



UNIVERSIDADE FEDERAL DE GOIÁS
ESCOLA DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

**ACORDOS DE NÍVEL DE OPERACIONAL
PARA O CONTROLE DO PROCESSO DE
MANUTENÇÃO DE SOFTWARE**

Marcia Schiavon

Orientador: Prof. Dr. Leonardo G. de R. Guedes

Goiânia

2006

Livros Grátis

<http://www.livrosgratis.com.br>

Milhares de livros grátis para download.

MARCIA SCHIAVON

**ACORDOS DE NÍVEL OPERACIONAL
PARA O CONTROLE DO PROCESSO DE
MANUTENÇÃO DE SOFTWARE**

Dissertação apresentada ao Curso de Mestrado em Engenharia Elétrica e de Computação da Universidade Federal de Goiás, para obtenção do título de Mestre em Engenharia de Informação e de Energia.

Área de concentração: Sistemas e Informação
Orientador: Prof. Dr. Leonardo Guerra de Rezende Guedes

Goiânia

2006

MARCIA SCHIAVON

**ACORDOS DE NÍVEL DE OPERACIONAL
PARA O CONTROLE DO PROCESSO DE
MANUTENÇÃO DE SOFTWARE**

Dissertação defendida e aprovada em 30 de setembro de 2006 pela
Banca Examinadora constituída dos seguintes professores:

Prof. Dr. Leonardo Guerra de Rezende Guedes
Presidente da Banca

Prof. Dr. Luis Fernando Ramos Molinaro

Prof. Dr. Rodrigo Pinto Lemos

A

Minha mãe, Stanley e Luísa.

Agradecimentos

À Universidade Federal de Goiás.

À Escola de Engenharia Elétrica e de
Computação.

Ao orientador Prof. Leonardo Guerra de
Rezende Guedes pelo acompanhamento
pontual e competente.

A todos os que direta ou indiretamente
contribuíram para a realização desta
pesquisa.

“Uma descoberta, seja feita por um menino na escola ou por um cientista trabalhando na fronteira do conhecimento, é em sua essência uma questão de reorganizar ou transformar evidências, de tal forma que se possa ir além delas assim reorganizadas, rumo a novas percepções.”

Jerone Bruner

SUMÁRIO

LISTA DE FIGURAS	10
LISTA DE TABELAS	12
LISTA DE TABELAS	12
LISTA DE QUADROS	13
RESUMO	14
ABSTRACT	15
1. Introdução	16
1.1 Objetivo Geral.....	18
1.2 Objetivos Específicos	18
1.3 Objeto da Pesquisa	18
1.4 Metodologia	20
1.5 Estrutura da Dissertação	21
2. CobiT	23
2.1 Visão Geral.....	26
2.2 O modelo do CobiT	35
2.3 Detalhamento do modelo de processos	36
3. ITIL	46
3.1 Visão Geral.....	48
3.2 Suporte de Serviços de TI	49
3.3 Entrega de Serviços de TI	56
4. Padrão IEEE para processos de engenharia de sistemas	65
4.1 O processo de engenharia de sistemas	67
4.2 O sub-processo de controle	67

5.	Revisão da Bibliografia.....	76
5.1	Manutenção de software	77
5.2	O Gerenciamento de TI	80
5.3	Governança.....	81
5.4	Lei Sarbanes-Oxley	89
5.5	Relatório de pesquisa global sobre governança.....	93
5.6	Casos	95
6.	Acordos de nível de serviço	98
6.1	Gerenciar Riscos.....	100
6.2	Gerenciar o prazo e o custo e garantir a qualidade da manutenção .	102
6.3	Gerenciar o desempenho da manutenção	104
6.4	Garantir a continuidade	104
6.5	Garantir a segurança.....	105
6.6	Treinar usuários.....	106
6.7	Gerenciar versões	106
7.	O modelo de acordos operacionais para controle do processo de manutenção de <i>software</i>	109
7.1	Gerenciar riscos	113
7.2	Gerenciar o prazo da manutenção	116
7.3	Gerenciar o custo da manutenção.....	119
7.4	Gerenciar o desempenho da manutenção	122
7.5	Garantir a continuidade	125
7.6	Garantir o controle da qualidade	128
7.7	Garantir a segurança.....	131
7.8	Treinar usuários.....	135
7.9	Gerenciar versões	139

8.	Conclusões.....	143
8.1	Recomendações para trabalhos futuros.....	145
9.	Referências Bibliográficas	146
	APÊNDICE	150

LISTA DE FIGURAS

Figura 2.1 – Publicações componentes do CobiT.....	24
Figura 2.2 – Exemplo da relação entre os processos, objetivos e métricas	35
Figura 2.3 – As dimensões do CobiT.....	36
Figura 2.4 – O modelo de processos CobiT	37
Figura 3.1 – Publicações componentes do ITIL.....	47
Figura 3.2 – Componentes típicos de um processo.....	50
Figura 3.3 – Processo do Atendimento ao cliente.....	51
Figura 3.4 – Processo Gerenciamento de Incidentes	52
Figura 3.5 – Os processos do Suporte de Serviços de TI e o Banco de Dados de Gerenciamento da Configuração	53
Figura 3.6 – As atividades do Gerenciamento de Versões	56
Figura 3.7 – Processo de Gerenciamento do Nível de Serviço	57
Figura 3.8 – Estrutura de suporte de um Acordo de Nível de Serviço	61
Figura 3.9 – Processo de Gerenciamento Financeiro dos Serviços de TI ...	62
Figura 3.10 – Processo de Gerenciamento da Capacidade	63
Figura 3.11 – Processo de Gerenciamento da Continuidade dos Serviços de TI	64
Figura 3.12 – Processo de Gerenciamento da Disponibilidade	64
Figura 4.1 – Os processos do ciclo de vida de um sistema no padrão 1220 do IEEE	66
Figura 4.2 – Detalhamento do processo de engenharia de sistemas	67
Figura 4.3 – Detalhamento do sub-processo de controle	68
Figura 5.1 – As áreas chaves de processos do CMM [PAU1995]	86
Figura 5.2 – As perspectivas do Balanced Scored Card [KAP1992].....	87

Figura 5.3 – Fases e disciplinas do RUP	88
Figura 5.4 – Atividades de TI para aderência à SOX [ITC2004].....	91
Figura 6.1 – A interação dos modelos de gestão COSO, ITIL, BS7799 e COBIT [GHN2005]	101

LISTA DE TABELAS

Tabela 5.1 – Situação da implementação de Governança de TI	94
Tabela 5.2 – Situação da implementação parcial de Governança	94
Tabela 5.3 – Modelos de Governança utilizados	95

LISTA DE QUADROS

Quadro 2.1 – Objetivos de TI x Objetivos de Negócio	27
Quadro 2.2 – Processos do CobiT x Objetivos de TI	29
Quadro 2.3 – Níveis do Modelo de Maturidade	33
Quadro 5.1 – Categorias de Manutenção de <i>Software</i> (ISO/IEC 14764).....	78
Quadro 5.2 – Os títulos da lei Sarbanes-Oxley.....	90

RESUMO

A exigência de qualidade nos produtos dos projetos de desenvolvimento de *software* cresce a cada dia. Especialmente importantes são os custos e a qualidade percebida no produto após sua implantação, ou ao iniciar-se o uso. Estima-se cerca de 80% do orçamento total do ciclo de vida de um produto associado a custos de manutenção de *software*.

Assim, devido à importância da fase de manutenção no ciclo de vida dos produtos de *software*, as organizações buscam as melhores práticas neste aspecto. O estabelecimento de acordos de nível de serviço representa uma dessas práticas. Esses acordos norteiam a execução de manutenções de *software* através da descrição dos critérios, restrições e procedimentos de mudança no escopo e na avaliação do serviço previsto.

Este trabalho propõe a definição de acordos de nível operacional para o controle do processo de manutenção de *software* orientados a aspectos de governança de tecnologia da informação.

São apresentados dois modelos de governança – CobiT e ITIL – difundidos mundialmente e utilizados como base teórica para proposição dos controles. São destacados os conceitos de manutenção de *software* e governança. O ciclo de vida de sistemas proposto pelo IEEE e a Lei Sarbanes-Oxley completam a fundamentação da proposta.

São propostos nove acordos operacionais de controle alinhados ao processo do ciclo de vida de sistemas do IEEE. É apresentado o mapeamento destes acordos junto ao CobiT, ITIL e à Lei Sarbanes-Oxley.

Palavras chave: Manutenção de Sistemas, Acordos de Nível Operacional, Governança de Tecnologia da Informação.

ABSTRACT

The requirement of quality in the products of the projects of software development grows to each day. Especially important they are the costs and the quality perceived in the product after its implantation, or when initiating their use. About 80% of the total budget of the life cycle of a product is related to the costs of software maintenance.

Thus, due to importance of the phase of maintenance in the life cycle of software products, the organizations search for best practices in this aspect. The establishment of service level agreements represents one of these practices. These agreements guide the execution of software maintenances through the description of the criteria, restrictions and procedures of change in the scope and in the evaluation of the foreseen service.

This work proposes the definition of operational level agreements for control the software maintenance process guided to the aspects of information technology governance.

Two models of governance are presented - CobiT and ITIL – both spread out world-wide and used as theoretical base for proposal of the controls. The concepts of software maintenance and governance are presented. The life cycle of systems as proposed by IEEE and the Sarbanes-Oxley Law completes the base of the proposal.

Nine operational level agreements are introduced lined up to the process of IEEE's systems life cycle. It is presented the mapping of these agreements next to the CobiT, ITIL and to the Sarbanes-Oxley Law.

Key-words: Software Maintenance, Operational Level Agreements, Information Technology Governance.

1. Introdução

Cada vez mais, exige-se qualidade nos produtos dos projetos de desenvolvimento de software. Durante um projeto desta natureza leva-se em conta aspectos de todo o ciclo de vida do produto, ou seja, do *software* aplicativo produzido. Com relação a custos, por exemplo, é necessário observar inclusive os custos necessários para a realização de uma análise de viabilidade do projeto ou mesmo custos de P&D – Pesquisa e Desenvolvimento [DIN2003].

