	S	S	S	S	S	X	X	X	X
	DS2	Gerenciar serviços de terceiros	P	P	S	S	S	S	S	X	X	X	X
	DS3	Gerenciar desempenho e capacidade	P	P			S				X	X	
	DS4	Assegurar a continuidade do	P	S			P			X	X	X	X

		serviço											
	DS5	Assegurar a segurança dos sistemas			P	P	S	S	S	X	X	X	X
	DS6	Identificar e alocar custos		P					P	X	X	X	X
	DS7	Educar e treinar usuários	P	S						X			
	DS8	Gerenciar o atendimento aos clientes e incidentes	P	P						X	X		
	DS9	Gerenciar as configurações	P				S		S		X	X	
	DS10	Gerenciar problemas e incidentes	P	P			S			X	X	X	X
	DS11	Gerenciar dados				P			P				X
	DS12	Gerenciar as instalações				P	P						
	DS13	Gerenciar as operações	P	P		S	S			X	X		X
Monitoramento e Avaliação	MA1	Monitorar e avaliar a performance da TI	P	P	S	S	S	S	S	X	X	X	X
	MA2	Monitorar e avaliar os controles internos da TI	P	P	S	S	S	P	S	X	X	X	X
	MA3	Assegurar conformidade com as práticas regulatórias	P	P	S	S	S	P	S	X	X	X	X
	MA4	Prover a governança de TI	P	P	S	S	S	P	S	X	X	X	X

(P)primário (S) secundário (X) aplicável à

Figura 4.10 – Domínios e processos do COBIT (Adaptado de: *IT Governance Institute, Information Systems Audit and Control Foundation, COBIT 4.0, 2005*).

4.7 ACEITABILIDADE DO COBIT

O COBIT é baseado na análise e harmonização de padrões existentes de TI e de melhores práticas, convergindo com as práticas de governança mais aceitas. Ele atua como um integrador de outros *frameworks* e práticas de governança e foi projetado para ser usado em uma implementação de governança de TI juntamente com um outro padrão ou conjunto de melhores práticas.

O COBIT é orientado em direção aos objetivos e escopo da governança de TI, garantindo que seu *framework* de controle é compreensivo e alinhado com os princípios de governança corporativa, atendendo as demandas das diretorias, gerências (executiva, negócio e TI), auditores e reguladores. Ele foi desenvolvido e é mantido pelo Instituto de Governança de TI – ITGI, trata-se de um instituto independente que se dedica à pesquisas contínuas na área de governança e controle.

Os objetivos de controle do COBIT podem ser mapeados nas cinco áreas foco da governança de TI conforme a Tabela 4.5.

Tabela 4.5 - O COBIT e as áreas foco da governança de TI

	Objetivos	Métricas	Práticas	Modelos de Maturidade
Alinhamento estratégico	Alvo Primário	Alvo Primário		
Entrega de Valor		Alvo Primário	Alvo Secundário	Alvo Primário
Gerenciamento de Risco		Alvo Secundário	Alvo Primário	Alvo Secundário
Gerenciamento de Recursos		Alvo Secundário	Alvo Primário	Alvo Primário

	Objetivos	Métricas	Práticas	Modelos de Maturidade
Avaliação de Desempenho	Alvo Primário	Alvo Primário		Alvo Secundário

5 O ITIL⁴

Este capítulo apresenta o modelo ITIL – *Information Technology Infrastructure Library* ou biblioteca para infra-estrutura de Tecnologia da Informação – um padrão internacional aberto, composto de documentos que reúnem as melhores práticas para gerenciamento de serviços de TI e que pode ser utilizado por qualquer empresa que detenha uma área de TI e queira gerenciar/otimizar sua gerência de serviços. O ITIL é um *framework* genérico baseado na experiência de profissionais da área, focando o gerenciamento e provisão dos serviços operacionais de TI e a formalização dos processos dentro das organizações.

Este capítulo não contém referências, trata-se de um resumo dos documentos que compõe o ITIL , disponibilizados e mantidos pelo ITSMF - The IT Service Management Forum.

5.1 O CRIADOR

O ITIL (ITSMF, 2003) foi inicialmente desenvolvido pela *Central Computer and Telecommunications Agency* (CCTA) do governo britânico, sendo originalmente conhecido como *Government IT Infrastructure Management Method* (GITIMM). Em 1989, as melhores práticas informadas por diferentes organizações do setor público, privado e empresas de consultoria, foram consolidadas, integradas e nominadas como ITIL. Em 2001, o CCTA fundiu-se ao *Office of Government Commerce* (OGC), o qual atualmente possui os direitos sobre o material publicado sobre o ITIL. A partir de 2001, o modelo ganhou popularidade, consolidando-se na Europa e sendo reconhecido por diversas organizações como um guia para gerência efetiva de serviços de TI.

O ITIL, além de conter uma série de livros úteis apresentando as melhores práticas em gerência de recursos de TI, envolve várias organizações,

⁴ Este capítulo é um resumo dos documentos que compõe o ITIL Versão 2 disponibilizado pelo ITSMF, 2003.

ferramentas, serviços de treinamento e consultoria, outros *frameworks* relacionados e publicações. O ITIL também é considerado, além de um *framework*, uma abordagem e filosofia difundida entre aqueles o utilizam em seu trabalho. Um aspecto que deve ser ressaltado do ITIL é que ele oferece um *framework* genérico baseado em experiências práticas de usuários profissionais em uma infra-estrutura de TI.

5.2 O FRAMEWORK ITIL

O *IT Infrastructure Library* (ITIL) é um conjunto de práticas para prover serviços eficientes e efetivos de TI, além do gerenciamento da infra-estrutura de TI.

O desenvolvimento do ITIL foi motivado pelo fato das organizações estarem cada vez mais dependentes de TI para alcançarem os objetivos corporativos traçados. Essa dependência levou a necessidade de serviços de TI com qualidade correspondendo aos objetivos de negócio de cada organização e atingindo os requerimentos e expectativas de seus clientes. Paulatinamente, a ênfase da TI tem mudado do desenvolvimento de aplicações para o gerenciamento de serviços. Os serviços de TI devem ser confiáveis, consistentes, de alta qualidade e com um custo aceitável. Considerando-se o ciclo de vida dos produtos de TI, estima-se que a fase operacional represente 70 a 80% do custo e tempo empregados. Isto demonstra a necessidade de uma gerência de serviços eficiente para garantir o sucesso da área de TI.

O gerenciamento de serviços de TI aborda a provisão e suporte do serviço de TI personalizado às necessidades de cada organização. O ITIL foi desenvolvido para disseminar as melhores práticas em gerenciamento de serviços de TI de forma sistemática e coesa. A abordagem se baseia na qualidade do serviço e no desenvolvimento de processos efetivos e eficientes.

O ITIL oferece um *framework* comum para todas as atividades do departamento de TI, como parte do provimento do serviço, sendo baseado na infra-

estrutura de TI. Estas atividades são divididas em processos, os quais criam um *framework* efetivo para tornar mais maduro o gerenciamento dos serviços de TI. Cada um dos processos cobre uma ou mais atividades pertinentes ao departamento de TI. Esta abordagem de processos permite descrever as melhores práticas de TI de forma independente da estrutura organizacional do departamento de TI.

Muitas destas melhores práticas são claramente identificadas e de fato usadas em alguma extensão pela maior parte das organizações de TI. O ITIL apresenta essas práticas de forma coerente. Os livros do ITIL descrevem como estes processos, algumas vezes identificáveis, podem ser otimizados e como a iteração entre os processos pode ser melhorada. Além disso, explicam como os processos podem ser formalizados dentro da organização. Os livros do ITIL ainda provêm um quadro de referência para a organização com terminologias relevantes, que ajuda a definir os objetivos e determinar o esforço requerido para alcançá-los.

Usando a abordagem de processos, o ITIL primariamente descreve o que deve ser incluído no gerenciamento de TI para prover serviços de TI com a qualidade requerida. A estrutura e alocação de tarefas e responsabilidades entre funções e departamentos dependem do tipo de organização. Estas estruturas normalmente variam entre os departamentos de TI. A descrição da estrutura dos processos provê um ponto em comum de referência que muda lentamente e pode ajudar a manter a qualidade dos serviços de TI durante e depois de reorganizações entre provedores e parceiros.

O ITIL surge em um contexto, onde as tendências de mercado apontam dificuldades crescentes no setor TI, tais como:

- custo crescente da prestação de serviços de TI (entrega e manutenção);
- aumento do nível de exigência quanto a qualidade e justificativa dos recursos empregados nos serviços de TI;
- complexidade crescente da infra-estrutura e mudanças aceleradas em sua composição;
- dependência de diversas áreas do negócio quanto aos serviços prestados pela TI.

As organizações estão cada vez mais dependentes da TI, e esta necessita ter seus objetivos incorporados às necessidades do negócio.

O autor coloca que o ITIL não é uma metodologia, nem fornece um livro de receita. Trata-se de um *framework* não-proprietário e de domínio público. O ITIL não é acadêmico, ele é baseado em exemplos coletados das melhores práticas aplicadas em empresas reais.

A lista que segue identifica algumas vantagens e desvantagens do framework. A lista não é definitiva e depende dos interesses de cada organização e da forma como elas aplicarão o ITIL.

Algumas vantagens do uso do ITIL para os consumidores/usuários finais da TI são:

- O provimento dos serviços de TI torna-se mais focado nos consumidores e acordos sobre o melhoramento na qualidade do serviço melhoram o relacionamento;
- os serviços são mais bem descritos, em linguagem inteligível para o cliente, e em um detalhe apropriado;
- a qualidade e os custos dos serviços são mais bem gerenciados;
- a comunicação com a organização de TI é melhorada pelo acordo através de pontos de contato.

Vantagens observadas para a organização da própria área de TI que utilizar o ITIL são as que seguem:

- A organização da TI desenvolve uma estrutura mais clara, tornando-se mais eficiente e focada nos objetivos corporativos;
- o gerenciamento é mais controlável e mudanças tornam-se mais facilmente gerenciáveis;
- uma estrutura de processos efetiva provê um *framework* para uma efetiva terceirização de elementos de serviços de TI;
- o seguimento das melhores práticas providas pelo ITIL encoraja uma mudança cultural em direção ao provimento de serviço e suporta a

introdução de um sistema de gerenciamento de qualidade baseado na norma ISO-9000, e

- o ITIL provê um quadro de referência para comunicação interna e com os provedores e a padronização e identificação de procedimentos.

Alguns problemas potenciais relativos ao ITIL são:

- a introdução pode tomar um longo tempo e esforço significativo, requerendo uma mudança de cultura organizacional;
- uma ambiciosa introdução pode levar a frustração, porque os objetivos podem nunca ser alcançados;
- se a estrutura do processo torna-se o objetivo final, a qualidade da prestação de serviço pode acabar sendo influenciada;
- a burocracia incluída com processos definidos pode se tornar obstáculo a ser evitado quando possível;
- pode existir nenhuma melhora devido a falta de compreensão sobre o que os processos deveriam prover, quais os indicadores de desempenho chaves e como os processos podem ser controlados;
- o melhoramento na prestação dos serviços e as reduções de custo esperadas são insuficientemente visíveis;
- uma implantação para alcançar sucesso necessita envolvimento e comprometimento de todo o pessoal em todos os níveis da organização, e
- insuficiente investimento em ferramentas de suporte pode acarretar com que os processos não sejam abordados de maneira justa e o serviço de maneira geral não melhore. Recursos adicionais e mão-de-obra extra podem ser necessários se a organização já estiver sobrecarregada pela rotina e atividades do gerenciamento de serviços de TI.

5.3 OS LIVROS DO ITIL - VERSÃO 2

Esta subseção abordará a forma como o ITIL está organizado e, descreverá de forma sucinta, os livros mais conhecidos do ITIL. Convém citar que muitas outras publicações relacionadas estão disponíveis no mercado.

Este trabalho abordará os 7 (sete) principais conjuntos do ITIL, agrupados em seus níveis de atuação conforme ilustrado na Figura 5.1.



Figura 5.1 – Livros do ITIL. (Adaptado de: ITSMF, ITIL, 2003).

Cada livro do ITIL é endereçado a uma parte do *framework*. Cada um provê uma descrição geral do que é necessário para organizar o gerenciamento dos serviços de TI. O ITIL define os objetivos e atividades, as entradas e saídas para os processos de TI. Entretanto, não é uma descrição específica de como deve ser implementado o processo. A ênfase é na abordagem que tem sido aprovada na

prática, mas, que dependendo da circunstância, pode ser implementada de várias maneiras. O ITIL não é um método, mas um *framework* para planejar os processos mais comuns, papéis e atividades, indicando as ligações entre eles e quais linhas de comunicação são necessárias.

O ITIL é baseado na necessidade de se prestar serviços de alta qualidade, com ênfase nas relações com os clientes. A organização de TI deverá cumprir os acordos com o cliente, o que significa manter boas relações com os clientes e parceiros, tais como fornecedores. Parte da filosofia do ITIL é baseada em sistemas de qualidade, como a norma ISO-9000, e *frameworks* de qualidade, como o da *European Foundation for Quality Management* (EFQM). O ITIL suporta tais sistemas de qualidade através de uma descrição clara dos processos e melhores práticas em gerência de serviços de TI, o que poder reduzir significativamente reduzir o tempo requerido para obter as certificações ISO.

Originalmente o ITIL consistia em um grande número de livros núcleo, cada um descrevendo uma área específica de manutenção e operação da infraestrutura de TI. Os livros Suporte de Serviço e Prestação de Serviço são considerados o coração do ITIL. Existem aproximadamente 40 livros complementares que tratam do assunto Gerenciamento de Serviços de TI.

O ITIL se organiza em dois livros núcleo, sendo que um trata de Suporte de Serviço e, outro, Prestação de Serviço. Os cinco elementos básicos principais do *framework* estão ilustrados na Figura 5.2 conhecida como o quebra-cabeça do ITIL. O diagrama tenta ilustrar como os conceitos dentro do ITIL trabalham juntos.



Figura 5.2 – Diagrama do ITIL (Adaptado de: ITSMF, ITIL, 2003).

Os elementos de cada grupo podem ser definidos separadamente, entretanto na prática, ao analisar os processos mais detalhadamente verifica-se que os elementos se sobrepõe em alguma extensão.

Os cinco elementos principais do ITIL são: Suporte de Serviço, Prestação de Serviço, Perspectiva do Negócio, Gerenciamento de Infra-Estrutura de TI e Gerenciamento de Aplicações. Outro elemento existente é o Planejamento para Implementar Gerenciamento de Serviço, o qual explica os passos necessários para identificar como uma organização pode esperar os benefícios do ITIL e como se organizar para repetir estes benefícios.

O quebra-cabeça do ITIL também é comparado a placas tectônicas, ou continentes colidindo e sobrepondo-se, pois é difícil identificar as fronteiras de cada elemento e também existe clara fricção e estresse nessas fronteiras. Na Figura 5.3 pode-se observar a estrutura do ITIL e seus componentes.