São considerados ainda mais importantes os custos e a qualidade percebida no produto após sua implantação, ou ao iniciar-se o uso. Segundo Pfleeger, cerca de 80% do orçamento total do ciclo de vida de um *software* está associado a custos de manutenção de *software* [PFL2001].

Esse alto custo ocorre devido ao fato dos sistemas, após desenvolvidos, normalmente necessitarem de adaptações, seja devido a novos requisitos, mudanças no ambiente de negócio, novas oportunidades de mercado, atualização tecnológica ou mesmo devido a manutenções corretivas.

Assim, devido à importância da fase de manutenção no ciclo de vida dos produtos de *software*, as organizações buscam as melhores práticas neste aspecto. Contratos com empresas terceirizadas, especializadas neste tipo de serviço são comuns, tanto para manutenções corretivas quanto para manutenções evolutivas.

O estabelecimento de contratos de manutenção de software envolve a definição de acordos de nível de serviço – comumente chamados de SLAs – *Service Level Agreements*. Os SLAs norteiam a execução destes contratos através da descrição dos critérios, restrições e procedimentos de mudança no escopo e na avaliação do serviço previsto no contrato.

Contratos de apoio ou acordos operacionais também podem ser definidos, com o objetivo de auxiliar no controle e acompanhamento do processo de trabalho.

A utilização de acordos adequados – em ambos os níveis: de serviço e operacional – permite:

- A definição do grau de confiabilidade, portabilidade e disponibilidade esperado pela empresa proprietária do *software* a ser mantido pela empresa contratada;
- A avaliação do desempenho da empresa contratada no alcance dos acordos estabelecidos;
- Realização de previsões, análises de tendências e variações nas manutenções do *software*;
- A avaliação pós-implantação do projeto original de desenvolvimento do sistema aplicativo, externando falhas na condução do gerenciamento do projeto especialmente em termos de escopo e qualidade.

Neste contexto, a utilização de um modelo para definição de acordos de nível operacional em contratos de manutenção de *software* busca a melhor aplicação dos recursos das organizações, cada vez mais dependentes dos seus sistemas de *software* para executar suas atividades fins ou periféricas. Em consequência, a manutenção de *software* aparece como uma atividade estratégica de fundamental importância para a continuação da operação das próprias organizações.

1.1 Objetivo Geral

Este trabalho objetiva:

- Apresentar um modelo para definição de acordos de nível operacional para o controle do processo de manutenção de *software*.

1.2 Objetivos Específicos

Dentre os objetivos específicos deste trabalho, destacamos:

- Apresentar modelos de Governança de Tecnologia de Informação, especialmente nos aspectos aplicáveis à manutenção de *software*;
- Apresentar características técnicas particulares do processo de manutenção de *software*;
- Sugerir acordos de nível operacional adequados para processos desta natureza;
- Permitir a utilização dos acordos propostos em previsões, análises de tendências e variações durante o processo de manutenção.

1.3 Objeto da Pesquisa

1.3.1 Problema

O problema abordado neste trabalho pode ser descrito da seguinte maneira:

- Como aplicar um processo de desenvolvimento de software a sistemas desenvolvidos há vários anos? Como identificar e gerenciar os riscos de um projeto de manutenção de *software*?

1.3.2 Hipótese Básica

A hipótese básica deste projeto é:

- Um modelo para acordos de nível operacional pode ser proposto para realizar o controle do processo de manutenção de software.

1.3.3 Hipóteses Secundárias

As principais hipóteses secundárias deste projeto de pesquisa são:

- A manutenção de *software* possui características particulares a serem tratadas em um modelo para acordos de nível operacional;
- Acordos de nível operacional podem ser definidos orientados aos processos de governança de tecnologia da informação;
- A definição e utilização de acordos de nível operacional em processos de manutenção de *software* permitem realizar previsões, análises de tendências e variações durante o processo.

1.3.4 Variáveis

A corroboração ou refutação das hipóteses de estudos científicos é demonstrada pelas relações entre as variáveis componentes da pesquisa.

A variável independente (determinante, manipulada) deste estudo é:

- Determinação de um modelo para acordos de nível operacional em processos de manutenção de software

A variável moderadora (causa secundária) deste trabalho é:

- Alinhamento às proposições das teorias de governança de tecnologia da informação

As variáveis dependentes (conclusivas) deste projeto de pesquisa são:

- Avaliação do desempenho da empresa contratada para realizar a manutenção do *software* no alcance dos acordos operacionais estabelecidos;
- Realização de previsões, análises de tendências e variações nas manutenções do *software*;

- Avaliação pós-implantação do projeto original de desenvolvimento do sistema aplicativo, externando possíveis falhas na condução do gerenciamento do projeto especialmente em termos de escopo e qualidade.

1.4 Metodologia

O estudo da metodologia adequada para este trabalho baseou-se nos conceitos presentes na bibliografia assinada por Lakatos e Marconi [LAK2003].

1.4.1 Método de Abordagem

Neste trabalho utilizamos o método de abordagem hipotético-dedutivo. Partimos da constatação dos custos de manutenção de *software* representar parcela significativa no custo do ciclo de vida de sistemas de informação. Propomos a aplicação de um processo de manutenção e das teorias de Governança da Tecnologia da Informação para a determinação de um modelo para acordos de nível operacional para realizar o controle das atividades de manutenção de *software*.

1.4.2 Método de Procedimento

Esta pesquisa emprega o método estruturalista. Parte-se da investigação dos aspectos inerentes à manutenção de *software* e por intermédio da aplicação de teorias de ciclo de vida de sistemas e de Governança de Tecnologia da Informação propõe um modelo para acordos de nível de serviço em contratos dessa natureza.

1.4.3 Técnicas

Este estudo utiliza duas técnicas de pesquisa: documentação indireta e observação direta extensiva para verificação das hipóteses e variáveis.

A documentação indireta está presente na pesquisa bibliográfica necessária à fundamentação teórica do trabalho. A observação direta intensiva

é empregada nas entrevistas e exames dos fatos relacionados às particularidades dos contratos de manutenção de *software* nas organizações.

Não foi considerado escopo deste trabalho a aplicação do modelo proposto para efeito de sua validação.

1.4.4 Delimitação do Universo

Este trabalho visa propor um modelo para definição de acordos de nível operacional a serem aplicados por médias e grandes organizações no processo de manutenção de *software*.

1.5 Estrutura da Dissertação

Neste primeiro capítulo este trabalho apresenta os fundamentos metodológicos da pesquisa: problema, hipóteses, variáveis, métodos, técnicas e delimitação do universo. Após esta introdução, o texto é organizado em mais seis capítulos.

O universo teórico das premissas desta pesquisa são descritos nos seguintes trabalhos:

- CobiT – *Control Objectives for Information and related Technology*– Objetivos de Controle da informação e de Tecnologia da Informação [COB2005];
- ITIL – *Information Technology Infrastructure Library* – Conjunto de padrões e melhores práticas para o gerenciamento de serviços e infra-estrutura de Tecnologia da Informação [ITI2001];
- *Sarbanes-Oxley* – Lei *Sarbanes-Oxley* – Lei americana promulgada pelo governo americano em 2002 [SOX2002].

Desta forma, os dois capítulos seguintes são dedicados a apresentar os modelos de governança CobiT – no segundo capítulo – e ITIL no terceiro capítulo. Ambos modelos compreendem aspectos gerais da área de tecnologia da informação. A transcrição exposta nestes capítulos sobre os modelos de

governança tem foco nos aspectos relativos a acordos de nível operacional e manutenção de *software*, objetos deste estudo.

O quarto capítulo contempla o modelo de ciclo de vida de sistemas proposto pelo padrão 1220-1998 do IEEE – *Institute of Electrical and Electronics Engineers*, o processo de engenharia de sistemas e mais especificamente o sub-processo de controle e suas atividades.

No quinto capítulo é abordada uma revisão bibliográfica sobre os assuntos abordados neste trabalho: manutenção de *software*, governança, acordos de nível de serviço. São expostos os tipos de manutenção de sistemas e sua importância. Os conceitos de governança e de governança de tecnologia da informação são apresentados, seguidos de breves descrições de modelos auxiliares de governança, tais como BSC – *Balanced Score Card*, CMM – *Capability Maturity Model*, guia do PMBoK – *Project Management Body of Knowledge*, entre outros.

Ainda dentro da revisão bibliográfica é explorada a lei americana *Sarbanes-Oxley*, particularmente os aspectos relacionados a controles de tecnologia da informação.

Um relatório de pesquisa global sobre governança e casos de implantação de governança em organizações nacionais e internacionais também compõem o quarto capítulo.

Os acordos de nível de serviço são abordados no capítulo seis, onde é demonstrada a sua importância e são comentados os acordos operacionais propostos no modelo do capítulo seguinte.

O sétimo capítulo apresenta o modelo de acordos operacionais para controle do processo de manutenção de *software* orientados à governança de tecnologia da informação. Neste ponto estão formatados nove acordos, seus indicadores, localização no processo de manutenção de *software* e relação com os modelos de governança CobiT, ITIL e com a lei *Sarbanes-Oxley*.

Finalmente, no oitavo capítulo, são apresentadas as conclusões da pesquisa, sugestões e recomendações de trabalhos futuros relacionados ao tema.

2. CobiT

Em 1967, um pequeno grupo de auditores de sistemas de informação críticos para suas organizações reuniu-se para discutir a necessidade de uma fonte centralizada de informação para a área. Em 1969 esse grupo tornou-se uma associação formal e em 1976 formou uma fundação educacional com o objetivo de empreender pesquisas e expandir o conhecimento e o valor da governança e controle da Tecnologia da Informação.

Denominada Associação de Auditoria e Controle de Sistemas de Informação (*Information Systems Audit and Control Association – ISACA*) atualmente essa associação conta com membros em mais de 140 países, atuantes em áreas tais como auditoria, consultoria, educacional e profissionais de segurança da informação de diferentes áreas de negócio. A ISACA atua, através de seções regionais, em mais de 60 países, promovendo o estudo, compartilhamento de recursos e experiências entre seus membros.

Em 1998 foi criado o *IT Governance Institute – ITGI*, componente da ISACA, com o objetivo de promover o estudo de padrões de controle e direção da tecnologia da informação nas organizações. A efetiva governança da Tecnologia da Informação ajuda a garantir o alinhamento aos objetivos do negócio, a obter resultados dos investimentos na área e gerenciamento dos riscos e oportunidades associados. O ITGI oferece material de pesquisa para assistir as organizações em suas responsabilidades de governança.

Dentre os produtos do ITGI está o CobiT – *Control Objectives for Information and related Technology*, publicação composta por um conjunto de objetivos de controle de Tecnologia da Informação produzida com o objetivo de ser um recurso educacional para CIOs (*Chief Information Officers*), diretores e profissionais de gerenciamento e controle de TI.

A terceira versão do CobiT, lançada em julho de 2000, é a utilizada atualmente nas empresas. Em sua versão mais recente, lançada em dezembro de 2005, o CobiT 4.0 enfatiza a aderência a questões regulatórias, ajuda as organizações a aumentar o valor obtido da TI, permite o alinhamento e simplifica a implementação do modelo.

As publicações do CobiT estão organizadas em três níveis, para atender, em cada nível: a alta administração, gerentes de negócios e de TI e profissionais de governança, segurança e controle respectivamente. Os níveis e produtos do CobiT são apresentados na figura 2.1

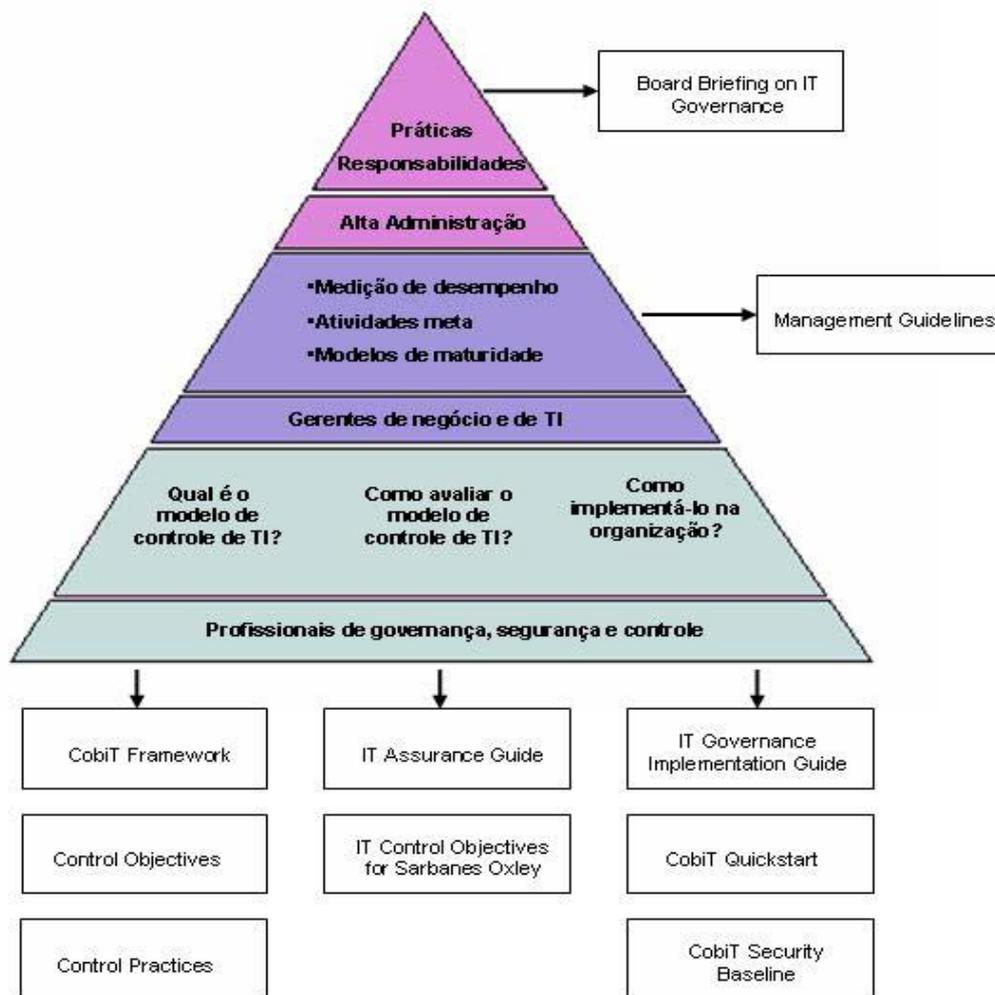


Figura 2.1 – Publicações componentes do CobiT

A publicação de maior interesse para a alta administração é o *Board Briefing on IT Governance*, onde é descrita a importância da governança de TI e quais questões são de sua responsabilidade neste contexto.

O documento *Management Guidelines* é dirigido principalmente a gerentes de negócios e de TI. Esta publicação orienta a atribuição de responsabilidades, a medição de desempenho, a realização de comparações e a identificação de falhas.

As demais publicações são orientadas aos profissionais de governança, segurança e controle:

- *Framework*, onde são descritos a organização dos objetivos e melhores práticas da governança de TI e os domínios e processos associados aos requisitos de negócio;
- *Control Objectives* provê as melhores práticas de gerenciamento dos objetivos genéricos para todas as atividades de TI;
- *Control Practices* justifica a importância de cada controle e orienta sua implementação;
- *IT Assurance Guide* provê uma abordagem para auditoria dos processos;
- *IT Controle Objectives for Sarbanes-Oxley*, contendo a orientação de aderência à Lei Sarbanes-Oxley (abordada na seção 4.5), através dos objetivos de controle do CobiT;
- *IT Governance Implementation Guide*, guia para a implementação da governança de TI através do modelo proposto pelo CobiT nas organizações;
- *CobiT Quickstart*, indicado para pequenas organizações ou como o passo inicial em organizações maiores;
- *CobiT Security Baseline*, com foco na segurança da informação dentro da organização.

As publicações dirigidas a diferentes perfis proporcionam o atendimento aos interesses e necessidades particulares de área de atuação. Para a alta administração o CobiT orienta a obtenção do retorno dos investimentos em TI, gerenciamento dos riscos e controle do investimento. Os gerentes de negócio obtêm garantia do gerenciamento e controle efetivo dos serviços providos por funcionários internos ou terceiros. Gerentes de TI provêm serviços gerenciados e controlados, para atingir aos requisitos e estratégia do negócio. Por fim, o CobiT substancia as opiniões de auditores e provê orientação para verificação dos controles internos.

2.1 Visão Geral

O CobiT é um modelo estruturado, composto por um conjunto de diretrizes baseadas em auditoria de processos, práticas e controles para a governança de Tecnologia da Informação. Voltado para a redução de risco, enfoca integridade, confiabilidade e segurança. Possui foco maior no controle e menor na execução.

As práticas tratadas pelo modelo visam tornar mais rentáveis os investimentos em TI, garantir a entrega de serviços e prover uma métrica para identificar atividades inadequadas. Para isso, o CobiT realiza o alinhamento e organização dos processos de TI aos requisitos de negócio, identifica os recursos de TI a serem considerados em cada atividade de cada processo e define os objetivos de controle a serem gerenciados.

O foco no negócio presente no CobiT consiste no estabelecimento da relação entre os objetivos do negócio aos objetivos de TI, provendo métricas e modelos de maturidade para medir esta relação e identificando as responsabilidades associadas a cada processo de TI e de negócio.

A orientação a processos, característica presente no modelo, constitui a forma de gerenciar as atividades de TI. O CobiT provê um modelo de processos genérico onde representa todos os processos usualmente encontrados em funções de TI, fornecendo um modelo de referência comum, compreensível tanto para gerentes de TI quanto para gerentes de negócios. Os quadros 2.1 e 2.2 demonstram a relação estabelecida entre os objetivos de negócio, os objetivos de TI e os processos do CobiT para implementar esses objetivos. No Quadro 2.1 são relacionados objetivos de negócio genéricos e os objetivos de TI associados. O relacionamento entre os objetivos de TI e os processos do CobiT é demonstrado no Quadro 2.2.

Os processos precisam de controle. Controles são desenvolvidos através de políticas, procedimentos, práticas e estruturas organizacionais. A definição de controles tem por objetivo garantir o alcance dos objetivos a existência de prevenção contra eventos indesejáveis, ou, ainda a detecção e correção desses eventos.