Estrutura do Framework ITIL

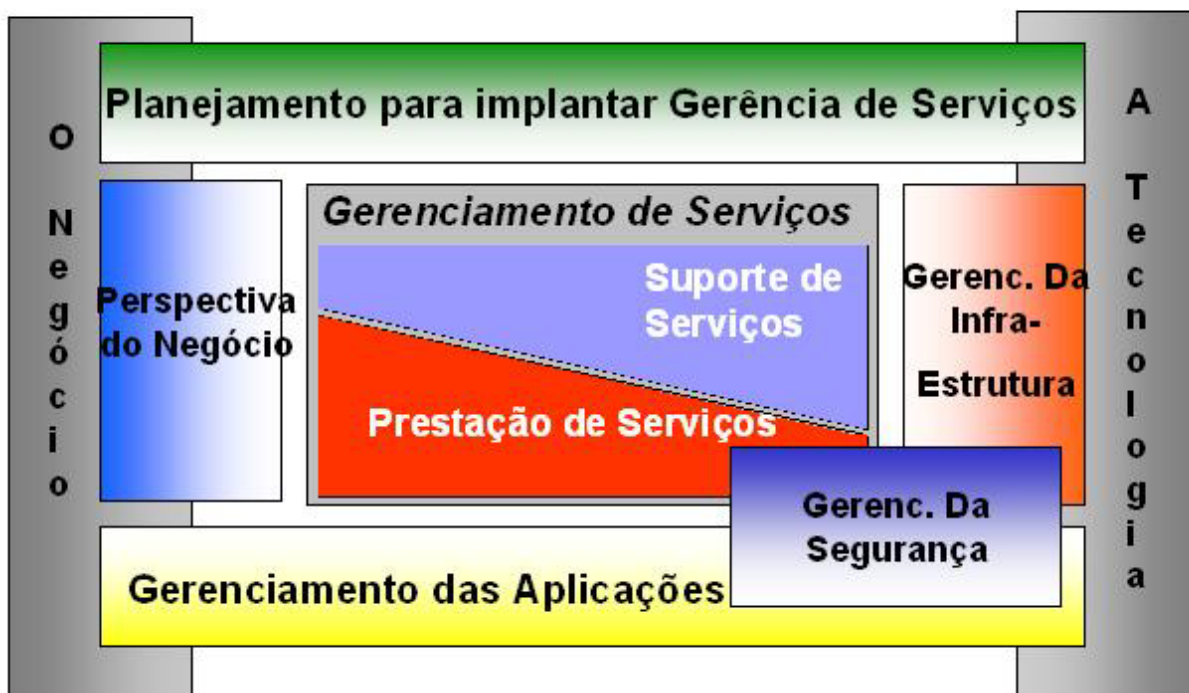


Figura 5.3 – Estrutura do Framework ITIL (Adaptado de: ITSMF, ITIL, 2003).

5.3.1 PRESTAÇÃO DE SERVIÇO

O conjunto de livros Prestação de Serviço juntamente com o Suporte de Serviço, formam o núcleo do ITIL. Este livro descreve os serviços que os clientes requerem e o que é necessário para prestar esses serviços. Os principais objetivos deste conjunto são:

- definir que tipos de serviços e que níveis serão suportados e prestados;
- assegurar que os serviços acordados estão disponíveis dentro dos níveis acordados;
- assegurar que os serviços acordados estão sendo prestados conforme requerido;

- assegurar que os serviços acordados estarão disponíveis em caso de interrupção, como parte do gerenciamento de continuidade dos negócios;
- assegurar que o orçamento, os clientes e a capacidade dos serviços de TI estão definidas.

Os assuntos abordados por este conjunto e que serão tratados nas próximas subseções são: Gerenciamento de Níveis de Serviço, Gerenciamento Financeiro dos Serviços de TI, Gerenciamento de Capacidade, Gerenciamento da Continuidade do Serviço de TI e Gerenciamento de Disponibilidade.

5.3.1.1 Gerenciamento de Níveis de Serviço

O Gerenciamento dos Níveis de Serviço trata do processo de negociação, definição, medição, gerenciamento e aperfeiçoamento da qualidade dos serviços de TI com um custo aceitável. Este tópico aponta como encontrar um balanceamento entre a qualidade e a demanda, a satisfação do cliente e o custo dos serviços de TI.

O principal objetivo do gerenciamento de níveis de serviço é tornar claros os acordos sobre os serviços de TI requeridos pelos clientes e como implementá-los. Conseqüentemente, este Gerenciamento necessita de informações sobre as necessidades dos clientes, facilidades providas pela organização da TI e os recursos financeiros disponíveis. O foco deste processo é o cliente e os serviços providos são dirigidos para as necessidades do consumidor final.

Este capítulo do livro *Prestação de Serviços* inclui o design, concordância e manutenção de SLA's (*Service Level Agreement*), OLA's (*Operational Level Agreements*), UC's (*Underpinning Contracts*), Planos de Qualidade de Serviço e descreve ainda:

- como um SLA claramente definido pode otimizar os serviços de TI com um custo justificável para o cliente;
- como o serviço pode ser monitorado e discutido;
- os serviços são suportados por fornecedores e contratos secundários.

O Gerenciamento de Níveis de Serviços é o processo que liga o provedor de serviços de TI ao cliente dos serviços. Dentre seus objetivos pode-se citar:

- Integrar os elementos requeridos para provisão de serviços;
- criar documentos que descrevam claramente os serviços e seus vários elementos;
- descrever o serviço prestado ao cliente em uma terminologia que ele compreenda e possa relatar;
- alinhar as estratégias da TI com as necessidades do negócio;
- aperfeiçoar a Prestação de Serviços da TI de forma organizada.

Na descrição do processo o ITIL coloca, de forma clara, as atividades envolvidas no processo, como ele se relaciona com os outros processos e livros, as atividades envolvidas em sua execução, os custos e possíveis problemas que podem surgir, além dos controles necessários em seu gerenciamento.

5.3.1.2 Gerenciamento Financeiro para os Serviços de TI

O Gerenciamento Financeiro caracteriza-se por controlar os recursos monetários na sustentação dos objetivos organizacionais, assegurando que as atividades se acoplem para atender as exigências definidas na gerência do nível de serviço e que estejam justificadas quanto ao custo e ao orçamento.

Observa-se no mercado, de forma crescente, que os negócios estão cada vez mais dependentes da TI para suportar suas operações. Como consequência, o número de clientes finais da TI foi dramaticamente incrementado, assim como o total de recursos financeiros empregados em seus processos (orçamento da TI).

Proporcionalmente ao alto investimento na área, aumentou também a cobrança das áreas clientes por aumento da qualidade e o incremento da eficiência dos serviços providos pela TI.

A dificuldade encontrada pelas organizações de TI consiste em expor de forma clara e linguagem não-técnica para as demais áreas envolvidas no negócio e para os clientes em geral, os custos reais e benefícios dos serviços prestados.

Geralmente, os clientes e administradores ficam relutantes em investir em serviços de TI, visto que não possuem uma visão clara dos custos envolvidos e dos benefícios gerados para o negócio. O Gerenciamento Financeiro para os Serviços de TI do ITIL, tem como objetivo tornar os custos claros, estabelecer um método de cobrança e proporcionar aos clientes uma idéia sobre a relação qualidade/preço. Em outras palavras, o Gerenciamento Financeiro promove a execução dos serviços de TI como uma operação do negócio.

O ITIL foi projetado para gerenciar a infra-estrutura de TI promovendo o uso econômico e eficiente dos recursos de TI. Prover serviços de TI com custos razoáveis depende de três fatores: **qualidade** (em termos operacionais de capacidade, disponibilidade, performance, contingência e suporte), **custo** (em termos de investimento e despesa) e **requerimentos do cliente** (o custo e a qualidade devem estar alinhados com as necessidades dos negócio e do cliente). Os dois primeiros fatores estão constantemente em conflito, já que incrementar a qualidade normalmente significa aumentar o custo, enquanto reduzir custos normalmente está associado a diminuir a qualidade. Contudo, estes dois fatores podem ser balanceados quando o foco está nas necessidades do cliente.

O Gerenciamento Financeiro objetiva auxiliar o setor de TI com um gerenciamento efetivo do custo dos recursos de TI requeridos para a provisão dos serviços. Por esta razão, o processo tende a promover uma ruptura no custo dos serviços da TI, associando- os com os vários serviços prestados. Assim, o processo de tomadas de decisões referentes ao investimento em TI torna-se mais simples.

Os principais objetivos da implantação do Gerenciamento Financeiro são:

- determinar os custos dos serviços de TI;
- identificar e classificar a estrutura de custos;
- alocar razoavelmente os custos dos serviços de TI prestados para clientes internos e externos;
- introduzir métodos de cobrança para o uso dos serviços de TI quando necessário;
- operar o departamento de TI como uma unidade do negócio quando requerido;

- recuperar todos os custos, incluindo custos de capital (investimento, depreciação, reembolso e interesses) do cliente;
- checar as cobranças em intervalos regulares para determinar se elas estão realísticas e aceitáveis;
- estabelecer um mapa do comportamento dos clientes e usuários, construindo uma consciência dos custos e amarrando os custos diretamente aos serviços.

Os principais benefícios da Gerência Financeira de TI para os serviços de TI são:

- a contabilidade de TI suporta a Gerência de Serviços de TI;
- situação dos custos dos serviços de TI individualmente;
- facilidade nas decisões essenciais sobre os serviços prestados pela TI e os investimentos requeridos;
- dados para justificar as despesas;
- facilidade na elaboração de planejamentos e orçamentos;
- visão geral dos custos oriundos de falhas de serviço, como uma base para a justificativa de despesas no planejamento estratégico;
- os usuários podem acompanhar os custos dos serviços que estão utilizando.

Os fatores críticos de sucesso para a Gerência Financeira dos serviços de TI são:

- envolver peritos financeiros/contabilidade no processo;
- conectá-lo com os outros processos da Gerência de Serviços de TI;
- a monitoração do custo deve fornecer detalhes e justificativas da despesa;
- a gerência da organização deve estar inteiramente ciente do impacto e dos custos da introdução da gerência financeira na TI e deve estar comprometida com este aspecto;

- a Gerência de Configuração deve prover informações relevantes sobre a estrutura dos serviços para que uma contabilidade apropriada seja executada;
- os resultados dos serviços devem ser direcionados para os clientes.

Os principais possíveis problemas na implantação da Gerência Financeira de TI são:

- as atividades requeridas para a implantação e monitoramento dos custos são freqüentemente um assunto novo para o pessoal de TI e deve ser introduzido aos poucos;
- é difícil encontrar mão-de-obra familiarizada com aspectos técnicos de TI e contabilidade;
- os sistemas, possivelmente, não foram desenvolvidos/documentados claramente e torna-se difícil considerar os investimentos necessários;
- os benefícios do processo freqüentemente não são compreendidos de forma suficiente, tendo por resultado uma cooperação insuficiente dos envolvidos.

5.3.1.3 Gerenciamento da Capacidade

O Gerenciamento da Capacidade busca assegurar que todos os aspectos atuais e futuros da infra-estrutura de TI, conseguem atender as demandas do negócio da maneira mais econômica, efetiva e oportuna possível. Trata-se de um processo de otimização do custo, tempo de aquisição e implantação dos recursos de TI para suportar os acordos com os clientes.

Este gerenciamento compreende diversas sub-atividades ou sub-processos, dentre eles destaca-se: gerenciamento de recursos, gerenciamento de desempenho, gerenciamento de demanda, modelagem, plano de capacidade, gerenciamento de capacidade, gerenciamento de carga e dimensionamento de aplicações.

As responsabilidades desta gerência envolvem:

- monitorar o desempenho e as saídas dos serviços de TI;

- empreender atividades de ajuste, tornando o uso dos recursos mais eficiente;
- compreender as demandas correntes, que estão sendo direcionadas para os atuais recursos de TI e produzir previsões para as exigências futuras;
- ajudar a influenciar/justificar as demandas de recurso, conjuntamente com a Gerência Financeira;
- produzir um Plano de Capacidade, predizendo os recursos de TI necessários, que permitirão fornecer serviços da qualidade definida nas SLAs.

O Gerente da capacidade de controlar os processos e assegurar-se de que o Plano de Capacidade esteja desenvolvido e atualizado, assegurar que as bases de dados da capacidade esteja atualizadas e que os relatórios requeridos são produzidos.

Os benefícios da aplicação desta gerência envolvem:

- os recursos são controlados eficazmente, e o desempenho do equipamento é monitorado continuamente;
- o impacto de aplicações novas/modificadas em sistemas existentes é conhecido;
- os investimentos são feitos em um tempo apropriado, nem demasiado cedo, nem demasiado tarde;
- necessidade de mudanças urgentes resulta de estimativas incorretas da capacidade;
- eficiência alta e demandas prioritárias são equilibradas e avaliadas com antecedência;
- as despesas controladas, ou mesmo reduzidas, *capacity-related* como a capacidade, são usadas mais eficientemente ;
- os gastos com recursos de capacidade, assim como o custo dos recursos existentes, é mais eficiente, ou mesmo reduzido, quando gerenciado.

Os fatores críticos de sucesso, na implantação da Gerência de Capacidade são:

- realizar previsões exatas do negócio;
- é necessário ter conhecimento da estratégia da TI e dos planos estabelecidos; sendo necessário que eles sejam precisos;
- é necessário haver uma compreensão das tecnologias atuais e futuras;
- habilidade em demonstrar a relação custo X eficiência é requerida;
- necessidade de interação com outros processos eficazes da gerência de serviço;
- necessidade de habilidade em planejar e executar a Capacidade de TI apropriada para satisfazer os requerimentos do negócio.

5.3.1.4 Gerenciamento da Continuidade dos Serviços de TI

Trata-se do processo de planejamento e coordenação técnica, financeira e gerenciamento de recursos requeridos para garantir a continuidade dos serviços após um desastre, conforme acordado com o cliente.

Este gerenciamento concentra-se em controlar a habilidade de uma organização de continuar a fornecer um pré-determinado e acordado nível de serviços de TI para suportar as exigências mínimas do negócio quando da ocorrência de interrupção/sinistro. O processo está focado na preparação e planejamento de medidas para recuperação de desastres nos serviços de TI, em um evento de interrupção do negócio.

O objetivo principal é suportar a gerência total da continuidade do negócio, assegurando que a infra-estrutura de TI e os serviços de TI requeridos, incluindo suporte, podem ser restaurados em um tempo limite especificado, após o desastre.

As responsabilidades desta gerência envolvem:

- avaliar o impacto da interrupção dos serviços de TI após um desastre;
- identificar os serviços críticos para o negócio, que requerem medidas de prevenção adicionais;

- definir os períodos para que os serviços sejam restaurados;
- definir a abordagem a ser usada para restaurar os serviços;
- desenvolver, testar e manter um plano de recuperação, com detalhes suficientes para sobreviver a um desastre e para restaurar os serviços normalmente após um período definido.

Os benefícios principais da aplicação desta gerência são:

- gerência do risco e a redução conseqüente do impacto da falha;
- aderência aos requerimentos dos órgãos reguladores;
- possível economia quando do contrato de seguros;
- desenvolvimento de uma abordagem mais pró-negócio durante a recuperação do desastre;
- redução na interrupção do negócio durante um incidente;
- aumento da confiança do cliente e credibilidade organizacional.

Os fatores críticos de sucesso envolvem:

- um processo eficaz de Gerência de Configuração (ver descrição desta no detalhamento do conjunto Suporte de Serviços);
- sustentação e compromisso da organização;
- ferramentas eficazes e atualizadas;
- treinamento dedicado para todos os envolvidos nos testes regulares;
- realização de testes periódicos do plano de recuperação.