	Expandir a participação no mercado	Aumentar receitas	Retorno do investimento	Utilizar melhor os recursos	Gerenciar os riscos do negócio	Aumentar a orientação ao cliente e aos serviços	Oferecer produtos e serviços competitivos	Disponibilidade dos serviços	Agilidade em responder a mudanças dos requisitos de negócios	Eficiência financeira da entrega de serviços	Automatizar e integrar a cadeia de valor do negócio	Melhorar e manter a funcionalidade do processo de negócio	Diminuir o custo do processo	Aderência a leis e regulamentos externos	Transparência	Aderência a políticas internas	Melhorar e manter a produtividade de recursos humanos de operação e apoio	Inovação de produtos e do negócio	Obter informações úteis e confiáveis para a tomada de decisões estratégicas	Contratar e manter pessoal qualificado e motivado
Obter a melhor utilização da infra-estrutura, recursos e capacidade da área													✓							
Reduzir o retrabalho e os defeitos das soluções e serviços prestados								✓												
Buscar a realização dos objetivos de TI					✓															
Estabelecer claramente o impacto dos riscos do negócio aos objetivos e recursos da área					✓										✓					
Garantir que informações críticas e confidenciais não estão ao alcance daqueles que não devem acessá-las					✓									✓						
Garantir que transações automatizadas e trocas de informações são confiáveis					✓									✓					✓	
Garantir que os serviços e infra-estrutura de TI resistem e se recuperam de falhas devido a erros, ataques ou desastres					✓									✓						
Garantir impacto mínimo no negócio em caso de interrupção ou mudança de um serviço					✓			✓						✓						
Garantir que os serviços permanecem disponíveis conforme requerido						✓		✓												
Aumentar a eficiência financeira da área e a sua contribuição para a lucratividade da organização			✓				✓			✓			✓							
Entregar projetos no prazo e custo planejados, mantendo os padrões de qualidade	✓	✓							✓									✓		
Manter a integridade da informação e a infra-estrutura de processamento														✓					✓	
Garantir a aderência da TI a leis e regulamentos														✓						
Garantir a demonstração de serviços de qualidade e eficiência financeira, de melhoria contínua e prontidão a mudanças futuras	✓	✓																✓		

Quadro 2.2 – Processos do CobiT x Objetivos de TI

	Responder aos requisitos de negócio alinhado à estratégia do negócio	Responder aos requisitos de governança alinhado à alta direção	Garantir a satisfação dos usuários finais com os serviços disponíveis e com o nível desses serviços	Extraí-los mais resultados das informações	Agilizar a área de Tecnologia da Informação	Definir como os requisitos funcionais e de controle do negócio são traduzidos em soluções efetivas e eficientes	Adquirir e manter sistemas aplicativos integrados e padronizados	Adquirir e manter uma infra-estrutura de TI integrada e padronizada	Adquirir e manter conhecimentos e habilidades de TI que respondem à estratégia da área	Garantir satisfação mútua no relacionamento com terceiros	Integrar sistemas aplicativos e soluções técnicas de forma transparente para os processos de negócio	Garantir transparência e o entendimento dos custos, benefícios, estratégias, políticas e níveis de serviço da área	Garantir o uso apropriado e o desempenho dos sistemas aplicativos e soluções técnicas	Identificar e proteger os recursos de TI	Obter a melhor utilização da infra-estrutura, recursos e capacidade da área	Reduzir o retrabalho e os defeitos das soluções e serviços prestados	Buscar a realização dos objetivos de TI	Estabelecer claramente o impacto dos riscos do negócio aos objetivos e recursos da área	Garantir que informações críticas e confidenciais não estão ao alcance daqueles que não devem acessá-las	Garantir que transações automatizadas e trocas de informações são confiáveis	Garantir que os serviços e infra-estrutura de TI resistem e se recuperam de falhas devido a erros, ataques ou desastres	Garantir impacto mínimo no negócio em caso de interrupção ou mudança de um serviço	Garantir que os serviços permanecem disponíveis conforme requerido	Aumentar a eficiência financeira da área e a sua contribuição para a lucratividade da organização	Entregar projetos no prazo e custo planejados, mantendo os padrões de qualidade	Manter a integridade da informação e a infra-estrutura de processamento	Garantir a aderência da TI a leis e regulamentos	Garantir a demonstração de serviços de qualidade e eficiência financeira, de melhoria contínua e prontidão a mudanças futuras	
Definir um planejamento estratégico de TI	✓	✓																											
Definir a arquitetura da informação	✓		✓	✓							✓																		
Determinar a direção tecnológica							✓								✓														
Definir os processos, a organização e relacionamentos de TI	✓	✓			✓																								
Gerenciar o investimento em TI												✓																	✓
Comunicar as metas da gerência												✓	✓						✓	✓	✓	✓							
Gerenciar recursos humanos de TI					✓			✓																					
Gerenciar a qualidade			✓												✓										✓				
Avaliar e gerenciar os riscos da área													✓				✓	✓											
Gerenciar projetos	✓	✓																							✓				
Identificar soluções automatizadas	✓					✓																							
Adquirir e manter sistemas aplicativos						✓	✓																						
Adquirir e manter infra-estrutura tecnológica					✓			✓							✓														
Habilitar a operação e utilização			✓								✓	✓			✓														
Contratar recursos de TI							✓	✓	✓																				
Gerenciar mudanças	✓					✓									✓											✓			
Instalar e validar soluções e	✓										✓	✓			✓								✓			✓			

	Responder aos requisitos de negócio alinhado à estratégia do negócio	Responder aos requisitos de governança alinhado à alta direção	Garantir a satisfação dos usuários finais com os serviços disponíveis e com o nível desses serviços	Extrair mais resultados das informações	Agilizar a área de Tecnologia da Informação	Definir como os requisitos funcionais e de controle do negócio são traduzidos em soluções efetivas e eficientes	Adquirir e manter sistemas aplicativos integrados e padronizados	Adquirir e manter uma infra-estrutura de TI integrada e padronizada	Adquirir e manter conhecimentos e habilidades de TI que respondem à estratégia da área	Garantir satisfação mútua no relacionamento com terceiros	Integrar sistemas aplicativos e soluções técnicas de forma transparente para os processos de negócio	Garantir transparência e o entendimento dos custos, benefícios, estratégias, políticas e níveis de serviço da área	Garantir o uso apropriado e o desempenho dos sistemas aplicativos e soluções técnicas	Identificar e proteger os recursos de TI	Obter a melhor utilização da infra-estrutura, recursos e capacidade da área	Reduzir o retrabalho e os defeitos das soluções e serviços prestados	Buscar a realização dos objetivos de TI	Estabelecer claramente o impacto dos riscos do negócio aos objetivos e recursos da área	Garantir que informações críticas e confidenciais não estão ao alcance daqueles que não devem acessá-las	Garantir que transações automatizadas e trocas de informações são confiáveis	Garantir que os serviços e infra-estrutura de TI resistem e se recuperam de falhas devido a erros, ataques ou desastres	Garantir impacto mínimo no negócio em caso de interrupção ou mudança de um serviço	Garantir que os serviços permanecem disponíveis conforme requerido	Aumentar a eficiência financeira da área e a sua contribuição para a lucratividade da organização	Entregar projetos no prazo e custo planejados, mantendo os padrões de qualidade	Manter a integridade da informação e a infra-estrutura de processamento	Garantir a aderência da TI a leis e regulamentos	Garantir a demonstração de serviços de qualidade e eficiência financeira, de melhoria contínua e prontidão a mudanças futuras		
mudanças																														
Definir e gerenciar níveis de serviço	✓		✓									✓																		
Gerenciar serviços de terceiros			✓							✓		✓																		
Gerenciar desempenho e capacidade	✓														✓								✓							
Garantir a continuidade dos serviços																				✓	✓	✓								
Garantir a segurança dos sistemas													✓						✓	✓	✓					✓				
Identificar e alocar custos												✓												✓						✓
Educar e treinar usuários			✓										✓																	
Gerenciar incidentes e o atendimento ao usuário			✓										✓										✓							
Gerenciar a configuração													✓	✓																
Gerenciar problemas			✓												✓	✓														
Gerenciar dados				✓																										
Gerenciar o ambiente físico													✓																	
Gerenciar operações			✓																				✓							
Monitorar e avaliar o desempenho de TI	✓	✓										✓										✓								✓
Monitorar e avaliar o controle interno													✓				✓					✓								
Garantir aderência regulatória																												✓		
Prover governança de TI		✓										✓																✓		✓

O CobiT é um modelo baseado em controles. Os objetivos de controle de cada processo representam os requisitos mínimos para alcançar o propósito ou resultado desejado com a atividade. Cada processo do modelo possui um objetivo de controle de alto-nível e um conjunto de objetivos de controle detalhados. Juntos, esses objetivos de controle representam as características de um processo bem gerenciado.

Além dos objetivos de controle detalhados, cada processo do modelo é caracterizado por mais seis requisitos de controle:

- Responsável: torna explícita a responsabilidade sobre o processo;
- Repetibilidade: define cada processo de forma a poder ser repetido;
- Metas e objetivos: estabelece metas e objetivos claros para cada processo;
- Papéis e responsabilidades: define claramente papéis, atividades e responsabilidades na execução do processo;
- Desempenho: mede o desempenho do processo em comparação com suas metas e
- Políticas, planos e procedimentos: documenta, revisa, atualiza, formaliza e comunica a todos os envolvidos quaisquer política, plano ou procedimento orientadores do processo.

O modelo apresenta ainda, para cada processo: exemplos de entradas e saídas, atividades e orientações sobre papéis e responsabilidades; objetivos-chaves da atividade e métricas.

A identificação das entradas e saídas de um processo permite ao responsável por um processo o entendimento sobre quais informações necessita de outros processos e quais informações deve prover a outros processos. Por outro lado, a compreensão dos perfis e responsabilidades é extremamente importante. O modelo apresenta, em cada processo, um quadro identificando quem é responsável, aprova, é consultado ou informado da atividade. O papel do “responsável” é fazer a atividade acontecer. A “aprovação” é realizada por quem possui o papel de autorizar a atividade. A

informação das pessoas “consultadas” e “informadas” garante o envolvimento de todos os interessados no processo.

Outra característica do CobiT é ser dirigido a métricas. Uma necessidade básica para toda organização é conhecer o estado de seus sistemas informatizados e decidir qual nível de gerenciamento e controle deve realizar. Nesse sentido, o CobiT provê um modelo de maturidade, métricas e metas de desempenho.

2.1.1 O modelo de maturidade

O CobiT realiza a avaliação da maturidade para o gerenciamento e controle de processos de TI através dos próprios processos existentes no modelo: partindo de não existente – o nível mais baixo de maturidade, a otimizado – o nível mais alto. Esta abordagem é derivada do modelo de maturidade definido pelo *Software Engineering Institute* para avaliar a maturidade no desenvolvimento de software, chamado CMM – *Capability Maturity Model*.

O modelo de maturidade do CobiT é definido para cada processo, ou seja, os níveis de maturidade não são determinados genericamente para toda a organização, mas para cada um dos 34 processos componentes do modelo. Esses níveis de maturidade são definidos como características a serem reconhecidas nos processos de TI da organização. Desta forma, o modelo de maturidade permite identificar:

- O desempenho atual da organização – onde a empresa está no momento;
- O estado atual da área de negócio da organização – a comparação e
- O desempenho-alvo da organização – onde a empresa deseja chegar.

O modelo de maturidade é aplicado em cada processo conforme o padrão apresentado no Quadro 2.3 – Níveis do Modelo de Maturidade.

Quadro 2.3 – Níveis do Modelo de Maturidade

0 – Não existente	Ausência completa de qualquer processo identificável. A organização nem mesmo identifica a existência de uma questão a ser tratada
1 – Inicial	Há evidências de identificação, na empresa, da existência de questões a serem tratadas. Entretanto, não são executados processos padronizados, mas diferentes abordagens aplicadas em casos específicos. A visão geral é de falta de organização da gerência
2 – Repetível	Os processos foram desenvolvidos a um estágio no qual procedimentos similares são seguidos por pessoas diferentes fazendo o mesmo trabalho. Não há treinamento formal ou comunicação de procedimentos padronizados, a responsabilidade pertence a cada indivíduo. Há um grande grau de confiança no conhecimento de cada um, conseqüentemente, os erros são comuns
3 – Definido	Os procedimentos são padronizados e documentados, e comunicados através de treinamento. Entretanto, ainda é responsabilidade de cada indivíduo seguir os processos, sendo improvável a detecção de desvios. Os procedimentos representam a formalização das práticas existentes
4 – Gerenciado	É possível monitorar e medir a real aplicação dos procedimentos e agir sobre as áreas onde os processos não estiverem apropriados. Os processos estão em constante melhoria. Ferramentas automatizadas são utilizadas de forma limitada ou parcial.
5 – Otimizado	Os processos são refinados ao nível de melhores práticas, baseados no resultado de melhoria contínua e de comparação com outras organizações. A TI é utilizada de forma integrada para automatizar o fluxo de processos, provendo subsídios à melhoria da qualidade e efetividade dos processos.

2.1.2 Medição do desempenho

Os objetivos e métricas são definidos em três níveis no CobiT:

- Objetivos e métricas de TI: definem a expectativa do negócio sobre a área de Tecnologia da Informação;
- Objetivos e métricas de processos: definem quais resultados dos processos de TI indicam o alcance dos referidos Objetivos de TI e
- Métricas de desempenho do processo: indicam a probabilidade de alcance dos Objetivos de Processos.

O CobiT utiliza dois tipos de métricas: indicadores de objetivos e de desempenho. Os indicadores de objetivo do nível mais baixo são os indicadores de desempenho do nível mais alto.

Os Indicadores-Chave de Objetivos, ou *KGI – Key Goal Indicators*, definem métricas para demonstrar se um processo atingiu os requisitos de negócio, normalmente explícitos em termos dos seguintes critérios:

- Disponibilidade da informação;
- Integridade e confidencialidade da informação;
- Eficiência financeira dos processos e
- Confiabilidade, eficácia e adequação.

Os Indicadores-Chave de Desempenho, ou *KPI – Key Performance Indicators*, definem métricas para demonstrar o quanto um processo de TI leva ao alcance do objetivo. Esses indicadores não demonstram habilidades, práticas e potencialidades. Por outro lado, medem os objetivos das atividades, ou quais são as ações necessárias para o responsável pelo processo atingir seu efetivo desempenho.

A figura 2.2 traz um exemplo da relação entre os processos, objetivos de negócio e de TI e métricas para o processo do CobiT: Garantir a segurança dos sistemas.

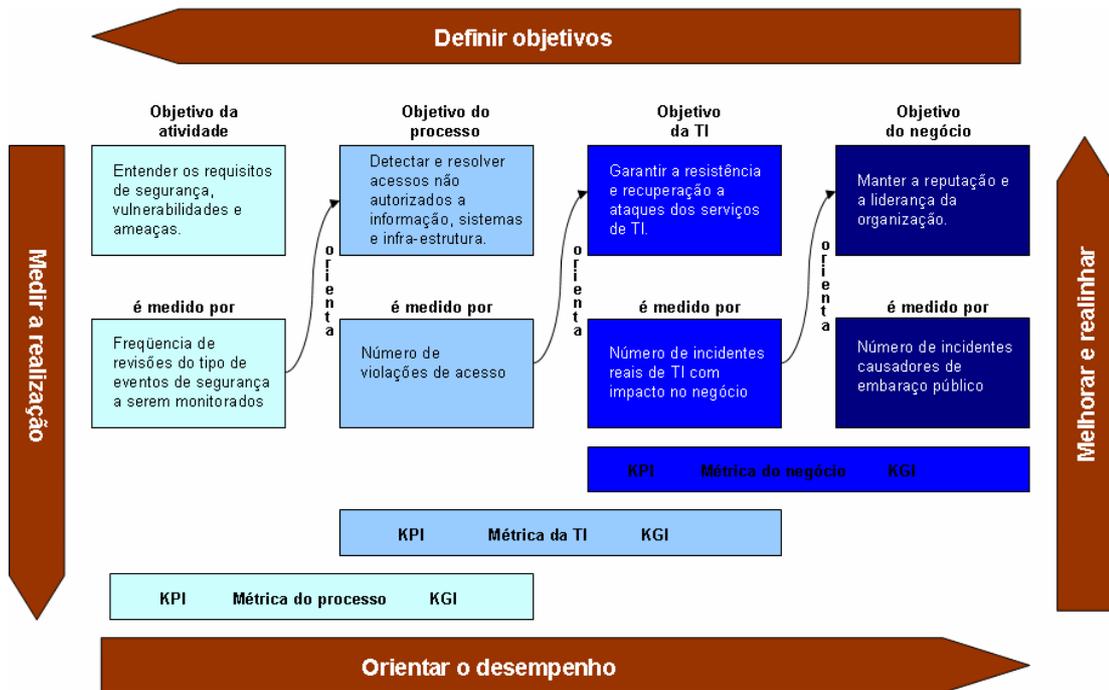


Figura 2.2 – Exemplo da relação entre os processos, objetivos e métricas

2.2 O modelo do CobiT

O modelo de processos do CobiT propõe-se a relacionar os requisitos de informação e governança da organização aos objetivos dos serviços de TI. No modelo, as atividades e os recursos utilizados pela área são definidos de forma a permitir o gerenciamento e controle baseado nos objetivos de controle, alinhados e monitorados através dos Indicadores-Chave de Objetivos e dos Indicadores-Chave de Desempenho.

A figura 2.3 demonstra o princípio básico do modelo. No CobiT, os recursos são gerenciados pelos processos de TI para alcançar os objetivos da própria TI visando responder aos requisitos de negócio.

Os processos do CobiT são organizados em quatro domínios:

- Planejamento e Organização;
- Aquisição e Implementação;
- Entrega e Suporte e
- Monitoração e Avaliação.

Dentro dos domínios de processos estão distribuídos os 34 objetivos de controle descritos de forma a proporcionar uma visão completa da TI, detalhando os recursos essenciais para cada processo, tais como infraestrutura, pessoal, informações e sistemas aplicativos. A figura 2.4 apresenta o modelo de processos de quatro domínios, contendo 34 objetivos de controle, gerenciando os recursos de TI para prover a informação à organização, de acordo com os requisitos de governança e do negócio.

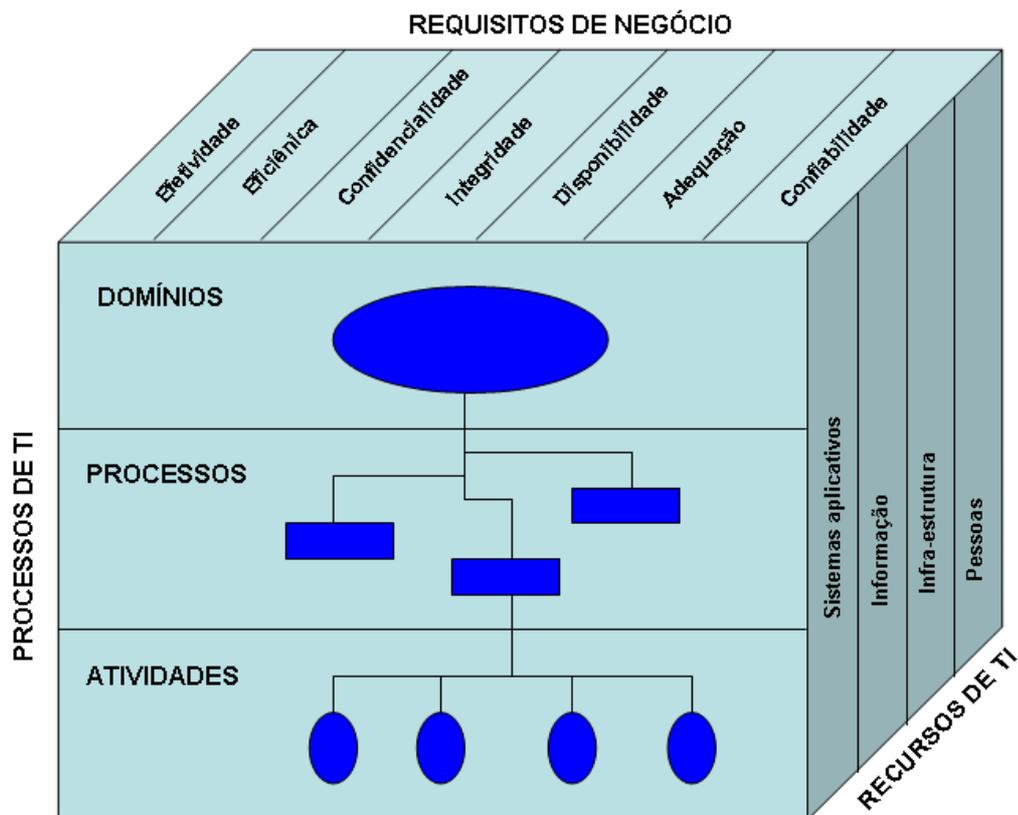


Figura 2.3 – As dimensões do CobiT

2.3 Detalhamento do modelo de processos

Nesta seção estão detalhados os controles cujos aspectos serão utilizados no modelo para acordos de nível de serviço em contratos de manutenção de software proposto no capítulo sete.