5.3.1.5 Gerenciamento da Disponibilidade

O objetivo deste processo é garantir uma implantação dos recursos de TI apropriada, além de métodos e técnicas, para suportar a disponibilidade acordada com os clientes dos serviços de TI. Estão envolvidas atividades como a otimização da manutenção e a avaliação de medidas para minimizar o número de incidentes. Assim, pretende-se atingir um nível eficaz e sustentável de disponibilidade, que permita atender aos objetivos do negócio.

Este capítulo oferece várias técnicas e métodos auxiliares na definição dos níveis de disponibilidades necessários, citamos: *Component Failure Impact Analysis (CFIA)*, *Fault Tree Analysis (FTA)*, *CCTA Risk Analysis Management Method (CRAMM)*, *Service Outage Analysis (SOA)*, *Technical Observation Post (TOP)*.

As responsabilidades desta gerência envolvem:

- determinar as exigências de disponibilidade em termos do negócio;
- prever e projetar a disponibilidade para níveis aceitáveis;
- otimizar a disponibilidade com monitoramento e relatórios;
- produzir um Plano de Disponibilidade e estabelecer prazos para as melhorias.

Os benefícios principais da aplicação desta gerência são:

- define exigências fundamentais do negócio para a disponibilidade;
- projeta os serviços para atender as exigências;
- fornece uma disponibilidade com custo justificável;
- avalia a disponibilidade necessária para suportar os SLAs;
- reduz a incidência de interrupções do serviço.

Os fatores críticos de sucesso envolvem:

- os objetivos de disponibilidade do negócio devem estar claramente definidos,
- a Gerência do Nível de Serviço deve ter sido ajustada para formalizar os acordos;
- o negócio e a área de TI devem estar cientes dos benefícios da Gerência de Disponibilidade.

5.3.2 SUPORTE DE SERVIÇO

Este livro descreve os processos associados com o suporte rotineiro e a manutenção das atividades associadas com a prestação dos serviços de TI. Os

assuntos abordados por este conjunto e que serão tratados nas próximas subseções são: Atendimento ao Cliente, Gerenciamento de Incidentes, Gerenciamento de Problemas, de Configuração, de Mudanças e de Versões.

Os principais objetivos deste conjunto são:

- resolver os incidentes conforme sua ocorrência;
- identificar as causas principais dos incidentes e submeter RFC's (*Request for changes*) para solucioná-las;
- unificar e centralizar os contatos com os usuários dos serviços da TI;
- assegurar que métodos padrões e procedimentos são aplicados para tratamento das fragilidades detectadas;
- gerenciar as versões de hardware e software como partes do gerenciamento de Mudanças efetivo;
- gerenciar informações técnicas considerando a versão, estado, proprietários e relacionamentos entre os recursos de TI.

5.3.2.1 Serviço de Atendimento ao Cliente

O ITIL considera este tópico como uma função e não um processo. Seu objetivo é fornecer um ponto central estratégico de contato com os cliente e um único ponto operacional de contato para incidentes e soluções. Além disso, o Atendimento ao Cliente manipula as solicitações de serviço.

As atividades envolvidas neste processo são:

- melhorar os serviços em benefício do negócio;
- fornecer orientação aos clientes;
- fornecer restauração rápida dos serviços;
- realizar as expectativas acordadas nos SLA's;
- comunicar e promover os serviços da TI;

Os benefícios principais da aplicação deste processo são: a melhora do serviço prestado ao cliente, facilidade nos acessos aos serviços, com a unificação do ponto de contato, e as melhorias na comunicação com a área de TI e dentro dela.

Os fatores críticos de sucesso envolvem a resistência para seguir os procedimentos, a possível sobrecarga no setor de TI, a falta de uma política organizacional adequada e a comum dificuldade de comunicação encontrada na área de TI.

5.3.2.2 Gerenciamento de Incidentes

O objetivo deste processo é restaurar a operação normal dos serviços tão rápido quanto possível e minimizar o impacto adverso nos negócios. Este processo considera que um incidente é qualquer evento fora do padrão de operações de um serviço e que causa, ou pode causar, uma interrupção ou redução na qualidade daquele serviço.

Sob a ótica do negócio, a implantação desta gerência agrega os seguintes benefícios: redução do impacto de incidentes no negócio e identificação pró-ativa de incidentes.

Sob a ótica da TI, a implantação desta gerência agrega os seguintes benefícios: aumento do monitoramento das SLA's, melhora na documentação de incidentes e utilização deste conhecimento para ganho de eficiência.

Os fatores críticos de sucesso envolvem a possível inexistência de um responsável por gerenciar e documentar os incidentes, a falta de conhecimento para resolução dos incidentes, treinamento inadequado, falta de integração com os outros processos e a não provisão de níveis de serviço adequados.

5.3.2.3 Gerenciamento de Problemas

O objetivo deste processo é minimizar o impacto adverso no negócio, de incidentes e problemas causados por erros na infra-estrutura de TI e prevenir a reincidência destes erros. O Gerenciamento de Problemas busca encontrar a causa principal dos problemas e iniciar a ação que eliminará o erro.

Esta gerência considera um problema uma condição identificada de múltiplos incidentes que exibem sintomas comuns ou um único incidente bastante significativo, que indica um erro cuja causa é desconhecida.

A implantação desta gerência agrega os seguintes benefícios: manipulação mais eficiente e efetiva dos incidentes, incremento na qualidade dos serviços, redução no número de problemas e incidentes e desenvolvimento de soluções permanentes.

Os fatores críticos de sucesso envolvem a implantação de um procedimento de controle de incidentes, processos de avaliação e implantação de uma base de conhecimento.

5.3.2.4 Gerenciamento de Mudanças

O objetivo deste processo é assegurar que métodos e procedimentos padronizados estão sendo utilizados para a manipulação eficiente de todas as mudanças, minimizando o impacto dos incidentes relacionados às mudanças e aprimorando as operações diárias.

Este gerenciamento considera que uma mudança é uma ação que resulta em um novo estado para um ou mais itens da configuração da infra-estrutura de TI, sendo que é preciso garantir que as mudanças ocorram de forma organizada e coordenada, seguindo-se um caminho de definição, planejamento, construção e teste, aceitação, implementação e avaliação.

A implantação desta gerência agrega os seguintes benefícios: melhora no alinhamento dos serviços prestados pela TI com os requerimentos do negócio; garantias de que todas as mudanças serão formalmente aprovadas, diminuição das chances de problemas durante o processo de mudança, aumento da produtividade dos usuários e aumento da capacidade de gerenciar um grande número de mudanças ao mesmo tempo.

Os fatores críticos de sucesso envolvem a visão de que este pode ser um processo puramente burocrático, dificuldades culturais em aceitar o gerenciamento de mudanças, falta de auditorias que verifiquem a conformidade do processo do Gerenciamento de Mudanças e a caracterização de todas as mudanças como urgentes.

5.3.2.5 Gerenciamento de Versões

O objetivo deste processo é garantir o sucesso no lançamento de versões, incluindo integração, teste e armazenamento. Esta gerência garante que somente versões corretas e testadas de software e hardware autorizados são entregues, estando profundamente relacionada às atividades de Gerenciamento de Configuração e Mudanças. A entrega de versões é vista como uma mudança para um serviço de TI e é necessário assegurar que todos os aspectos, técnicos ou não, são considerados juntos.

As versões com classificadas em categorias que podem ser: versão completa, versão delta, pacote de versões, versão emergencial ou de política.

A implantação desta gerência agrega os seguintes benefícios: aumento da consistência no processo de atualização de versões, melhora dos níveis de expectativas, manutenção de um histórico de dados relacionados às versões lançadas, redução no risco de versões não autorizadas ou *softwares* ilegais.

Os fatores críticos de sucesso envolvem a resistência inicial às mudanças, responsabilidades não estabelecidas e formalizadas e a pressão por mudanças e liberações rápidas de versões.

5.3.2.6 Gerenciamento de Configuração

O objetivo deste processo é garantir o controle da mudança na infraestrutura de TI, através de padronização e monitoramento. Esta gerência realiza a identificação dos itens de configuração (inventário, ligações mútuas, verificação e registro) e coleta/gerencia a documentação sobre a infra-estrutura de TI, provendo informação para todos os outros processos. Este processo requer a implantação de um CMDB – Base de dados da gerência de configuração, onde todos os itens da infra-estrutura que pertencerem ao escopo deste processo devem ser armazenados e gerenciados.

A implantação desta gerência agrega os seguintes benefícios: disponibilidade de informação precisa e atualizada sobre os itens de configuração, aderência às obrigações legais, contribuição ao plano de continuidade dos serviços, auxílio no planejamento financeiro.

Os fatores críticos de sucesso envolvem o nível de comprometimento da gerência e o detalhamento exagerado dos processos.

5.3.2 PERSPECTIVA DO NEGÓCIO

Este conjunto de livros do ITIL descreve muitos assuntos relacionados a compreensão e apreciação de serviços de TI como um aspecto integrado da gerência do negócio. O conjunto Perspectivas do Negócio, assim como o livro de mesmo título (que eventualmente refere-se ao conjunto) trata dos seguintes assuntos: Gerenciamento de Continuidade de Negócio, Parcerias e Terceirização, Sobrevivência à Mudanças e Adaptação do Negócio à Mudanças Radicais. Outros livros que abordam alguns aspectos deste elemento são o de Gerenciamento da Gestão de Facilidades e o de Gerenciamento da Gestão de Fornecedores.

5.3.3 GERENCIAMENTO DE INFRA-ESTRUTURA DE TI - ICT

O ICT – *Information & Communications Technology Infrastructure Management* cobre todos os aspectos do gerenciamento da infra-estrutura de informações e comunicações, desde a identificação dos requerimentos do negócio, os testes, instalações, distribuição, operação e otimização dos componentes da infra-estrutura de TI e seus serviços. Alguns assuntos que são tratados neste contexto são o planejamento e controle das redes e comunicações da organização, a operacionalização dos serviços de TI, o gerenciamento das instalações, equipamentos e processos correlatos.

O conjunto descreve a maioria dos processos envolvidos no gerenciamento de todas as áreas e aspectos da TI e inclui os livros : Gerenciamento e Administração, Planejamento e Projeto, Operações, Suporte Técnico e Distribuição.

Um gerenciamento sólido desta infra-estrutura é essencial para o bom funcionamento do conjunto de processos Gerenciamento de Serviços. Esta gerência busca transmitir os requerimentos do cliente para uma estruturada e gerenciada

estrutura de serviços de TI (Prestação de Serviços) e controlar a prestação de serviços de infra-estrutura para o cliente (Suporte de Serviços).

Dentre os benefícios da aplicação desta gerência estão: melhor coordenação entre os planos de negócio e as atividades, ganho de produtividade proporcional ao bom gerenciamento da infra-estrutura, diminuição do custo e ganho de eficiência para os serviços prestados, melhor gerenciamento da informação acerca dos serviços e processos do negócio, diminuição do risco de falhas dos serviços, aumento da capacidade de implementação de projetos e mudanças, melhor controle dos serviços terceirizados e sua performance.

5.3.4 GERENCIAMENTO DAS APLICAÇÕES

O gerenciamento de aplicações no contexto do ITIL é considerado como um gerenciamento de ativos que deve assegurar que os sistemas de informação da organização podem responder com flexibilidade às mudanças de mercado. Os objetivos desta gerência subdividem-se em: selecionar a abordagem estratégica apropriada entre os processos do negócio e as aplicações; e assegurar que a organização da TI pode gerenciar as aplicações durante seu ciclo de vida.

Dentre os benefícios da aplicação desta gerência estão: melhor controle dos processos de TI sobre o ciclo de vida dos aplicativos, garantindo que estejam alinhados com as regras estabelecidas pela organização e assegurando que os investimentos corretos estão sendo efetuados e facilidade da definição de estratégias de testes e mudanças.

Os principais processos envolvidos são: suporte ao ciclo de vida do aplicativo e testes dos serviços operacionais de TI.

A atividade de suporte objetiva acompanhar todo o ciclo de vida do *software*, incluindo o projeto, construção, teste, instalação, operação, manutenção e, eventualmente, o desuso. Além disso, a seleção de um modelo de ciclo de vida de *software* pode impactar significativamente os serviços de TI. Os testes visam garantir que a operação apropriada de serviços de TI, novos ou modificados, esteja testada

antes de entrar em operação. Alguns testes podem ser realizados para validação da aplicação, tais como de sistema, instalação e aceitação de usuário.

5.3.5 GERENCIAMENTO E ORGANIZAÇÃO

Este conjunto do ITIL inclui alguns livros que se concentram em assuntos de nível estratégico, como o desenvolvimento de políticas e planejamento de longo prazo para os serviços de TI. Além desses tópicos são abordados ainda: a qualidade no gerenciamento de serviços de TI, a organização dos serviços de TI e o planejamento e controle dos serviços de TI.

A atividade de qualidade no gerenciamento de serviços de TI relaciona os padrões ISO-9000 com os módulos do ITIL e aborda a introdução de um sistema de qualidade na organização incluindo como definir e implementar a política de qualidade e o gerenciamento do sistema de qualidade, incluindo auditorias.

A organização de serviços de TI trata da estrutura da organização de TI, descrevendo como a organização pode ser analisada e avaliada, particularmente em termos de atividades, autoridade e responsabilidade. As principais atividades do processo de organização incluem a determinação e definição da estrutura organizacional e a descrição de papéis e funções.

O planejamento e controle dos serviços de TI objetiva prover um sistema coerente de planejamento, relatório e controle da organização de TI para garantir que a organização atinja seus objetivos e requerimentos baseado nas estratégias de negócio e da TI, o que inclui a coordenação do planejamento e reporte de vários processos de gerenciamento de serviços de TI.

5.3.6 PLANEJAMENTO E IMPLEMENTAÇÃO

Este conjunto trata do planejamento e implementação de processos de otimização do gerenciamento de serviços de TI na organização. Considera aspectos

como onde e quando começar, cultura organizacional, planejamento de projetos e programas, definições de processos e otimização de performance.

O processo de análise das necessidades da organização e implementação das soluções requeridas requer que a organização se prepare para isso. Analisar as necessidades da organização e implementar a solução necessária pode requerer a criação de uma organização temporária. Isto pode ser considerado como um projeto ou uma série de projetos em um programa de implantação. Uma vantagem é que este processo permitirá à organização estar apta a perceber pontos claros de decisão para identificar os processos que devem ser eliminados, continuados ou modificados no projeto. Neste contexto os livros do ITIL recomendam a adoção de metodologias de gerenciamento de projetos, como o PRINCE2 (*Projects In Controlled Environments*).

Cada projeto é baseado numa análise da situação atual, a situação desejada e o caminho entre ambas. Na maioria dos casos, as alternativas serão comparadas baseando-se em requisitos como: vantagens para a organização, riscos, obstáculos, problemas potenciais, custos transitórios, custos de longa duração e custos de continuar a abordagem atual.

5.3.7 GERENCIAMENTO DA SEGURANÇA

Este conjunto trata do planejamento e implementação de níveis de segurança na organização, tal que estejam de acordo com a disponibilidade da infraestrutura e dos serviços de TI, assim como com os processos do negócio, sem comprometê-los. Esta atividade busca ainda, assegurar que a segurança esteja de acordo com os requerimentos legais, políticas de privacidade e as SLA's.

Fazem parte deste processo o estudo das demandas de segurança, vulnerabilidade, relacionamentos com terceirizados e fornecedores, riscos de segurança e definição de uma estratégia de segurança. O processo do gerenciamento de segurança é flexível e necessita ser revisado continuamente para assegurar que está atualizado, devendo ser planejado, executado e monitorado como um ciclo contínuo.