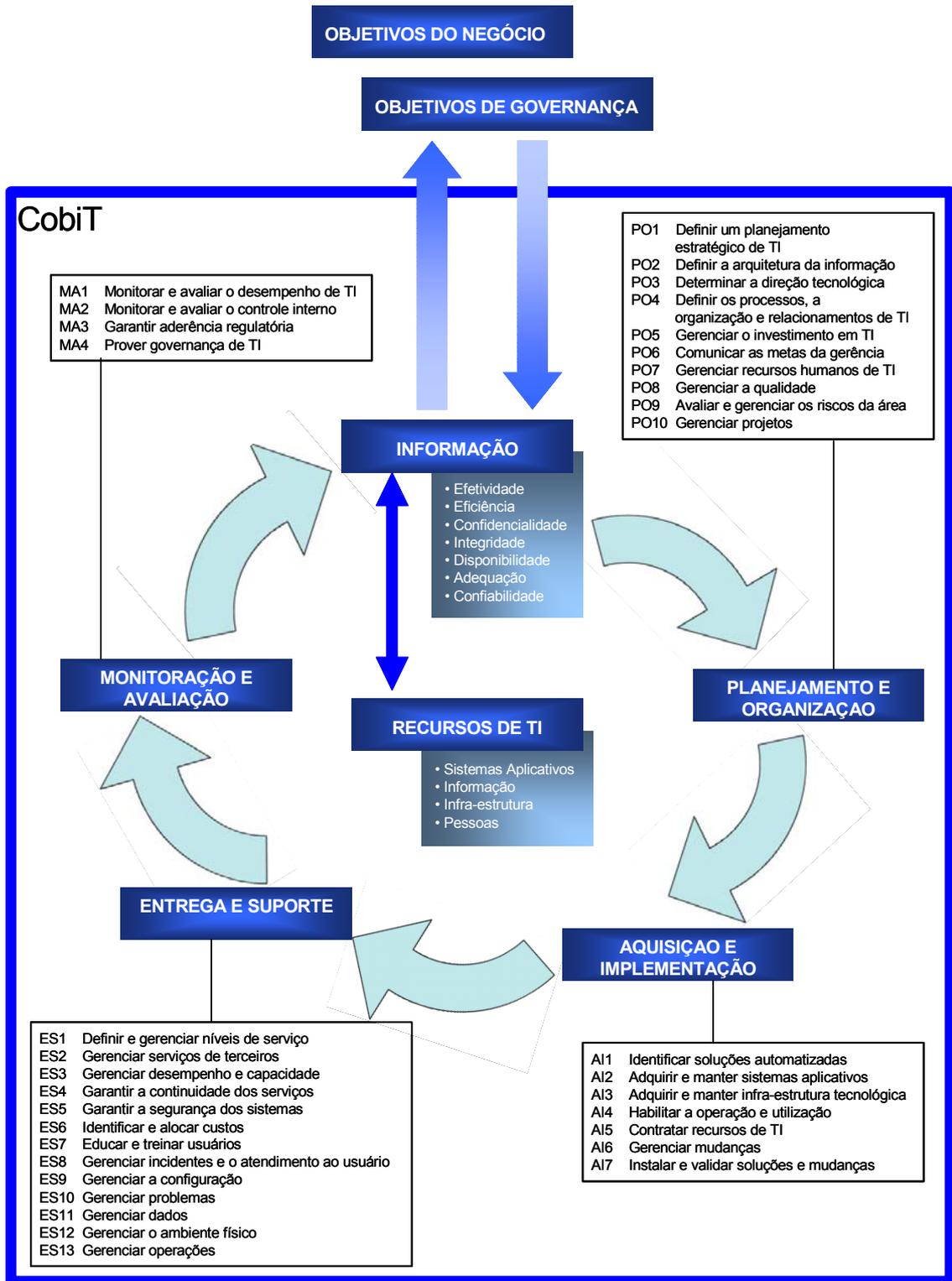


Figura 2.4 – O modelo de processos CobiT

O processo Avaliar e gerenciar os riscos da área, dentro do domínio de Planejamento e Organização propõe a criação e manutenção de um modelo de gerenciamento de riscos. Qualquer impacto potencial nos objetivos da organização causado por um evento não planejado deve ser identificado, analisado e avaliado. Estratégias de redução de riscos devem ser adotadas com o objetivo de minimizar riscos residuais a um nível aceitável. O resultado da avaliação deve ser compreensível para as partes envolvidas e expressa em termos financeiros, permitindo o alinhamento do risco ao nível de tolerância admitido.

De forma mais detalhada, a avaliação e gerenciamento dos riscos da Tecnologia da Informação é composta por:

1. Alinhamento do gerenciamento dos riscos de TI aos riscos do negócio, inclusive em relação aos aspectos de apetite e a riscos;
2. Estabelecimento dos contextos interno e externo de avaliação de riscos, o objetivo e critérios da avaliação;
3. Identificação dos eventos de riscos – ameaças e vulnerabilidades – com impacto potencial (positivo ou negativo) ao negócio, sejam eventos de natureza regulatória, legal, tecnológica, operacional, humana ou de mercado;
4. Avaliação da probabilidade e impacto dos riscos identificados através de métodos qualitativos e quantitativos;
5. Identificar responsáveis pelos riscos e pelos processos afetados, desenvolver e manter uma estratégia de resposta (evitar, reduzir, compartilhar ou aceitar) considerando os custos e benefícios envolvidos e o nível de tolerância aceitável para riscos residuais;
6. Manter e monitorar um plano de ação de resposta a riscos identificando custos, benefícios e responsáveis por sua execução.

Gerenciar projetos é outro processo pertencente ao domínio de Planejamento e Organização utilizado no modelo de acordos de nível de serviço apresentado neste trabalho. Deve-se estabelecer e aplicar um modelo

de gerenciamento de todos os programas e projetos de TI garantindo a correta priorização e coordenação de todos os projetos. Os elementos componentes do modelo são: um plano mestre, atribuição de recursos, definição de entregas, aprovação de usuários, abordagem de entrega por fases, garantia da qualidade, plano formal de testes, realização dos testes e a revisão pós-implantação. Tal estratégia tem por objetivos reduzir o risco de custos inesperados e o cancelamento de projetos, aumentar a comunicação e envolvimento de clientes e usuários e garantir a qualidade e o valor agregado em cada entrega, aumentando a contribuição de cada projeto nos programas de investimento em TI.

Detalhadamente, o controle do gerenciamento de projetos envolve:

1. Manutenção de um modelo de programação de projetos, envolvendo as atividades de identificar, definir, avaliar, priorizar, selecionar, gerenciar e controlar os projetos alinhados ao *portfolio* de investimentos em TI;
2. Estabelecimento e manutenção de um modelo de gerenciamento dos projetos empreendidos onde sejam abordados os aspectos de definição de escopo, fronteiras e metodologias a serem utilizadas, envolvendo os aspectos de iniciação, planejamento, execução, controle e encerramento; pontos de controle e aprovação;
3. Estabelecimento de uma abordagem de gerenciamento proporcional ao tamanho, complexidade e exigências regulatórias do projeto e explicitação de papéis e responsabilidades dos envolvidos e de mecanismos de reporte de desempenho;
4. Obtenção do compromisso e participação das partes interessadas afetadas na definição e na execução do projeto dentro do contexto do programa de investimento;
5. Definição, documentação e aprovação formais da natureza e do escopo do projeto visando confirmar e desenvolver entre os envolvidos uma compreensão comum do escopo do

projeto e sua relação com outros projetos dentro do programa de investimento;

6. Comunicação e aprovação formal da iniciação das fases principais do projeto às partes interessadas e aprovação das fases subseqüentes baseada na revisão e na aceitação das entregas da fase precedente;
7. Elaboração de um plano de projeto integrado e formal para orientar sua execução e controle;
8. Definição das responsabilidades, relacionamentos, autoridades e critérios do desempenho dos membros da equipe de projeto;
9. Eliminação ou redução dos riscos específicos associados com os projetos individuais através de um processo sistemático de planejamento, identificação, análise, resposta, monitoração e controle das áreas ou eventos com impacto negativo potencial;
10. Elaboração de um plano de gerenciamento da qualidade formal e aprovado, descrevendo o sistema de qualidade do projeto e sua execução;
11. Estabelecimento de sistema de controle da mudanças para cada projeto, com a revisão, aprovação, documentação e incorporação das mudanças realizadas à linha de base do projeto (por exemplo, mudanças relativas a custo, cronograma, escopo ou qualidade);
12. Medição do desempenho do projeto com relação aos critérios chaves do projeto (por exemplo, escopo, cronograma, qualidade, custo e risco); identificação dos desvios em relação ao planejado; avaliação de seu impacto no projeto e no programa total; relato dos resultados às partes interessadas;

13. Formalização da entrega do projeto com os resultados e benefícios esperados; identificação e comunicação das ações necessárias para alcance destes benefícios bem como das lições aprendidas para utilização em projetos futuros.

O terceiro processo diretamente associado aos acordos de nível operacional para controle do processo de manutenção de software alinhados à governança é Gerenciar desempenho e capacidade, integrante do domínio Entrega e Suporte. A necessidade de controlar o desempenho e a capacidade dos recursos de TI requer a revisão periódica do desempenho e capacidade atuais destes recursos. Este processo inclui as previsões de necessidades futuras de recursos baseadas em exigências de carga, armazenamento e contingência, visando garantir a disponibilidade das informações e o atendimento aos requisitos do negócio.

De forma mais detalhada, o processo de gerenciamento do desempenho e capacidade dos recursos de TI envolve:

1. Estabelecer um processo de planejamento para a revisão do desempenho e a capacidade dos recursos visando prover capacidade e desempenho capazes de atender aos acordos de nível de serviço estabelecidos e com custo apropriado;
2. Rever o desempenho e a capacidade atuais dos recursos e determinar sua habilidade em alcançar os acordos do nível de serviço firmados;
3. Elaborar previsões de desempenho e capacidade dos recursos em intervalos regulares com o objetivo de minimizar o risco de interrupções de serviços e identificar tendências de carga;
4. Prover a capacidade e o desempenho requeridos com relação a aspectos de carga, contingência e armazenamento;
5. Monitorar continuamente o desempenho e a capacidade dos recursos visando: a) manter e ajustá-los à carga e necessidade de contingência atuais e projetadas, b) reportar a disponibilidade do serviço e c) analisar relatórios de exceções ocorridas para permitir a tomada de ações corretivas.