6 ANÁLISE DO *FRAMEWORK* COBIT

O COBIT é considerado a metodologia base para a governança de TI, projetado para ser uma ferramenta de gestão da área de Tecnologia da Informação que ajuda a compreender e gerenciar os riscos e benefícios associados com a informação e relacionados com TI (ITGI, 2000).

Conforme exposto no capítulo 4, o COBIT não determina como os processos devem ser estruturados, e sim os controles que eles devem possuir para que TI cumpra seus objetivos em termos de governança, ou seja: alinhamento e entrega de valor por parte da área de TI para o negócio; correta alocação e medição dos recursos envolvidos; a mitigação dos riscos em TI.

Originalmente uma ferramenta de auditoria, o COBIT é usado para avaliar o alinhamento estratégico da tecnologia com as áreas de negócio, aprimorando os processos desde a alta direção da empresa até o departamento de TI e auxiliando a associação entre os riscos de negócio, as necessidades de controle e os aspectos tecnológicos.

Não existem dúvidas sobre o benefício da tecnologia aplicada aos negócios. Entretanto, para serem bem sucedidas, as organizações devem compreender e controlar os riscos associados no uso das novas tecnologias. O COBIT é uma ferramenta eficiente para auxiliar o gerenciamento e controle das iniciativas de TI nas empresas (FAGUNDES, 2004).

O principal objetivo do COBIT é pesquisar, desenvolver, publicar e promover um conjunto atualizado, autorizado e com foco internacional, de objetivos de controle geralmente aceitos e aplicáveis à TI para o uso por gestores de TI, administradores, usuários e auditores de sistemas (ITGI, 2000).

O COBIT pode ser considerado como um caminho para a governança de TI, devendo ser adaptado à real situação da organização onde será implantado. Em sua essência, sua implantação consiste na determinação de controle de objetivos que determinam o que deve ser executado e supervisionado (CAMPBELL, 2006).

A estrutura do COBIT cobre todos os aspectos da tecnologia da informação, além do detalhamento dos processos. Cada um dos 34 processos de alto nível está associado às Diretrizes de Auditoria (*Audit Guidelines*) para facilitar a revisão dos processos de TI e dos 318 objetivos de controle detalhados e recomendados pelo COBIT (ITGI, 2000).

Para conseguir obter benefícios do COBIT, é preciso entender suas competências e avaliar as evoluções. A correta utilização de suas diretrizes pode ajudar os gestores de TI a atingir suas metas, integradas com as metas da empresa. Os guias de gerenciamento do COBIT se baseiam na administração da qualidade e performance dos serviços prestados pela área de TI, utilizando os fundamentos do *Balanced Scorecard* (CACIATO, 2005).

Alguns *cases* de aplicação de COBIT com sucesso conhecidos:

- A **Sun Microsystems** – multinacional americana – utilizou o COBIT para atingir a conformidade SOX e alinhar os objetivos da TI ao negócio (ISACA, 2007);
- A **Unisys** - multinacional americana - utilizou o COBIT para padronizar a estratégia de TI visando suportar as operações globais da empresa, alinhar a infra – estrutura da TI ao negócio e obter a conformidade SOX (ISACA, 2007);
- A **Curtin University** – universidade australiana – a equipe de auditoria de sistemas adotou o COBIT como padrão e obteve bons resultados na organização da área de TI e economicidade nos processos (ISACA, 2007);
- A **Harley-Davidson** - multinacional americana – utilizou o COBIT para otimizar o gerenciamento de TI, auditoria e controles internos e obteve resultados significativos na gerência de riscos (ISACA, 2007);
- A **WEG** Equipamentos Elétricos realizou uma avaliação de maturidade em seus controles e processos de TI através do COBIT, e obteve como resultados a identificação do nível de maturidade atual e o desejado para a empresa, a definição de uma matriz de prioridades para atuar

naquelas atividades que gerassem um melhor retorno e a elaboração de um plano de ação baseado nas não conformidades (CNASI,2007).

- A **Dell Computer** usa o COBIT como parte da sua política corporativa *Control Self-Assesment* (CSA), um conjunto de controles e verificações que ajudam a companhia a manter sua alta qualidade (MORAES,2006);

Como principais resultados da aplicação do COBIT citamos: otimização da gestão e controle do ambiente de TI, melhor distribuição das responsabilidades, levantamento detalhado dos processos, facilidade da análise da relação custo x benefício, levantamento dos indicadores de desempenho, levantamento dos fatores críticos de sucesso, levantamento dos riscos e identificação do nível de maturidade dos processos.

7 ANÁLISE DO *FRAMEWORK* ITIL

O ITIL tem sido utilizado em diversos setores atuantes na área de TI como um guia, um modelo para a gestão de serviços também aplicado em consultoria, educação, suporte e auditoria. Seu foco é a infra-estrutura, concentrando-se em seis domínios de atuação: prestação de serviços, suporte, gerenciamento de infra-estrutura (hardware) e aplicações (software), alinhamento aos objetivos do negócio e serviços de TI. Trata-se de uma ferramenta útil, proporcionando identificação, organização, otimização e padronização dos processos envolvidos nestas seis esferas.

Os principais objetivos do ITIL são: fornecer um guia para a gestão estratégica, tática e operacional da infra-estrutura de TI, melhorar a eficiência dos processos, reduzir riscos, prover compatibilidade com os requerimentos das normas e melhores práticas do mercado.

Segundo Lorenzato (apud Ferreira, 2005), o ITIL é uma cartilha do bom senso na administração de TI, não sendo necessário implementar tudo o que o modelo apresenta e sim apenas o essencial para a empresa e seus negócios.

Através da aplicação do ITIL, a área de TI passa a conhecer o impacto que pode provocar na organização e a disponibilidade dos recursos passa a ser transparente para os clientes (FERREIRA, 2005).

O ITIL funciona de maneira horizontal, ou seja, no departamento de TI. Em alguns casos pode atingir as áreas de negócios pelos processos combinados entre os departamentos, obtendo integração e sinergia, este padrão de documentação de hardware, software, procedimentos e processos é o TOP do momento e cada vez mais empresas buscam conhecer seus benefícios (INFO CORPORATE, 2007).

A utilização do ITIL para gestão dos serviços de TI não obriga a adoção de uma nova maneira de gerir o negócio da empresa. A utilização do *framework* apenas fornece uma plataforma onde encaixar as atividades, métodos e processos existentes em um contexto estruturado.

O ITIL mostra-se bastante eficaz também na implantação de processos pontuais. Ricardo Mansur (2004) aplicou o modelo na implantação de um sistema de inventário, com prazo de dois dias, e o resultado demonstrou que diversos aplicativos não estavam em uso pela empresa e que as licenças poderiam ser disponibilizadas para os usuários que estavam solicitando a aquisição destes produtos – proporcionando a racionalização dos recursos.

Alguns cases de aplicação de ITIL com sucesso conhecidos:

- A **Procter & Gamble** – multinacional americana - que inicialmente reduziu em 10% as chamadas no *HelpDesk* após implantação do ITIL e em um segundo momento do projeto reduziu entre 6 e 8% os custos operacionais de tecnologia (ITIL SURVIVAL, 2007);
- A **Cartepillar** – multinacional americana - que após aplicar os princípios de ITIL aumentou de 60 para 90% o nível de acerto do *Helpdesk* para os incidentes (MANSUR,2004);
- A **Mead** e a **Westvaco** - as duas maiores empresas de embalagens e produtos químicos dos Estados Unidos - se fundiram em 2002 e Jim McGrane (CIO da empresa) formalizou um plano de reconstruir seu departamento de TI usando ITIL. Como resultado eliminou mais de 100 mil dólares anuais em contratos de manutenção de TI e obteve 10% de aumento na estabilidade operacional (MANSUR,2004);
- Na **Pershing**, empresa norte-americana de serviços financeiros, que adotou o ITIL em janeiro de 2004, desde que o *Helpdesk* foi estruturado seguindo as diretrizes do ITIL, o tempo de resposta a incidentes caiu 50% (COMPANYWEB *apud* CIO,2007);
- O **Governo de Ontario**, Canadá, adotou ITIL para melhorar o serviço de 25.000 usuários em 1.000 locais. Criou um *service desk* que melhorou a resposta e reduziu os custos com chamados em 40% (MORAES,2006);
- O **ABN Amro Bank** iniciou a aplicação do ITIL em 2001 – *datacenter* e implantação de equipamentos do banco, incluindo agências. Promoveu a centralização do *help-desk* com aumento de chamados de 20.000

para 60.000 (aumentou o controle, não os chamados), teve seu tempo de atendimento reduzido em 20%, volume de reclamações reduzido em 80% e 94% dos atendimentos completados em menos de 20 segundos (MORAES,2006);

- A **UNICEF** implantou o ITIL com foco na gerência de infra-estrutura e através da coleta sistemática de dados, monitoramento de chamadas e gestão de problemas conseguiu com que os recursos fossem direcionados para as áreas que exigem correção rápida e eficaz (WEILL; ROSS, 2006).

Como principais resultados da aplicação do ITIL, citamos: fortalecimento dos controles e da gestão dos ambientes de TI; orientação a processos com significativa redução nos tempos de execução e distribuição de serviços; diminuição gradativa da indisponibilidade dos recursos e sistemas de tecnologia da informação; causados por falhas no planejamento das mudanças e implantações em ti; elevação dos níveis de satisfação dos usuários internos e clientes com relação à disponibilidade e qualidade dos serviços de TI; redução dos custos operacionais de TI; reconhecimento da capacidade de gerenciamento pelos acionistas, colaboradores e clientes.

8 ANÁLISE COMPARATIVA DOS *FRAMEWORKS* COBIT E ITIL

Atualmente a TI dirige os negócios para diversas organizações em variados setores da economia. O sucesso da empresa no mercado depende da alta disponibilidade, segurança e desempenho dos serviços de TI. Esta dependência determinou o desenvolvimento de ferramentas, técnicas e metodologias que propõem práticas para implantação da governança e gestão eficaz dos serviços de TI. O crescimento dos investimentos, aumento das exigências dos órgãos reguladores e da complexidade das operações de TI, levou as empresas a buscarem modelos que facilitassem a descrição e os objetivos dos vários serviços e ambientes de TI, a representação de como esses serviços se inter-relacionam e orientação para a implementação e controle destes serviços.

A governança de TI é um fator relevante diante do cenário apresentado e os modelos estudados mostram-se eficazes para sua implantação em uma organização.

A análise dos *frameworks* apresentados torna claro que seus objetivos não são os mesmos, embora apresentem algumas similaridades:

- tratam do gerenciamento de processos genéricos,
- não restringem o segmento de negócio da organização que deseja aplicar o modelo para a otimização na gestão de TI;
- não abordam detalhes específicos de como implantar os controles em cada área de TI;
- são compatíveis com a maioria das ferramentas, modelos e normas para boas práticas de governança de TI existentes no mercado;
- permitem a realização de um *benchmark* entre a situação da organização e a situação do mercado;
- abordam de forma abrangente todo o gerenciamento de TI de uma organização;

- são orientados à processos e segmentam esses processos em objetivos/atividades, e
- geram produtos para todos os níveis da organização :
 - para o operacional, aplicam-se as recomendações do que se deve fazer e como;
 - para o nível tático, aplicam-se as métricas para se avaliar a execução dos processos de TI;
 - para o nível estratégico, aplica-se o alinhamento dos objetivos do negócio com os objetivos de TI da organização.

O COBIT é o modelo indicado para mapear a situação da área de TI de uma organização, como ela se posiciona em relação as melhores organizações do seu ramo e em relação aos padrões internacionais e onde a organização deseja chegar. Para esta tarefa são definidos os indicadores de desempenho que medirão se a performance dos processos de TI está na direção correta para se atingir os objetivos. Este processo auxiliará a organização na definição do que precisa ser implementado para que o nível acordado de controle seja efetivamente alcançado.

O COBIT deve ser utilizado como uma ferramenta para avaliação dos riscos e os resultados de sua aplicação podem ser utilizados para informar aos administradores se os processos de TI estão de acordo com os requerimentos do negócio.

Por apresentar modelos genéricos de processo, modelos de maturidade e avaliação e guias de auditoria definidos, o COBIT aplica-se como um modelo para auditoria de sistemas eficaz.

Conforme exposto, O COBIT não determina como os processos devem ser estruturados, e sim os controles que eles devem possuir para que TI cumpra seus objetivos em termos de governança, ou seja: alinhamento e entrega de valor por parte da área de TI para o negócio; correta alocação e medição dos recursos envolvidos; a mitigação dos riscos em TI.

O COBIT não apresenta formas para estruturar os processos ou implantar os controles, apenas aponta que controles devem ser implantados. Nesta

estruturação surge a necessidade da utilização de ferramentas, conceitos e modelos que o complementem, umas delas é o ITIL.

O ITIL apresenta um foco menos estratégico, mais tático e operacional, voltado à identificação, organização, execução e padronização dos processos. Através da sua aplicação, pode-se atingir a eficiência dos processos, redução de riscos e conformidade estabelecidos através do COBIT.

Conforme colocado anteriormente, o COBIT é voltado para os gerentes, que necessitam avaliar os riscos e controlar os investimentos de TI; os usuários, que precisam assegurar a qualidade dos serviços prestados para clientes internos e externos; e os auditores de sistemas que necessitam avaliar a gestão da TI e apontar recomendações para o aperfeiçoamento do controle interno da organização.

O ITIL aponta as melhores práticas para todas as atividades gerenciais às quais for aplicado, relembramos algumas: gerenciamento de incidentes, de problemas, financeiro, para serviços de TI e suporte, entre outras.

É importante ressaltar que os autores dos dois modelos colocam que não se trata de receitas ou fórmulas prontas. Ambos devem ser encarados como quadros de referência para as estruturas dos processos de TI visando sua otimização e não como um algoritmo de como se deve implementar os processos de TI. Devem ser utilizados como guias para melhorar a estrutura de TI da organização.

Para que as metodologias empregadas tenham resultados, é preciso que exista comprometimento da administração e investimento de recursos. É necessário ainda, realizar uma avaliação dos processos para a identificação das fragilidades e dos pontos fortes de TI na organização, é preciso identificar quais processos realmente precisam ser implantados, quais os pontos de maior risco e qual será o impacto nos outros setores da empresa.

9 INTEGRAÇÃO DAS METODOLOGIAS E PADRÕES PARA GOVERNANÇA E/OU GESTÃO DE TI

O objetivo deste capítulo é apresentar uma visão geral de como alguns dos principais modelos e padrões aplicáveis à TI disponíveis no mercado se relacionam e podem contribuir em um processo de implantação da governança de TI. A integração dos modelos COBIT e ITIL será apresentada de forma detalhada no capítulo 10.

Visto que cada modelo foca em um aspecto específico da governança e gestão de TI, apresentaremos neste capítulo alternativas de integração de seus processos. O COBIT é focado na implantação da governança de TI e no controle dos processos, o ITIL é focado no gerenciamento de serviços, porém algumas atividades são complementares.

Existem várias metodologias disponíveis no mercado e cada uma foca em um aspecto específico da governança ou gestão de TI, conforme apresentado na Tabela 9.1.

Tabela 9.1 - Quadro comparativo de modelos e seus objetivos

Modelo	Objetivo	Foco Primário
BSC	Planejamento e gestão estratégica	Governança Corporativa
COBIT	Governança e controle de processos	Governança de TI
ITIL	Gerenciamento de serviços	Gerenciamento de TI
CMMI	Desenvolvimento de soluções	Gerenciamento de TI
ISO/IEC 9001	Qualidade de processos e produtos	Governança Corporativa
PMBok	Gerenciamento de projetos	Gerenciamento de TI
ISO/IEC 17799 e BS 7799	Segurança da Informação	Gerenciamento de TI
ISO/IEC 20000	Gestão de Serviços	Gerenciamento de TI

Conjunto de normas ISO/IEC 27000	Gerência da Segurança da Informação	Gerenciamento de TI
BS 15000	Gestão de Serviços	Governança de TI
PRINCE2	Gerenciamento de projetos	Gerenciamento de TI

As normas BS 15000 e ISO/IEC 20000 são consideradas normas de Gestão de Serviços. A BS 15000 foi a primeira norma formal para gestão de serviços de TI desenvolvido pela *British Standards Institution* (BSI). Embora seja baseada no modelo de processos do ITIL, fornece especificações claras para implementação de um processo de gestão de serviços em TI.

A BS 15000 é dividida em 2 partes, sendo que a primeira parte especifica 13 processos e é a base para implementar e certificar um sistema de gerenciamento para fornecimento de serviços de TI. A segunda parte é um código de práticas que amplia os requerimentos da primeira. Fazem parte de seu escopo:

- escopo dos serviços de sistema de gestão;
- termos e definições;
- planejamento e implementação dos processos de gestão de serviços;
- planejamento e implementação de gestão de novos serviços ou modificações dos serviços existentes.

A ISO 20000 surgiu como uma evolução da ISO 15000, e embora as alterações sejam mínimas, trata-se de um formato internacional mais adequado. Assim como sua predecessora, a ISO 20000 é dividida em duas partes: a ISO 20000-1, promove a adoção de processos integrados para a gestão de serviços a fim de alcançar os requerimentos dos clientes e do negócio; e a ISO 20000-2 é um código de práticas e descreve as melhores práticas para a gestão de serviços dentro do escopo da ISO 2000-1.

As normas BS 15000 e ISO 20000 são alinhadas em seus objetivos com o modelo ITIL, sendo que, o ITIL fornece o conjunto de melhores práticas que, uma vez adotadas, auxiliarão as organizações a encontrarem a qualidade de gestão de serviço requerida pelas normas BS 15000 e ISO 20000. O modelo ITIL serviu de

base para o desenvolvimento da BS 15000, que por sua vez serviu de base para o desenvolvimento da ISO 20000.

A norma britânica BS 7799 – *British Standard 7799* - publicada em 1995, é um código de práticas planejado para ser usado como uma referência para os gerentes e responsáveis pela segurança da informação nas organizações. Deve servir de base para a criação de uma política de segurança e aborda os seguintes tópicos: avaliação de riscos, gestão de riscos, implementação de meios de segurança, declaração de aplicabilidade. A BS 7799 foi internacionalizada pelo padrão ISO/IEC 17799, que tem como equivalente brasileiro a ABNT NBR ISO/IEC 17799.

A série ISO 27000 está de acordo com outros padrões de sistemas de gerência ISO, como a ISO 9001. A ISO/IEC 27001 é um padrão para sistema de gerência da segurança da informação (ISMS - *Information Security Management System*) publicado em outubro de 2005. Seu objetivo é ser usado em conjunto com ISO 17799, o código de práticas para gerência da segurança da informação, que lista objetivos do controle de segurança e recomenda um conjunto de especificações de controles de segurança. Organizações que implementam um ISMS de acordo com as melhores práticas da ISO 17799 estão simultaneamente em acordo com os requisitos da ISO 27001. Esta família de normas contempla também padrões específicos para: Vocabulário de Gestão da Segurança da Informação, Gestão de Risco, Mecanismos de Mediação e de Relatório de um Sistema de Gestão de Segurança da Informação e Implementação, Monitoramento e Melhoria Contínua do Sistema de Controles.

Informações detalhadas e outras normas para tecnologia da informação e gerência de TI continuam a ser publicadas pela ISO e podem ser adquiridas no *site* oficial da organização.

Embora com objetivos distintos, existem diversas áreas de interseção entre os modelos apresentados. O *framework* COBIT e os padrões ISO 9001 e ISO 17799 podem ser utilizados na identificação do que deve ser gerenciado; para como deve ser efetuada a gerência pode-se utilizar o COBIT, CMMI, ISO 17799 e PMBoK; para o que deve ser executado pode-se utilizar o ITIL, CMMI, ISO 17799 e PMBoK;

para os detalhes da execução é necessário a utilização de outras ferramentas e métodos específicos. Estes relacionamentos estão horizontalmente ilustrados na Figura 9.1.

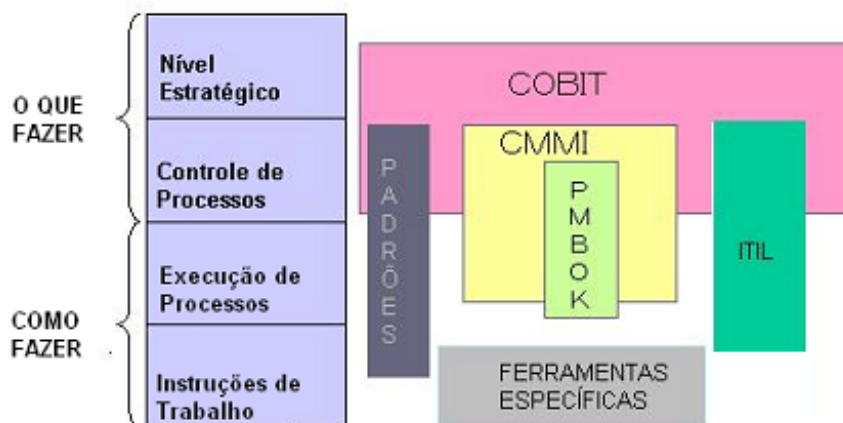


Figura 9.1 – Relacionamento entre os modelos, padrões e suas áreas de atuação (Adaptado de: *Project Management University*, 2006).

As melhores práticas de TI devem ser alinhadas às exigências do negócio e integradas com os procedimentos internos de cada organização. O COBIT pode ser utilizado em um nível mais elevado, fornecendo uma estrutura de controle baseada nos processos de TI. As áreas específicas devem ser cobertas por outros padrões como o ITIL ou as normas BS e padrões ISO, que podem ser integradas ao COBIT.

10 INTEGRAÇÃO DOS *FRAMEWORKS* COBIT E ITIL PARA UM PROCESSO DE IMPLANTAÇÃO DE GOVERNANÇA DE TI

Com os processos de cada modelo classificados e detalhados, torna-se necessário realizar um mapeamento de correspondência entre os processos para que ambos os modelos possam ser usados conjuntamente em um processo de implantação da governança de TI.

Durante um processo de implantação da governança de TI em uma organização, é prudente a utilização de frameworks que abordem os aspectos relacionados com as áreas foco da governança: Alinhamento Estratégico, Entrega de Valor, Gerência de Recursos, Gerência de Riscos e Medição de Desempenho.

Realizando-se uma análise dos padrões COBIT e ITIL é possível estabelecer uma matriz genérica de correspondências e relacionamento entre os seus processos, visando a implantação da governança de TI, conforme demonstrado na Tabela 10.1.

Tabela 10.1 - Relacionamento entre os livros do ITIL e os objetivos do COBIT para governança de TI

Livros do ITIL	Objetivos de Controle Relacionados do COBIT
Prestação de Serviço	PO9, AI1, DS1, DS2, DS3, DS4, DS5, DS6, DS8, DS9, MA3
Suporte de Serviço	DS8, DS9, DS10, AI5, AI6
Gerenciamento da Infra-Estrutura	PO1, PO3, PO4, AI1, AI3, AI5, DS8, DS10, DS12, DS13, MA2
Gerenciamento de Aplicações	AI1, AI2, AI5, PO2, PO6
Planejamento para Implementação do Gerenciamento de Serviços	PO4, PO6, DS1, DS2, MA1
Perspectiva do Negócio	PO1, DS1, DS2, MA1

Atendimento ao Cliente	PO8, DS8, MA2
Gerenciamento da Segurança	PO9, DS5, DS11, DS12, MA2,

Os objetivos de controle do COBIT não se relacionam diretamente às atividades descritas no ITIL. Para integrá-los é preciso observar os objetivos detalhados. Esta análise é apresentada na Tabela 10.2.

Tabela 10.2 - Integração dos frameworks COBIT e ITIL

Domínios e Objetivos de Controle do COBIT Áreas do ITIL	Suporte de Serviço					Prestação de Serviço					Perspectiva do Negócio	Gerenc. De Aplicações	Gerenc. Da Infra-Estrutura	Gerenc. Da Segurança	Planejamento e Implementação	Atendimento ao Cliente	
	Gerenc. De Incidentes	Gerenc. De Problemas	Gerenc. De Mudanças	Gerenc. De Versões	Gerenc. De Configuração	Gerenc. De Níveis de Serv.	Gerenc. Financeiro	Gerenc. De Capacidade	Gerenc. De Continuidade	Gerenc. De Disponibilidade							
PO - Planejamento e Organização																	
PO1 - Definir um plano estratégico de TI											X		X				
PO2 - Definir a arquitetura das informações												X					
PO3 - Determinar a direção tecnológica													X				
PO4 - Definir a estrutura e o relacionamento de TI											X		X		X		
PO5 - Gerenciar o investimento em TI							X										
PO6 - Divulgar os objetivos e a orientação da gerência											X	X			X		

Domínios e Objetivos de Controle do COBIT	Suporte de Serviço					Prestação de Serviço										
	Gerenc. De Incidentes	Gerenc. De Problemas	Gerenc. De Mudanças	Gerenc. De Versões	Gerenc. De Configuração	Gerenc. De Níveis de Serv.	Gerenc. Financeiro	Gerenc. De Capacidade	Gerenc. De Continuidade	Gerenc. De Disponibilidade	Perspectiva do Negócio	Gerenc. De Aplicações	Gerenc. Da Infra-Estrutura	Gerenc. Da Segurança	Planejamento e Implementação	Atendimento ao Cliente
DS1 – Definir e gerenciar níveis de serviços						X					X				X	
DS2 – Gerenciar serviços de terceiros						X					X				X	
DS3 – Gerenciar desempenho e capacidade								X		X						
DS4 – Assegurar a continuidade do serviço									X	X						
DS5 – Assegurar a segurança dos sistemas										X				X		
DS6 – Identificar e alocar custos							X									
DS7 – Educar e treinar usuários																
DS8 – Gerenciar o atendimento aos clientes e incidentes	X	X				X							X			X
DS9 – Gerenciar as configurações					X			X								
DS10 – Gerenciar problemas e incidentes	X	X											X			
DS11 – Gerenciar informações														X		
DS12 – Gerenciar as instalações													X	X		
DS13 – Gerenciar as operações													X			

Domínios e Objetivos de Controle do COBIT	Suporte de Serviço					Prestação de Serviço										
	Gerenc. De Incidentes	Gerenc. De Problemas	Gerenc. De Mudanças	Gerenc. De Versões	Gerenc. De Configuração	Gerenc. De Níveis de Serv.	Gerenc. Financeiro	Gerenc. De Capacidade	Gerenc. De Continuidade	Gerenc. De Disponibilidade	Perspectiva do Negócio	Gerenc. De Aplicações	Gerenc. Da Infra-Estrutura	Gerenc. Da Segurança	Planejamento e Implementação	Atendimento ao Cliente
Áreas do ITIL																
MA – Monitoramento e Avaliação																
MA1– Monitorar e avaliar a performance da TI											X				X	
MA2 – Monitorar e avaliar os controles internos da TI												X	X			X
MA3 – Assegurar conformidade com as práticas regulatórias							X									
MA4 – Prover a governança de TI																

(X) Processos que tratam de temas correlatos, são complementares ou podem ser integrados.

No mapeamento apresentado nas tabelas 10.1 e 10.2 considera-se os macro-processos, e os objetivos de controle detalhados, respectivamente, apenas dos modelos COBIT e ITIL. Porém, em ITGI (2007) encontram-se mapeamentos genéricos entre estes e outros modelos, como o padrão BS7799.

Os processos que se encontram marcados na Tabela 10.2 apresentam correspondência direta entre seus objetivos, contudo realizando uma análise mais ampla observa-se que, devido ao fato de ambos os modelos apresentarem como objetivo estratégico o alcance da governança de TI, a aplicação de atividades que aparentemente não estão relacionadas contribui para um mesmo fim: aprimorar os controles no ambiente de TI e conseqüentemente atingir os objetivos da governança.

11 CONCLUSÃO

11.1 CONSIDERAÇÕES FINAIS

Para muitas organizações a Tecnologia da Informação representa um recurso precioso e um fator crítico para o negócio. Os desafios enfrentados na administração de TI são significativos e progressivos: os objetivos estratégicos do negócio dependem do desempenho da TI; a criticidade dos serviços prestados pela TI requer aumento da confiabilidade, disponibilidade e qualidade dos serviços; o aumento da complexidade e do custo dos recursos de TI precisa ser gerenciado dinamicamente; medidas regulatórias e demandas legais aumentam a visibilidade do desempenho e das fragilidades da área de TI.

Estes desafios atuam como motivadores para a implantação da governança de TI. Segundo o ITGI (2006), as empresas bem sucedidas compreendem os benefícios da Tecnologia de Informação e usam este conhecimento para agregar valor ao negócio.

A introdução da governança de TI na cultura de uma organização requer mudanças estruturais profundas, que necessitam de esforço e investimento. Neste processo, é necessária uma análise da relação custo x benefício e dos objetivos que a organização pretende atingir. É consenso entre os autores pesquisados que, adotar um *framework* de melhores práticas para implantação da governança de TI é recomendável. As melhores práticas internacionais disponíveis representam a experiência prática acumulada por inúmeras empresas, profissionais de TI e auditores, o que poupa as organizações do esforço de desenvolvê-las, testá-las e, conseqüentemente, minimizando a possibilidade de erros.

Para empresas que necessitam adequar-se à legislação SOX ou que pretendem estar de acordo com as conformidades estabelecidas por esta e outras legislações, visando maior competitividade no mercado ou buscando expansão internacional, as melhores práticas apresentam-se como guias estratégicos de diretrizes a seguir. Embora existam vários padrões que uma empresa pode usar na

definição e documentação de seus controles internos para governança de TI, a maioria das organizações e auditores adotou o COBIT.

Constatou-se que em um processo de implantação da governança de TI em uma organização, uma abordagem inicial utilizando-se o modelo COBIT é recomendada. O COBIT foca na definição de estruturas organizacionais, controles, processos e responsabilidades, permitindo que as partes interessadas (executivos, alta direção, gerentes, investidores, auditores etc.) tenham um diagnóstico da situação da área de TI. Seu objetivo é garantir que a TI sustente as estratégias do negócio e contribua para o alcance das metas da organização. Para atingir este resultado, o COBIT aponta diversos controles sobre os recursos de TI, apresentados neste trabalho. A aplicação desses controles objetiva assegurar a qualidade, confiabilidade, disponibilidade e segurança das informações. Os objetivos de controle focam nas cinco áreas principais da governança de TI: alinhamento estratégico, gerência de recursos, gerência de riscos, entrega de valor e métricas de desempenho.