Garantir a continuidade dos serviços, dentro do domínio de Entrega e Suporte é o processo de desenvolver, manter, e testar planos de continuidade e estruturas de *backup*. Um processo eficaz de garantia da continuidade dos serviços minimiza a probabilidade e o impacto de uma interrupção do serviço nas funções e nos processos chaves do negócio. É composto pelas atividades:

1. Desenvolver e manter um modelo de continuidade de TI para orientar a recuperação em caso de desastres e suportar a necessidade de continuidade do negócio. Tal modelo deve conter papéis, tarefas, responsabilidades de fornecedores de serviços externos e internos; prever a realização de testes de planos de contingência e de recuperação de desastres; identificar recursos críticos e prever a monitoração e reporte da disponibilidade destes recursos;
2. Atentar para os recursos considerados críticos no plano de continuidade e evitar o engano de dedicar-se à recuperação de itens menos críticos;
3. Testar o plano de continuidade de TI regularmente, visando garantir a efetiva recuperação de sistemas e a adequação do plano;
4. Garantir o treinamento dos envolvidos nos planos de continuidade e o conhecimento do seu papel e responsabilidades em caso de incidentes ou desastres;
5. Distribuir o plano de continuidade de forma a garantir sua segurança e disponibilidade para as pessoas autorizadas quando necessário;
6. Planejar ações a serem tomadas durante o processo de recuperação, tais como a ativação de estruturas de *backup*, iniciação de processamentos alternativos, comunicação de usuários, clientes e demais interessados;

7. Armazenar os recursos (cópias de dados, documentos) necessários à recuperação em local fisicamente diferente ao da empresa.

O processo Gerenciar a qualidade, integrante do domínio Planejamento e Organização, refere-se à elaboração e manutenção de um Sistema de Gerenciamento da Qualidade – SQG, incluindo padrões de desenvolvimento e aquisição de sistemas. Devem-se estabelecer os requisitos de qualidade a serem atingidos e comunicá-los e medi-los de forma quantitativa. A busca pela melhoria contínua da qualidade é realizada através da monitoração, tomada de ações corretivas e comunicação dos resultados aos interessados.

Os objetivos detalhados do gerenciamento da qualidade compreendem:

1. Estabelecimento, manutenção e revisão contínua de um sistema provedor de uma abordagem padronizada, formal e alinhada aos requisitos de negócio para o gerenciamento da qualidade;
2. Identificação e manutenção de padrões, procedimentos e práticas para os principais processos da organização, utilizando as melhores práticas de mercado como referência para promover a melhoria contínua da qualidade;
3. Adoção e manutenção de padrões para os desenvolvimentos e aquisições de sistemas, tais como padrões de codificação de *software*, convenções de nomenclatura, formatos de arquivos, padrões de interface com usuários, interoperabilidade, desempenho e escalabilidade, padrões de desenvolvimento, testes e validação;
4. Garantia do foco dos requisitos de qualidade nas necessidades do cliente;
5. Definição, planejamento e implementação de medidas para monitorar a conformidade com o sistema de qualidade, bem como para monitorar o valor agregado pelo próprio sistema.

O último processo relacionado no modelo proposto neste trabalho para acordos de nível operacional alinhados à governança de tecnologia da

informação é Garantir a segurança dos sistemas, dentro domínio Entrega e Suporte. A necessidade de manter a integridade da informação e proteger os recursos de TI requer um processo de gerenciamento da segurança. Este processo inclui o estabelecimento e manutenção de papéis e responsabilidades, políticas, padrões e procedimentos. O efetivo gerenciamento da segurança protege os recursos de TI, minimizando o impacto de incidentes e vulnerabilidades no negócio.

Detalhadamente, o processo envolve:

1. Elaborar um plano de segurança da informação compreendendo as políticas e procedimentos de segurança dos requisitos de informação, configurações de TI, informações de riscos e planos de ação;
2. Identificar unicamente todos os usuários internos, externos ou temporários, suas atividades (tais como negócio, operação, desenvolvimento ou manutenção de sistemas) e direitos de acessos;
3. Garantir o alinhamento dos direitos de acesso a dados com as necessidades do negócio e função desempenhada. ;
4. Solicitação de direitos de acesso pelo superior hierárquico do usuário, aprovação pelo “dono” do sistema e implementação pela pessoa responsável pela segurança;
5. Estabelecimento de um processo formal para solicitação, estabelecimento, suspensão e encerramento de uma conta de acesso e divulgação dos direitos e deveres associados à concessão do direito de acesso. Aplicação do processo estabelecido para todos os usuários internos ou externos, inclusive administradores de sistemas em situações normais ou de emergência;
6. Garantia de testes e monitoração pró-ativa e periódica da política de segurança;

7. Definição das características de potenciais incidentes segurança e sua comunicação, visando o tratamento o tratamento apropriado;
8. Determinação das políticas e procedimentos de geração, alteração, suspensão, distribuição, destruição, certificação, armazenamento, entrada, utilização, e arquivamento de chaves de criptografia com o objetivo de garantir a proteção contra alteração ou divulgação não autorizada;
9. Existência de medidas de prevenção, detecção e correção de vírus computacionais de qualquer natureza (sistemas antivírus atualizados);
10. Utilização de técnicas de segurança tais como *firewalls*, aplicativos de segurança, segmentação de rede e detecção de intrusão.

3. ITIL

O ITIL é uma biblioteca estruturada de padrões e melhores práticas de gerenciamento de serviços e infra-estrutura de Tecnologia da Informação. Entende-se por serviços o conjunto de sistemas de informação existentes para implementar os processos de negócio, na forma de produtos para os clientes da organização.

Concebido pela CCTA – *Central Computer and Telecommunications Agency*, órgão do governo inglês, na década de 80, com o objetivo de otimizar seus processos internos, originalmente o ITIL foi composto por dez livros, cobrindo as áreas de suporte e entrega de serviços de Tecnologia da Informação.

Por ser um modelo público, disponível para qualquer organização, outras empresas de governo, energia, indústria e varejo; grande, médio e pequeno porte, começaram a utilizá-lo.

Com o passar do tempo, o ITIL demonstrou-se um modelo útil em organizações de diferentes setores, sendo adotado como base para o gerenciamento de serviços. A criação de um fórum, o *itSMF – IT Service Management Forum* – para divulgar as experiências dessas organizações impulsionou ainda mais o modelo. Resultando, no ano de 2000, na criação do OGC – *Office of Government Commerce*, com o objetivo de regulamentar o uso do ITIL em âmbito mundial com a colaboração e experiências acumuladas por essas organizações.

Em 2001 foi lançado o conjunto de publicações integrantes da versão atual do modelo. Na oportunidade, o modelo foi revisto, atualizado e consistido. Os sete principais elementos componentes dessa série de publicações são:

- Planejamento do Gerenciamento de Serviços: trata das tarefas envolvidas no planejamento, implementação e aperfeiçoamento dos processos de gerenciamento de serviços e suas implicações;
- Perspectiva do Negócio: esse livro trata a compreensão e melhoria da provisão de serviços como parte integrante do requisito genérico de negócio, de alta qualidade dos sistemas de informação;

- Gerenciamento de Aplicativos: abordagem do ciclo de vida de desenvolvimento de software;
- Entrega de Serviços: livro onde são tratados quais serviços o negócio requer para atender o cliente;
- Suporte de Serviços: aborda a garantia de acesso dos usuários aos serviços apropriados para suportar as unidades organizacionais;
- Gerenciamento da Segurança: detalha o processo de planejamento e gerenciamento do nível de segurança de informações e serviços de tecnologia da informação;
- Gerenciamento da Infra-estrutura: trata o gerenciamento de rede, operações, processadores, instalações e sistemas.

A figura 3.1 ilustra a conexão e interação de cada elemento com os demais.

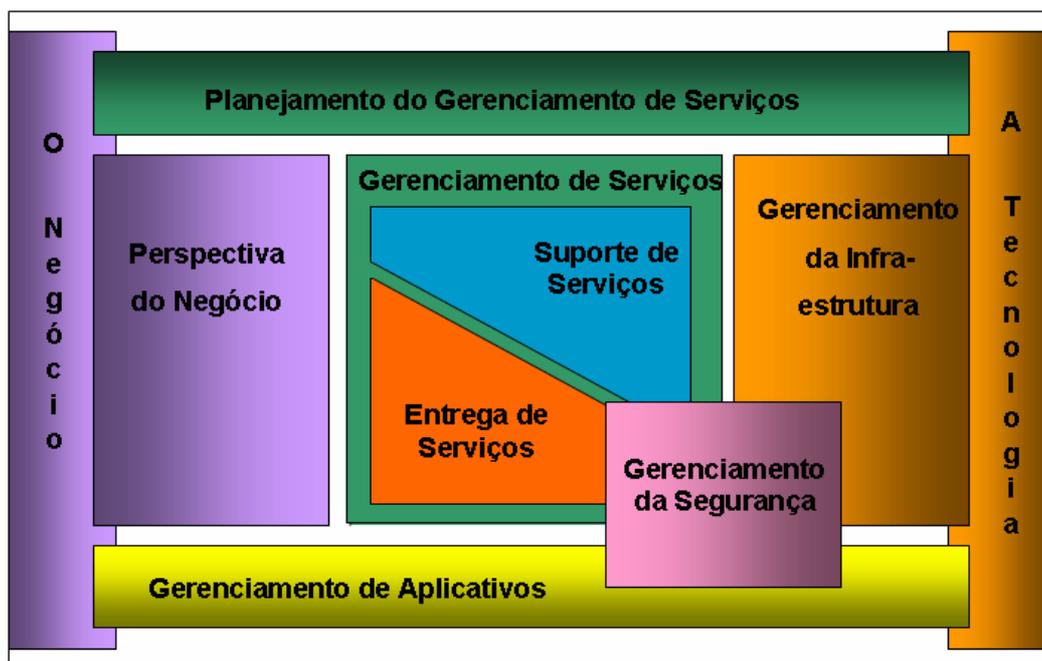


Figura 3.1 – Publicações componentes do ITIL

Os serviços de tecnologia da informação podem ser realizados pela própria organização, por terceiros ou parceiros. Os livros componentes do ITIL são dirigidos aos profissionais envolvidos na entrega ou suporte de serviços

de Tecnologia da Informação, sejam os serviços realizados pela própria organização ou por terceiros – fornecedores. Assim, gerentes de negócio também encontram, nas práticas descritas pelo modelo, orientações sobre a definição de acordos de níveis de serviço em contratos com terceiros.