Conforme apresentado neste trabalho, o COBIT atua em um nível estratégico, apontando o que precisa ser feito para atingir a governança de TI, mas sem mais especificações de como este processo deve ser realizado. Assim, em uma segunda etapa do processo de implantação da governança ou de aprimoramento dos controles internos da área de TI, recomenda-se a utilização de outros modelos, como o ITIL.

O ITIL consiste em um conjunto de livros, que traz uma descrição detalhada de recomendações e melhores práticas para gerenciamento de serviços e infra-estrutura de TI. Seus objetivos principais são alinhar os objetivos da TI aos objetivos do negócio, melhorar a qualidade do serviço prestado e reduzir custos. A aplicação do ITIL contribui para a implantação da governança em um nível mais tático, cobrindo aspectos relevantes para o gerenciamento de TI, em níveis distintos de detalhamento. O ITIL aborda a TI como uma prestadora de serviço que fornece requisitos básicos para a operação do negócio e que necessita garantir a prestação dos serviços dentro dos parâmetros definidos. Dentre os controles estabelecidos para garantir o funcionamento deste processo, destaca-se os acordos de níveis de

serviço, que buscam formalizar a confiabilidade (suporte ao negócio), qualidade (disponibilidade e desempenho) e custo estabelecidos. Uma estratégia inicial para implementar ITIL é realizar uma avaliação dos processos da organização utilizando COBIT, desta forma pode-se identificar as fraquezas e forças da estrutura de TI. Estas avaliações podem se repetir posteriormente para avaliar o progresso do projeto.

Existem outros modelos e padrões com focos em aspectos específicos da governança e gestão de TI, este trabalho procurou citar normas e outras metodologias que podem ser integradas ao COBIT e ITIL em um processo de governança, tais como CMMI, Prince2 e PMBoK, além de outras normas e padrões internacionais.

A integração dos modelos COBIT e ITIL apresentada neste trabalho teve como objetivo relacionar de forma simplificada o maior número possível de controles. Visto que, em um processo de governança, quanto maior o número de atividades estiver em consonância com as melhores práticas, maiores chances de alcance do alinhamento estratégico.

Os autores citados neste estudo deixam claro que as melhores práticas não são fórmulas mágicas. Devem ser encaradas como quadros de referência para as estruturas dos processos de TI, visando sua melhoria, e não como receitas de como se deve implementar os processos. Além disso, podem ser utilizadas como guias para melhor estruturar a TI da organização.

Destaca-se que os padrões e as melhores práticas não garantem sucesso na implantação da governança, sua eficácia depende de como foram executados e do comprometimento com a continuidade do processo. Porém, são bastante úteis quando aplicados como um guia para implantar e organizar procedimentos de controle específicos. Para evitar o obstáculo da resistência, a gerência e a equipe devem compreender o que fazer, como fazer e por que é importante.

Conforme exposto ao longo deste estudo, a organização pode implementar tantos processos, ou controles sugeridos pelos modelos apresentados, quanto necessário, sempre observando se o custo e os benefícios da implantação estão de acordo com as estratégias do negócio. Os modelos e padrões

apresentados, assim como a integração proposta neste trabalho, permitem realizar uma avaliação detalhada da estrutura de TI, facilitando o gerenciamento e controle dos processos, e conseqüentemente, contribuindo para os objetivos da governança.

11.2 QUANTO AOS OBJETIVOS ESPECÍFICOS

Para cada objetivo estabelecido no início do trabalho, sucederam-se tarefas no sentido de alcançar os resultados esperados. Considerando-se que este trata-se de um trabalho teórico, o mecanismo utilizado foi uma vasta pesquisa e revisão de material bibliográfico, que serviu como base para os capítulos apresentados. A seguir apresenta-se a lista de objetivos e os resultados de cada etapa.

11.2.1 OBJETIVO ESPECÍFICO I

I – Apresentar o conceito de governança em TI e a importância dos controles para a otimização dos processos de TI.

Para o estudo da governança de TI foi utilizada uma vasta revisão bibliográfica baseada em livros e artigos que abordam o assunto, o resultado apresenta-se no capítulo 3. Acredita-se que este objetivo foi alcançado, uma vez que através da leitura do capítulo pode-se perceber o que é a governança de TI, a que ela se propõe, formas de implantá-la e quais objetivos deve-se pretender na implantação de um processo de governança.

11.2.2 OBJETIVO ESPECÍFICO II

II - Apresentar detalhadamente as metodologias aplicáveis para alcance da governança de TI – COBIT.

Para o estudo do COBIT, foram utilizadas as referências bibliográficas apresentadas em ITGI (2005), sendo a principal o documento do COBIT na íntegra, constituído pelo Sumário Executivo, Estrutura do *Framework* e os quatro livros correspondentes aos domínios ou processos-macro: Planejamento e organização, Aquisição e implementação, Distribuição e suporte e Monitoração e avaliação.

Após a leitura e análise do material, apresentou-se um resumo do *framework*, no capítulo 4. Acredita-se que este capítulo proporciona ao leitor uma visão abrangente e detalhada do modelo e suas propostas. Como a organização do capítulo segue a mesma estrutura do documento original, ele atua também como guia, propiciando ao leitor uma visão de em que parte do COBIT procurar a informação que necessita.

Acredita-se que o COBIT é bastante útil em um processo de implantação da governança de TI e recomenda-se o seu uso na fase inicial, para levantamento e avaliação do nível de maturidade dos processos. Após esta etapa, o COBIT pode ser utilizado como um guia para definição dos objetivos estratégicos que devem ser alcançados pela TI para atender os objetivos do negócio. Este processo envolve o uso dos indicadores de desempenho e requer um *benchmark* com os controles apresentados pelo modelo.

Observou-se também que o COBIT vem sendo adotado pelos órgãos reguladores e fiscalizadores de alguns setores da economia, assim ele se mostra igualmente útil para administradores de TI que necessitam atingir a conformidade com as práticas exigidas pelo mercado e para auditores que necessitam verificar se os processos de TI estão aderentes às melhores práticas.

Os desenvolvedores do COBIT, ISACA – *Systems Audit and Control Association* – e *IT Governance Institute*, acreditam que o modelo incorpora e aprofunda as práticas internacionais de Governança de TI já mencionadas por outros *frameworks* como ITIL, ISO/IEC 17799, ISO/IEC 13335, ISO/IEC 15408, TickIT, NIST e COSO.

O COBIT pode ser utilizado como base na definição de planos de auditoria em TI, visto que contempla todos os processos principais de um departamento de tecnologia.

11.2.3 OBJETIVO ESPECÍFICO III

III - Apresentar detalhadamente as metodologias aplicáveis para alcance da governança de TI – ITIL.

Para o estudo do ITIL, foram utilizadas as referências bibliográficas apresentadas em ITSMF(2003), sendo a principal o documento *IT Service Management*, que traz uma descrição dos conceitos e características que são aprofundadas nos mais de 40 livros e materiais componentes do modelo. Por tratar-se de um material bastante extenso, optou-se por apresentar uma visão geral dos 7 livros principais, que proporcionasse ao leitor uma base do “coração” do *framework* e atuasse como guia para os demais assuntos.

O resumo apresentado no capítulo 5 apresentou um resumo do modelo, sua estrutura e os detalhes de seus componentes principais: Prestação de Serviço e Suporte de Serviço. Foram abordadas todas as áreas cobertas por estes 2 livros, com foco nos controles que devem ser gerenciados em cada um.

Acredita-se que o ITIL, assim como o COBIT, é bastante útil em um processo de implantação e aprimoramento da governança de TI em uma organização. Observa-se porém, que este deve ser implantado em uma segunda etapa, após a avaliação e identificação dos controles necessários, o ITIL revela-se uma ferramenta poderosa para mapear os recursos de infra-estrutura de TI e estabelecer critérios para gerenciá-la com foco na prestação de serviço. O ITIL considera a área de TI uma prestadora e, em algumas organizações, o cliente é o próprio negócio. Através do ITIL, é possível desenvolver estruturas que garantam a continuidade da prestação de serviço, a qualidade do serviço prestado e a gerência responsável dos recursos envolvidos. Por trata-se de um conjunto de práticas já testadas e aprovadas, a chance de sucesso na implantação de processos do ITIL é maior. Ainda que seu objetivo principal não seja a governança de TI, este modelo busca em seus processos o alinhamento estratégico como resultado final e seus resultados colaboram com os objetivos da governança de TI.

11.2.4 OBJETIVO ESPECÍFICO IV

IV - Apresentar outros modelos e padrões que possam ser integrados ao COBIT e ITIL, buscando cobrir áreas da governança de TI que não estejam contempladas nestes modelos.

Através do estudo dos modelos COBIT e ITIL observou-se que estes não são suficientes para contemplar todos os aspectos da implantação de um processo de governança de TI. Assim, no capítulo 9 foi apresentada uma visão geral de como alguns dos principais modelos e padrões aplicáveis à TI disponíveis no mercado se relacionam e podem contribuir com este processo. A pesquisa baseou-se em verificar as áreas específicas não cobertas pelo COBIT e ITIL, ou cobertas apenas superficialmente, e posteriormente em identificar outros modelos disponíveis no mercado. Conforme previsto, os modelos e principais normas e padrões foram citados, abordando-se resumidamente sua compatibilidade com os 2 principais *frameworks* analisados. Acredita-se que o capítulo informa ao leitor, resumidamente, quais modelos procurar (além de COBIT e ITIL) para implantar e aprimorar os controles no ambiente de TI, ressaltando-se que para os detalhes da execução é necessário a utilização de outras ferramentas e métodos específicos que variam de acordo com a necessidade da organização e o problema enfrentado durante o processo de governança.

Acredita-se que as melhores práticas de TI devem ser alinhadas às exigências do negócio e integradas aos procedimentos internos de cada organização. O COBIT pode ser utilizado em um nível mais elevado, fornecendo uma estrutura de controle baseada nos processos de TI. As áreas específicas devem ser cobertas por outros padrões como o ITIL, as normas BS e padrões ISO, e demais modelos apresentados.

11.2.5 OBJETIVO ESPECÍFICO V

V - Apresentar uma análise comparativa, delimitando o escopo de aplicação dos modelos.

No capítulo 8, tomando-se como base a revisão dos capítulos 4 e 5, realizou-se uma análise comparativa do COBIT e ITIL, resumindo suas principais características, finalidades, semelhanças e pontos de diferenciação. Neste capítulo pretendeu-se realizar uma conclusão geral sobre todos os aspectos estudados sobre os *frameworks*, situando suas indicações em um processo de governança de TI.

11.2.6 OBJETIVO ESPECÍFICO VI

VI - Citar casos de aplicação dos *frameworks* no mercado, evidenciando sua eficácia.

A análise individual do modelo COBIT e os casos pesquisados de aplicação foram apresentados no capítulo 6, tomando como base a revisão executada no capítulo 4 e artigos correlatos. No capítulo 7 seguiu-se o mesmo procedimento para o modelo ITIL, tomando como base a revisão do capítulo 5 e artigos correlatos. As informações apresentadas dos casos de aplicação dos modelos analisados, foram pesquisadas em artigos e sites de organizações, cujas referências podem ser obtidas nos capítulos de análise e no capítulo de Referências Bibliográficas.

11.2.7 OBJETIVO ESPECÍFICO VII

VII - Apresentar a integração dos modelos com foco na implantação de um processo de governança de TI.

Nos capítulos 8 e 10 observa-se a maior contribuição deste trabalho. Conforme descrito acima, no capítulo 8 apresentou-se uma análise comparativa dos modelos COBIT e ITIL, já no capítulo 10 apresentou-se um esboço de integração dos modelos. A técnica adotada foi elencar os domínios do COBIT e seus objetivos de controle e relacioná-los com as atividades tratadas nos livros do ITIL, de forma a proporcionar ao leitor maior facilidade na busca de informações. O objetivo foi relacionar o maior número possível de controles, visto que, em um processo de governança, quanto maior o número de atividades estiverem em consonância com as melhores práticas, maiores chances de alcance do alinhamento estratégico.

11.3 QUANTO AO OBJETIVO GERAL

Acredita-se que o objetivo principal deste trabalho foi atingido, compreendeu-se os conceitos da governança de TI e a relevância de sua aplicação nas organizações, e apresentou-se uma análise detalhada dos dois modelos mais aceitos no mercado (COBIT e ITIL), aplicáveis em um processo de implantação da governança de TI. Todos os objetivos específicos foram atingidos e foi apresentada ainda, uma integração dos modelos estudados.

11.4 QUANTO ÀS PERSPECTIVAS DE CONTINUIDADE

Por tratar-se de um assunto bastante extenso e complexo, muitas questões poderiam ser aprofundadas a partir dos conceitos aqui apresentados.

Estudos que dariam continuidade a este trabalho na área de conhecimento de Auditoria de Sistemas seriam os seguintes:

- desenvolvimento de uma metodologia de auditoria de sistemas baseada no COBIT e ITIL;
- desenvolvimento de planos de auditoria específicos com base nos modelos aqui apresentados;
- modelagem de um sistema para automatização de avaliação
- de maturidade baseado no COBIT.

Estudos que dariam continuidade a este trabalho na área de conhecimento de Governança e Gerência de TI seriam os seguintes:

- verificação prática da aplicabilidade da integração proposta no ambiente de uma organização;
- aplicação dos conceitos apresentados em estudos de caso, especificamente processos de implantação de governança de TI, para se comprovar na prática os resultados.

Estudos que dariam continuidade a este trabalho em outras áreas de conhecimento:

- ampliar o escopo da integração proposta, abordando-se outros *frameworks*.

11.5 LIMITAÇÕES DA PESQUISA

Este trabalho limitou-se a identificar o que é a governança de TI, suas características e benefícios de sua implementação. Sendo que o processo de implantação da governança é bastante amplo, elegeram-se dois *frameworks* de melhores práticas para estudo. Assim, o escopo deste trabalho restringiu-se a uma pesquisa teórica da aplicação dos modelos COBIT e ITIL , sem entrar em detalhes sobre outros modelos ou testes práticos.

12 REFERÊNCIAS

Aplicações Ou Casos De Sucesso. Disponível em:

<<http://www.cnasi.com.br/casosdesucesso>>.

BOAR, Bernard H. **Tecnologia da informação: a arte do planejamento estratégico.** São Paulo: Berkeley, 2002.

BOAR, Bernard H. **Practical Steps for Aligning Information Technology with Business Strategies: How to Achieve a Competitive Advantage.** John Wiley & Sons, 1994.

BOAR, Bernard H. **The art of strategic planning for information technology: crafting strategy for the 90s.** USA: John Wiley & Sons, 1993.

CACIATO, Luciano Eduardo. **Métricas e metodologias do gerenciamento de TI.** REVISTA TI, 25 de janeiro de 2005.

CAMPBELL, Philip L. **A COBIT® Primer Article.** 2006. Disponível em: <<http://www.osti.gov/bridge>> Acesso em: 03 de agosto de 2007.

CARVALHO, T. C. **Falta a Chamada Governança de TI.** 2004. Disponível em: <<http://www.itweb.com.br/colunista/artigo.asp?id=50613>>.

Casos de Sucesso COBIT. Disponível em:

<<http://www.isaca.org/Template.cfm?Section=COBIT6&CONTENTID=22129&TEMPLATE=/ContentManagement/ContentDisplay.cfm>>.

CHIAVENATO, Idalberto. **Introdução à teoria geral da Administração.** 4. ed. São Paulo: Makron Books, 1993.

CHIAVENATO, Idalberto. **Administração nos novos tempos.** 2 ed. Rio de Janeiro: Campus, 2003.

COBRA Risk Consultant – <http://www.securitypolicy.co.uk/risk.htm>. Acessado em 20 de fevereiro de 2003.

COBRA, Marcos. **Administração de Marketing.** 2. ed. São Paulo: Atlas, 1992.

CONGRESSO NACIONAL DE AUDITORIA DE SISTEMAS E SEGURANÇA DA INFORMAÇÃO, 2007. São Paulo. CNASI.

Conheça o que é o ITIL e o que é o COBIT. **Info Corporate.** Disponível em: <<http://www.path.com.br/noticia22.html>>. Acesso em: 14 agosto 2007.

- DRAFT BS 7799-2:2002**, Information Security Management - Part2: Specification for Information Security Management System. BSI, Novembro de 2001.
- DRUCKER, Peter F. Como reagir às mudanças. **Revista HSM Management L**, maio/abril, 1997.
- ESMERALDO, Cícero. **Governança de TI: Conceitos básicos de Governança de TI e a sua importancia para os negócios**. 2006. Disponível em: <http://www.tradein.com.br/default.asp?key=art&idi=5>.
- FAGUNDES, Eduardo Mayer. **Um Kit de Ferramentas para a Excelência na Gestão de TI**. 2004. Disponível em: http://www.efagundes.com/Artigos/Arquivos_pdf/COBIT.pdf
- FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços**. Rio de Janeiro: Brasport, 2006.
- FERREIRA, Aurélio Buarque de Holanda. **Dicionário da Língua Portuguesa**. Rio de Janeiro: Nova Fronteira, 1999.
- FERREIRA, Cláudio. **Governança: A nova direção de TI alinhada aos resultados corporativos**. TI Inside, São Paulo, v. 1, n. 3, jun. 2005.
- GARCIA, Wandair José. **Modelo de Planejamento Estratégico de Tecnologia da Informação em Empresas Globais**. 2005. Dissertação (mestrado em Engenharia de Produção). Universidade Federal de Santa Catarina.
- HOLM, Michael Larsen; KÜHN, Mogens Pedersen; VIBORG, Kim Andersen. **IT Governance: Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S**. Proceedings of the 39th Hawaii International Conference on Systems Sciences - 2006. IEEE. Koloa, Kauai. Janeiro, 2006, p. 11.
- IBGC. **Governança Corporativa**. Disponível em: <http://www.ibgc.org.br/ibConteudo.asp?IDArea=2>
- IETEC- Instituto de Educação Tecnológica. **ISO IEC 27000 e 20000 - os padrões para gerenciar a TI**. Disponível em: http://www.ietec.com.br/ietec/cursos/area_tecnologia_da_informaca

o/2007/05/24/2007_05_24_0001.2xt/materia_gestao/2007_05_24_0344.2xt/dtml_boletim_interna>

ISACA - Information Systems Audit and Control Association – 2006. Disponível em: <<http://www.isaca.org>>

ISO HOME <http://www.iso.org/iso/store.htm>

ISO 17799 World - <http://www.iso-17799-security-world.co.uk/>. Acesso em 20 de fevereiro de 2003

ISO 17799. Nascimento, Neide Landim Teixeira do Nascimento, UNEB - COPEX, Setembro de 2001.

ISO IEC INFORMATION CENTRE - <http://www.standardsinfo.net/isoiec/stdcat.html>

IT GOVERNANCE INSTITUTE – COBIT 4.0 . 2005 - 2006. Disponível em: <<http://www.itgi.org>>

ITIL na Prática. CIO. 09/10/2005. Data da publicação no Web site da CompanyWeb 26/01/2007. Disponível em: <http://www.companyweb.com.br/lista_artigos.cfm?id_artigo=255> Acesso em: 14 agosto 2007.

ITSMF - <<http://www.itsmf.com.br/itsmf/site/index.asp>>

KOTLER, Philip. Administração de Marketing: a edição do novo milênio. São Paulo: Prentice Hall, 2000.

LAHTI, Christian B.; PETERSON, Roderick. Sarbanes-Oxley: Conformidade TI usando COBIT e ferramentas open source. Rio de Janeiro: Alta Books, 2006.

LEITE, José Alfredo Américo. Metodologia de Elaboração de Teses. São Paulo: McGraw-Hill do Brasil Ltda, 1978.

LUZ, Charley. A SOX é um bicho-de-sete-cabeças? 2006. Disponível em: <<http://www.intranetportal.com.br/colab1/bicho>>. Acesso em: 24 agosto 2007.

MANSUR, Ricardo. O que é ITIL? 2004. Disponível em: <<http://www.profissionaisdetecnologia.com.br/modules.php?name=News&file=article&sid=47>> Acesso em: 14 agosto 2007.

MEDEIROS, João Bosco. Redação Científica: A Prática de Fichamentos, Resumos, Resenhas. São Paulo: Atlas, 1997.

- MENDES, Patrícia de Aquino. **A Lei Sarbanes-Oxley (SOX) e a governança de TI.** 2006. Disponível em:
<<http://webinsider.uol.com.br/index.php/2006/02/07/a-lei-sarbanes-oxley-sox-e-a-governanca-de-ti/>>. Acesso em: 24 agosto 2007.
- MIRANDA, Arnaldo José de; REIS, Rodrigo Quites. **Aplicação de Outsourcing no desenvolvimento e customização de software em Medicina Transfusional: impacto no Gerenciamento da Qualidade.** 2007. III Workshop Um Olhar Sociotécnico sobre a Engenharia de Software – WOSES. Universidade Federal do Pará (UFPA).
- MONTANA, Patrick J.; CHARNOV, Bruce H. **Administração.** São Paulo: Saraiva, 1999.
- MORAES, Marcos. **Governança de TI e Gestão da Segurança da Informação.** 2006. Disponível em:
<<http://www.ms.senac.br/uploads/13223936.ppt>> Acesso em: 14 agosto 2007.
- OLIVEIRA, Djalma Pinho Rebouças de. **Planejamento estratégico: conceitos, metodologias e práticas.** 16. ed. São Paulo: Atlas, 2001.
- Organização para a Cooperação e o Desenvolvimento Econômico. **OECD Principles of Corporate Governance**, 2004. página 11. Disponível em: <<http://www.oecd.org/dataoecd/32/18/31557724.pdf>>
- PEREIRA, Adriano de Souza; KRUGER, Erika Iorio; SILVEIRA, Jorge Alves da; FRANÇA, Karla Fabiana Cavalcante de; MOREIRA, Lauro Nobre Machado; VIEIRA, Marina da Silva; PATRÍCIO Mario Ney Campos Gomes Monteiro Rosemberg de Oliveira. **Indução e Dedução: Considerações sobre o Método Científico.** Programa de Engenharia de Transportes, COPPE/UFRJ. Data não disponível. Disponível em:
<<http://www.ldcinf.com.br/forum/detalhes.asp?local=res&id=41>>
- PINHO, Carlos Tadeu A. de. **Software livre - uma alternativa estratégica para as organizações públicas e privadas?** 2005. Disponível em:
<<http://www.dicas-l.com.br/dicas-l/20050418.php>>. Acesso em: 04 de setembro de 2007.

Portal ISO 17799 - <http://www.iso17799.hpg.ig.com.br/>. Acesso em 20 de fevereiro de 2003.

RAMIREZ, Jean-Claude; SENDER, Claudia. **Alinhando a tecnologia da informação à estratégia**. *Bain & Company*, 2003.

RAMIREZ, Pedro A. R.. **Alinhamento Estratégico de Negócios e TI Em um Ambiente de Hipercompetição**. 2007. Disponível em:
<http://www.suesc.com.br/extensao/conteudo/revista_online/06_artigo03.pdf>

REZENDE, Denis Alcides. **Alinhamento do Planejamento Estratégico da Tecnologia da Informação ao Planejamento Empresarial: proposta de um modelo e verificação da prática em grandes empresas brasileiras**. 2002. 278 f. Tese (Doutorado em engenharia de Produção), Universidade Federal de Santa Catarina, Florianópolis.

REZENDE, Denis Alcides; ABREU, Aline França de. **Planejamento Estratégico da Tecnologia de Informação Alinhado ao Planejamento Estratégico de Empresas**. Artigo publicado na REVISTA DE ADMINISTRAÇÃO MACKENZIE, Ano 3, n.2, p. 39-51, 2001.

RICCIARDI, Gianni. **IT Governance - Artigo III** - Otimização da estrutura dos processos de TI – COBIT, ITIL e demais conceitos, metodologias e ferramentas. 2005. Disponível em:
<http://www.anefac.com.br/m5.asp?cod_noticia=337&cod_pagina=903.htm>.

RICCIARDI, Gianni. **IT Governance - Artigo V** - Consolidação da IT Governance - Gestão da Mudança nas estruturas de TI e monitoramento dos indicadores. 2005. Disponível em:
<http://www.anefac.com.br/m5.asp?cod_noticia=371&cod_pagina=903.htm>.

SPOHR, Elizabet M. de Medeiros; SAUVÉ, Jacques P. **Avaliação do Impacto de Tecnologias da Informação Emergentes nas Empresas**. Rio de Janeiro: QualyMark, 2003.

WEILL, Peter; ROSS Jeanne. **Governança de TI: Tecnologia da Informação**. São Paulo: Mbooks, 2006.

Who in the US has implemented ITIL and what was the outcome? – **ITIL survival**.

Disponível em: <<http://www.itil survival.com>> Acesso em: 14 agosto 2007.

13 ANEXO – ARTIGO

Uma Análise Comparativa de Metodologias para Governança de Tecnologia da Informação – ITIL e COBIT

Marília Gabriela Sodr , Suzana Maria de Souza

Depto. de Inform tica e Estat stica – Universidade Federal de Santa Catarina (UFSC)
Florian polis – SC - Brasil

{lila, suzanna}@inf.ufsc.br

Abstract. *In the current dynamic and competitive scene of the businesses, the IT Governance is distinguished as a set of mechanisms that allows establishing objectives, to formulate controls, to execute strategies and to evaluate the Information Technology's results. The technology isn't more only an area of support. Now, it's a strategical partner in the reach of the business's objectives. The organizations that understand this concept and obtain to incorporate the objectives of the governance in your structure, acquire conditions to perfect the management of your infrastructure and IT services. In this work, a bibliographical revision of two models of prominence is become fulfilled: COBIT, as a framework of best practices for governance and IT audit, and ITIL, a framework for services management and IT infrastructure.*

Resumo. *A Governan a de TI destaca-se no atual cen rio din mico e competitivo dos neg cios como um conjunto de mecanismos que permitem estabelecer objetivos, formular controles, executar estrat gias e avaliar os resultados obtidos pela Tecnologia da Informa o. A tecnologia deixou de ser apenas uma  rea de suporte para tornar-se um parceiro estrat gico no alcance dos objetivos do neg cio. As organiza es que compreendem este conceito e conseguem incorporar os objetivos da governan a em sua estrutura adquirem condi es para aperfei oar o gerenciamento de sua infra-estrutura e servi os de TI. Neste trabalho realiza-se uma revis o bibliogr fica de dois modelos de destaque nessa  rea: o COBIT, como um framework de melhores pr ticas para governan a e auditoria de TI, e o ITIL, um framework para ger ncia de servi os e infra-estrutura de TI.*

1. INTRODU O

No cen rio atual das organiza es, a Tecnologia da Informa o (TI) tem, paulatinamente, deixado de ser uma  rea de suporte. Ela tem exercido cada vez mais um papel fundamental para as estrat gias de neg cio das organiza es. Com isso, as exig ncias quanto   organiza o e controle da  rea de TI tamb m

aumentaram dentro das empresas. A administração eficaz dos recursos de TI tornou-se um fator impactante para o desenvolvimento, fortalecimento e sucesso de uma organização no mercado.

As operações de TI envolvem altos riscos e demandam grandes investimentos. Alinhar os objetivos da TI ao negócio da empresa e gerenciá-los tornou-se uma tarefa complexa e, sem o auxílio de métodos confiáveis é difícil garantir o atendimento das necessidades com eficiência, eficácia e cumprimento dos prazos. Nesse contexto surge a necessidade da implantação da Governança de TI, objetivando o gerenciamento prudente dos recursos, o aprimoramento dos controles internos e a mitigação dos riscos envolvidos. Para auxiliar as empresas neste processo estão disponíveis no mercado diversos modelos ou padrões que contribuem para a Governança em TI, dentre eles: COBIT (Control Objectives for Information and related Technology), ITIL (Information Technology Infrastructure Library), CMMI (Capability Maturity Model Integration), PMBoK (Project Management Body of Knowledge) e padrões de segurança e melhores práticas como a ISO/IEC – 17799, ISO/IEC 20000 e 27001.

2. GOVERNANÇA EM TECNOLOGIA DA INFORMAÇÃO

O principal objetivo da Governança de TI é o alinhamento da TI aos requisitos do negócio, que se baseia na continuidade do negócio e no atendimento às suas estratégias e aos marcos de regulação externos. Fernandes e Abreu (2006), desdobraram esse objetivo principal em outros seis objetivos:

- permitir à TI um posicionamento mais claro e consistente em relação às outras áreas da empresa;
- alinhar e priorizar as iniciativas de TI com a estratégia do negócio;
- alinhar a arquitetura e a infra-estrutura de TI às necessidades do negócio, pensando não só no presente, mas também no futuro;
- munir a TI com processos operacionais e de gestão, necessários para atender os serviços de TI, conforme padrões que atendam às exigências do negócio;

- garantir à TI uma estrutura de processos que possibilite a gestão do seu risco para a continuidade operacional da empresa;

De acordo com o IT Governance Institute (2005 apud Fernandes; Abreu, 2006, p.11), “a governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização.” Já para Weill; Ross (2006), Governança de TI é “a especificação dos direitos decisórios e do framework de responsabilidades para estimular comportamentos desejáveis na utilização da TI”.

Os fatores motivadores para aplicação da governança de TI em uma organização, podem ser divididos em internos e externos. As motivações internas são: os investimentos em TI aumentam progressivamente; importância cada vez maior da segurança da informação; os clientes estão cada vez mais exigentes em relação aos produtos e serviços; a transparência nos negócios é cada vez mais exigida. Destacamos como fatores externos: garantia de ética na organização; criação e proteção de benefícios para os acionistas; adequação ao Ato Sarbanes-Oxley (SOX), que apesar de representar restrições ao negócio, atrai geração de lucros.

3. COBIT - CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY

O COBIT (ITGI, 2005) foi desenvolvido pelo IT Governance Institute (ITGI) e provê um conjunto de boas práticas através de um framework composto de domínios e processos, apresentando atividades dispostas em uma estrutura manejável e lógica. Ele apresenta um modelo de processo genérico que representa todos os processos freqüentemente encontrados nas atividades de TI, disponibilizando um modelo de referência compreensível para gerentes operacionais de TI e de negócios. As boas práticas do COBIT representam o consenso de peritos.

O framework é fortemente focado em controle e menos em execução. Suas práticas ajudam a aperfeiçoar os investimentos em TI, assegurar a prestação

de serviços e prover uma medida para avaliar quando algo não está sendo feito como deveria. Para obter êxito em suas metas e estar de acordo com as exigências empresariais, a administração necessita adotar um sistema de controle interno ou framework para TI. O COBIT contribui para estas necessidades fornecendo: um mecanismo para alinhar a TI com os objetivos do negócio; organizar as atividades da TI em um modelo de processo amplamente aceito; identificar os melhores investimentos em recursos de TI; definir os objetivos de controle que a administração deve considerar.

A orientação empresarial do COBIT consiste em unir os objetivos do negócio (metas da empresa) com os objetivos da TI e provê métricas e modelos de maturidade para avaliar a satisfação o cumprimento de tais objetivos, identificando as responsabilidades associadas aos processos. Sua estrutura é organizada em um modelo de processo que subdivide a TI em 34 processos alinhados com a responsabilidade das áreas de planejamento, construção, execução e monitoramento (auditoria), provendo uma visão fim-a-fim da TI.

O COBIT apóia a governança de TI, provendo um framework que assegura que a TI esteja alinhada ao negócio; contribua para o negócio e maximize benefícios; garanta que os recursos da TI sejam utilizados com responsabilidade e que os riscos envolvidos na TI estejam administrados adequadamente.

4. ITIL - INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY

O ITIL (ITSMF, 2003) foi inicialmente desenvolvido pela *Central Computer and Telecommunications Agency* (CCTA) do governo britânico, sendo originalmente conhecido como *Government IT Infrastructure Management Method* (GITIMM). Em 1989, as melhores práticas informadas por diferentes organizações do setor público, privado e empresas de consultoria, foram consolidadas, integradas e nominadas como ITIL. Em 2001, o CCTA fundiu-se ao *Office of Government Commerce* (OGC), o qual atualmente possui os direitos sobre o material publicado sobre o ITIL.

O *IT Infrastructure Library* (ITIL) é um conjunto de práticas para prover serviços eficientes e efetivos de TI, além do gerenciamento da infra-estrutura de TI. O seu desenvolvimento foi motivado pelo fato das organizações estarem cada vez mais dependentes de TI para alcançarem os objetivos corporativos traçados. Essa dependência levou à necessidade de serviços de TI com qualidade, correspondendo aos objetivos de negócio de cada organização e atingindo os requerimentos e expectativas de seus clientes.

O ITIL oferece um *framework* comum para todas as atividades do departamento de TI, como parte do provimento do serviço, sendo baseado na infra-estrutura de TI. Essas atividades são divididas em processos, os quais criam um *framework* efetivo para tornar mais maduro o gerenciamento dos serviços de TI. Cada um dos processos cobre uma ou mais atividades pertinentes ao departamento de TI. Essa abordagem de processos permite descrever as melhores práticas de TI de forma independente da estrutura organizacional do departamento de TI.

Usando a abordagem de processos, o ITIL primariamente descreve o que deve ser incluído no gerenciamento de TI para prover serviços com a qualidade requerida. A estrutura e alocação de tarefas e responsabilidades entre funções e departamentos dependem do tipo de organização. A descrição da estrutura dos processos provê um ponto em comum de referência que muda lentamente e pode ajudar a manter a qualidade dos serviços de TI durante e depois de reorganizações entre provedores e parceiros.

O uso do ITIL é vantajoso para os consumidores/usuários finais devido aos seguintes fatores: o provimento dos serviços de TI torna-se mais focado nos consumidores; os serviços são descritos em linguagem inteligível para o cliente e a qualidade e os custos dos serviços são melhor gerenciados.

Para a própria organização que utiliza o ITIL, as vantagens são estas: a organização da TI desenvolve uma estrutura mais clara, tornando-se mais eficiente e focada nos objetivos corporativos; o gerenciamento é mais controlável e mudanças tornam-se mais facilmente gerenciáveis; o seguimento das melhores práticas providas pelo ITIL encoraja uma mudança cultural em direção ao provimento de serviço e suporta a introdução de um sistema de gerenciamento de qualidade

baseado na norma ISO-9000, e o ITIL provê um quadro de referência para comunicação interna e com os provedores e a padronização e identificação de procedimentos.

5. ANÁLISE COMPARATIVA DAS METODOLOGIAS COBIT E ITIL

A análise dos *frameworks* COBIT e ITIL torna claro que seus objetivos não são os mesmos, embora apresentem algumas similaridades: tratam do gerenciamento de processos genéricos, não restringem o segmento de negócio da organização que deseja aplicar o modelo para a otimização na gestão de TI; não abordam detalhes específicos de como implantar os controles em cada área de TI; são compatíveis com a maioria das ferramentas, modelos e normas para boas práticas de governança de TI existentes no mercado; permitem a realização de um *benchmark* entre a situação da organização e a situação do mercado; abordam de forma abrangente todo o gerenciamento de TI de uma organização; são orientados à processos e segmentam esses processos em objetivos/atividades, e geram produtos para todos os níveis da organização (para o operacional, aplicam-se as recomendações do que se deve fazer e como; para o nível tático, aplicam-se as métricas para se avaliar a execução dos processos de TI, e para o nível estratégico, aplica-se o alinhamento dos objetivos do negócio com os objetivos de TI da organização).

O COBIT é o modelo indicado para mapear a situação da área de TI de uma organização, como ela se posiciona em relação às melhores organizações do seu ramo e aos padrões internacionais, e onde a organização deseja chegar. Para essa tarefa são definidos os indicadores de desempenho, que medirão se a performance dos processos de TI está na direção correta para se atingir os objetivos. O COBIT deve ser utilizado como uma ferramenta para avaliação dos riscos e os resultados de sua aplicação podem ser utilizados para informar aos administradores se os processos de TI estão de acordo com os requerimentos do negócio.

O COBIT não determina como os processos devem ser estruturados, e sim os controles que eles devem possuir para que a TI cumpra seus objetivos em termos de governança, ou seja: alinhamento e entrega de valor por parte da área de TI para o negócio; correta alocação e medição dos recursos envolvidos; a mitigação dos riscos em TI.

O COBIT não apresenta formas para estruturar os processos ou implantar os controles, apenas aponta que controles devem ser implantados. Nessa estruturação surge a necessidade da utilização de ferramentas, conceitos e modelos que o complementem, umas delas é o ITIL.

O ITIL apresenta um foco menos estratégico, mais tático e operacional, voltado à identificação, organização, execução e padronização dos processos. Através da sua aplicação, pode-se atingir a eficiência dos processos, redução de riscos e conformidade estabelecidos através do COBIT.

O ITIL aponta as melhores práticas para todas as atividades gerenciais às quais for aplicado, como gerenciamento de incidentes, de problemas, financeiro, para serviços de TI e suporte, entre outras.

Para que as metodologias empregadas tenham resultados, é preciso que exista comprometimento da administração e investimento de recursos. É necessário ainda, realizar uma avaliação dos processos para a identificação das fragilidades e dos pontos fortes de TI na organização, identificando quais processos realmente precisam ser implantados, quais os pontos de maior risco e qual será o impacto nos outros setores da empresa.

6. INTEGRAÇÃO DAS METODOLOGIAS E PADRÕES PARA GOVERNANÇA E/OU GESTÃO DE TI

Visto que cada modelo foca em um aspecto específico da governança e gestão de TI, existem alternativas de integração de seus processos. O COBIT é focado na implantação da governança de TI e no controle dos processos, o ITIL é

focado no gerenciamento de serviços, porém algumas atividades são complementares.

Existem várias metodologias disponíveis no mercado e cada uma foca em um aspecto específico da governança ou gestão de TI, conforme a tabela 1.

Tabela 3 - Quadro comparativo de modelos e seus objetivos

Modelo	Objetivo	Foco Primário
BSC	Planejamento e gestão estratégica	Governança Corporativa
COBIT	Governança e controle de processos	Governança de TI
ITIL	Gerenciamento de serviços	Gerenciamento de TI
CMMI	Desenvolvimento de soluções	Gerenciamento de TI
ISO/IEC 9001	Qualidade de processos e produtos	Governança Corporativa
PMBok	Gerenciamento de projetos	Gerenciamento de TI
ISO/IEC 17799 e BS 7799	Segurança da Informação	Gerenciamento de TI
ISO/IEC 20000	Gestão de Serviços	Gerenciamento de TI
Conjunto de normas ISO/IEC 27000	Gerência da Segurança da Informação	Gerenciamento de TI
BS 15000	Gestão de Serviços	Governança de TI
PRINCE2	Gerenciamento de projetos	Gerenciamento de TI

As normas BS 15000 e ISO 20000 são alinhadas em seus objetivos com o modelo ITIL, sendo que o ITIL fornece o conjunto de melhores práticas que, uma vez adotadas, auxiliarão as organizações a encontrarem a qualidade de gestão de serviço requerida pelas normas BS 15000 e ISO 20000. O modelo ITIL serviu de

base para o desenvolvimento da BS 15000, que por sua vez serviu de base para o desenvolvimento da ISO 20000.

A norma britânica BS 7799 (*British Standard 7799*) é um código de práticas planejado para ser usado como referência para os gerentes e responsáveis pela segurança da informação nas organizações. Ela aborda os seguintes tópicos: avaliação de riscos, gestão de riscos, implementação de meios de segurança, declaração de aplicabilidade. A BS 7799 foi internacionalizada pelo padrão ISO/IEC 17799.

A série ISO 27000 está de acordo com outros padrões de sistemas de gerência ISO, como a ISO 9001. A ISO/IEC 27001 é um padrão para sistema de gerência da segurança da informação (ISMS - *Information Security Management System*). Seu objetivo é ser usada em conjunto com a ISO 17799. Essa família de normas contempla também padrões específicos para: vocabulário de gestão da segurança da informação, gestão de risco, mecanismos de mediação e de relatório de um sistema de gestão de segurança da informação e implementação, monitoramento e melhoria contínua do sistema de controles.

Embora com objetivos distintos, existem diversas áreas de intersecção entre os modelos apresentados. O *framework* COBIT e os padrões ISO 9001 e ISO 17799 podem ser utilizados na identificação do que deve ser gerenciado. Para como deve ser efetuada a gerência, pode-se utilizar COBIT, CMMI, ISO 17799 e PMBoK. Para o que deve ser executado pode-se utilizar ITIL, CMMI, ISO 17799 e PMBoK. Para os detalhes da execução é necessária a utilização de outras ferramentas e métodos específicos.

As melhores práticas de TI devem ser alinhadas às exigências do negócio e integradas com os procedimentos internos de cada organização. O COBIT pode ser utilizado em um nível mais elevado, fornecendo uma estrutura de controle baseada nos processos de TI. As áreas específicas devem ser cobertas por outros padrões como o ITIL ou as normas BS e padrões ISO, que podem ser integradas ao COBIT.

7. CONCLUSÃO

Para muitas organizações a Tecnologia da Informação representa um recurso precioso e um fator crítico para o negócio. Os desafios enfrentados na administração de TI são significativos e progressivos: os objetivos estratégicos do negócio dependem do desempenho da TI; a criticidade dos serviços prestados pela TI requer aumento da confiabilidade, disponibilidade e qualidade dos serviços; o aumento da complexidade e do custo dos recursos de TI precisa ser gerenciado dinamicamente; medidas regulatórias e demandas legais aumentam a visibilidade do desempenho e das fragilidades da área de TI.

A introdução da governança de TI na cultura de uma organização requer mudanças estruturais profundas, que necessitam de esforço e investimento. Nesse processo, é necessária uma análise da relação custoxbenefício e dos objetivos que a organização pretende atingir. As melhores práticas internacionais disponíveis representam a experiência prática acumulada por inúmeras empresas, profissionais de TI e auditores, o que poupa as organizações do esforço de desenvolvê-las, testá-las e, conseqüentemente, minimizando a possibilidade de erros.

Em um processo de implantação da governança de TI, uma abordagem inicial utilizando o modelo COBIT é recomendada. O COBIT atua em nível estratégico, apontando o que precisa ser feito para atingir a governança de TI, mas sem especificar como o processo deve ser realizado. Assim, em uma segunda etapa do processo de implantação da governança ou de aprimoramento dos controles internos da área de TI, recomenda-se a utilização de outros modelos, como o ITIL.

A aplicação do ITIL contribui para a implantação da governança em um nível mais tático, cobrindo aspectos relevantes para o gerenciamento de TI, em níveis distintos de detalhamento. Uma estratégia inicial para implementar ITIL é realizar uma avaliação dos processos da organização utilizando COBIT, dessa forma pode-se identificar as fraquezas e forças da estrutura de TI.

Existem outros modelos e padrões com focos em aspectos específicos da governança e gestão de TI, tais como CMMI, Prince2 e PMBoK, além de outras normas e padrões internacionais.

As melhores práticas devem ser encaradas como quadros de referência para as estruturas dos processos de TI, visando sua melhoria, e não como receitas de como se deve implementar os processos. Além disso, podem ser utilizadas como guias para melhor estruturar a TI da organização.

Os padrões e as melhores práticas não garantem sucesso na implantação da governança, sua eficácia depende de como foram executados e do comprometimento com a continuidade do processo. Porém, são bastante úteis quando aplicados como um guia para implantar e organizar procedimentos de controle específicos. Para evitar o obstáculo da resistência, a gerência e a equipe devem compreender o que fazer, como fazer e por que é importante.

A organização pode implementar quantos processos forem necessários, sempre observando se o custo e os benefícios da implantação estão de acordo com as estratégias do negócio. Os modelos e padrões apresentados, assim como a sua integração, permitem realizar uma avaliação detalhada da estrutura de TI, facilitando o gerenciamento e controle dos processos, e conseqüentemente, contribuindo para os objetivos da governança.

8. REFERÊNCIAS

DRAFT BS 7799-2:2002, Information Security Management - Part2: Specification for Information Security Management System. BSI, Novembro de 2001.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI**: da Estratégia à Gestão dos Processos e Serviços. Rio de Janeiro: Brasport, 2006.

HOLM, Michael Larsen; KÜHN, Mogens Pedersen; VIBORG, Kim Andersen. **IT Governance**: Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S. Proceedings of the 39th Hawaii International Conference on Systems Sciences - 2006. IEEE. Koloa, Kauai. Janeiro, 2006, p. 11.

IBGC. **Governança Corporativa**. Disponível em:
<<http://www.ibgc.org.br/ibConteudo.asp?IDArea=2>>

IETEC- Instituto de Educação Tecnológica. **ISO IEC 27000 e 20000 - os padrões para gerenciar a TI**. Disponível em:
<http://www.ietec.com.br/ietec/cursos/area_tecnologia_da_informacao/2007/05/24>

[/2007_05_24_0001.2xt/materia_gestao/2007_05_24_0344.2xt/dtml_boletim_inter_na>](#)

ISACA - Information Systems Audit and Control Association – 2006. Disponível em: <<http://www.isaca.org>>

ISO HOME <http://www.iso.org/iso/store.htm>

ISO 17799 World - <http://www.iso-17799-security-world.co.uk/>. Acesso em 20 de fevereiro de 2003

ISO 17799. Nascimento, Neide Landim Teixeira do Nascimento, UNEB - COPEX, Setembro de 2001.

ISO IEC INFORMATION CENTRE - <http://www.standardsinfo.net/isoiec/stdcat.html>

IT GOVERNANCE INSTITUTE – **COBIT 4.0** . 2005 - 2006. Disponível em: <<http://www.itgi.org>>

ITSMF - <<http://www.itsmf.com.br/itsmf/site/index.asp>>

Portal ISO 17799 - <http://www.iso17799.hpg.ig.com.br/>. Acesso em 20 de fevereiro de 2003.

WEILL, Peter; ROSS Jeanne. **Governança de TI: Tecnologia da Informação**. São Paulo: Mbooks, 2006.