O OGC anuncia a atualização da série de publicações do ITIL para o ano de 2007.

3.1 Visão Geral

O ITIL é um modelo estruturado, voltado a proporcionar serviços de alta qualidade, com ênfase particular no relacionamento com clientes. Um de seus propósitos é alinhar a gestão da tecnologia com as necessidades de negócios, com foco integral na qualidade dos serviços prestados, assegurando os níveis de serviços imprescindíveis à sustentação das operações críticas. O ITIL define "o que deve ser feito", ficando a cargo das organizações a definição de "como será feito".

O modelo fornece um método para o planejamento de processos, papéis e atividades comuns, com a referência apropriada de um para o outro e de como devem ser as linhas de comunicação entre eles. O ITIL considera o gerenciamento de serviços de TI constituído de processos estreitamente relacionados e altamente integrados.

O ITIL apresenta ainda os objetivos, macro-atividades, entradas e saídas dos vários processos envolvidos no gerenciamento de serviços de TI. O modelo foca nas melhores práticas a serem utilizadas, considerando haver diferentes formas de aplicá-las. Assim, o modelo não tem por objetivo detalhar as ações cotidianas das organizações. Essa abordagem garante a possibilidade de utilização do modelo com diferentes métodos e atividades de gerenciamento de serviços.

Dentre os objetivos do ITIL estão:

- Otimizar a utilização de recursos;
- Reduzir os custos;
- Aumentar a disponibilidade dos sistemas;

- Ajustar a capacidade;
- Aumentar o desempenho e
- Melhorar a escalabilidade.

3.1.1 O modelo de processos

Há diferentes métodos e notações através dos quais processos podem ser definidos e documentados. De forma geral, os componentes típicos da definição de um processo são:

- Atividades: cada processo pode ser dividido em um conjunto de atividades e para cada atividade há um conjunto de entradas e saídas.
- Papel: cada atividade é realizada por um papel, seja ele uma pessoa ou um *software*. Caso o papel seja realizado por uma pessoa, esta deverá possuir um conjunto de competências para realizá-lo.
- Regras: o cumprimento do papel é governado por um conjunto de regras, simples ou complexas.
- Responsável: tipo particular de papel envolvido na atividade, cuja atribuição principal é a própria definição do processo.

A figura 3.2 ilustra os componentes de um processo.

Dentre os sete elementos principais do ITIL citados anteriormente, dois representam o núcleo do gerenciamento de serviços: a entrega e o suporte. A seguir são apresentados os componentes típicos desses processos.

3.2 Suporte de Serviços de TI

Dada a crescente demanda, serviços de qualidade representam o diferencial, a vantagem competitiva das organizações. O correto entendimento das reais necessidades do cliente e do negócio garante a entrega desses serviços por uma organização. Eficiência e alta qualidade no suporte da infra-

estrutura de computação são aspectos críticos para o alcance dos objetivos do negócio.

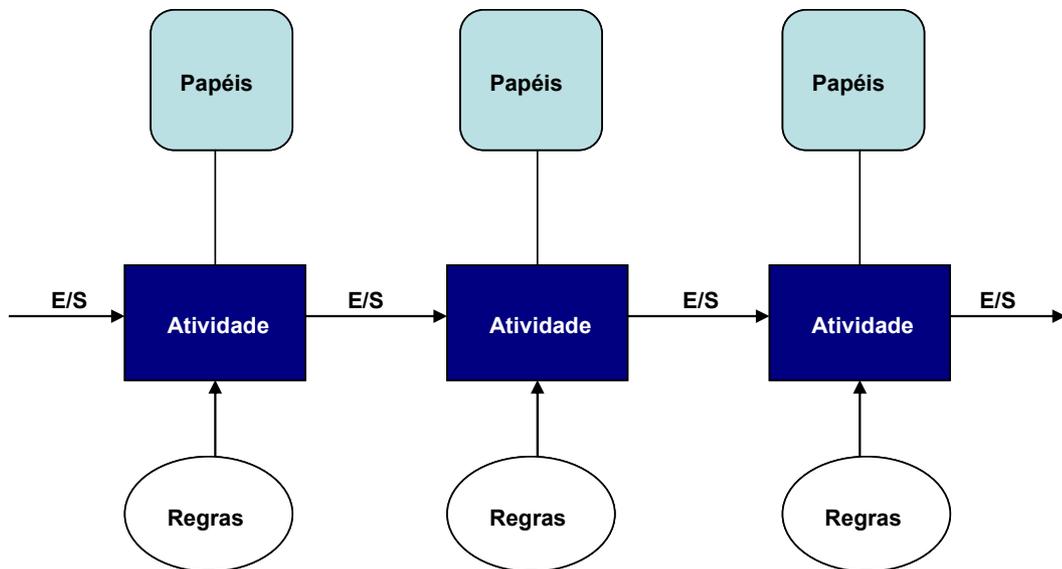


Figura 3.2 – Componentes típicos de um processo

Os ambientes de TI atuais, formados pela integração de arquiteturas diferentes, normalmente exigem altos custos de gerenciamento e manutenção. O suporte de serviços de TI trata o acesso dos usuários aos serviços apropriados para suportar as unidades organizacionais, com foco no controle da infra-estrutura, sendo considerado a base para a entrega dos serviços. Os componentes do suporte de serviços são:

- Atendimento ao Cliente
- Gerenciamento de Incidentes
- Gerenciamento de Problemas
- Gerenciamento da Configuração
- Gerenciamento de Mudanças
- Gerenciamento de Versões

O Atendimento ao Cliente, diferentemente dos demais componentes, não representa um processo, mas um departamento da organização de

extrema importância para o gerenciamento de serviços. Esta área representa o ponto de contato entre o cliente e o serviço oferecido.

Quando um cliente ou usuário tem um problema, dúvida ou reclamação, ele deseja uma resposta rápida, ou melhor, deseja uma solução. Dentre os objetivos da área de Atendimento ao Cliente destacam-se: primeiro, representar um facilitador na restauração dos serviços de TI com o menor impacto possível; segundo, contribuir para a retenção de clientes a longo prazo e na identificação de novas oportunidades de negócio e terceiro, permitir a identificação e redução de custos de propriedade com a infraestrutura de suporte e computação. A figura 3.3 representa o processo de trabalho do Atendimento ao cliente.

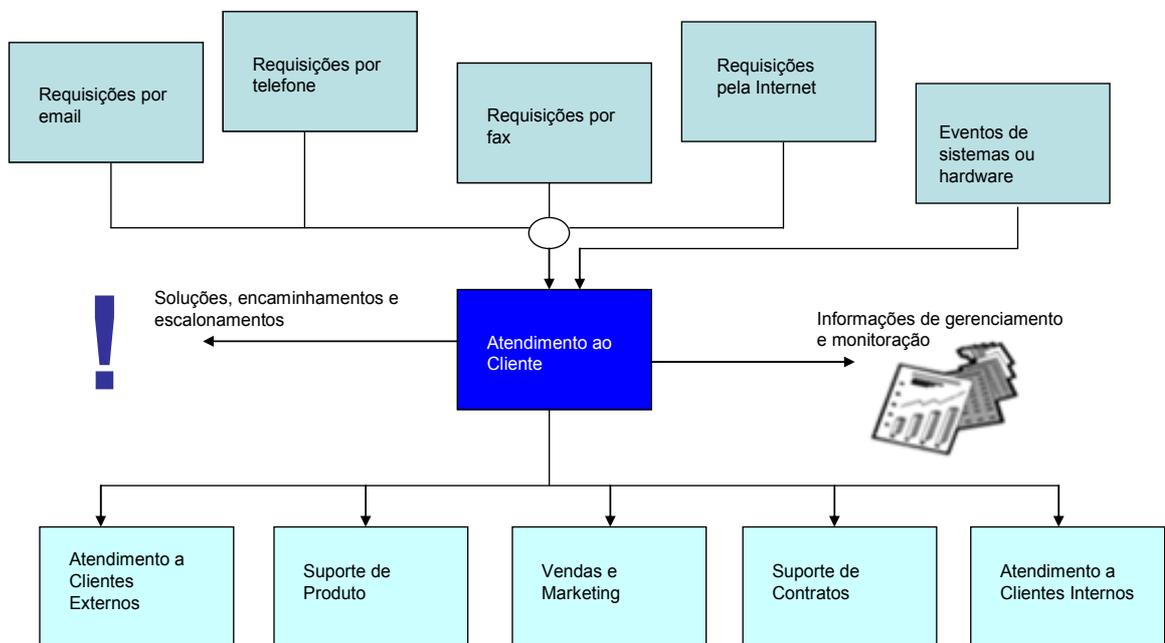


Figura 3.3 – Processo do Atendimento ao cliente

Incidentes representam insumos para o Atendimento ao Cliente. Quaisquer eventos não esperados na operação padrão de um serviço, cujo impacto potencial causa uma interrupção ou redução na qualidade daquele serviço são incidentes. Uma impressora não imprimir, um sistema fora do ar, extrapolar o uso de um disco são exemplos de incidentes. Uma solicitação de um novo serviço, como a manutenção em um sistema também é considerada um incidente no ITIL.

O Gerenciamento de Incidentes é o processo cujos objetivos são a restauração da operação normal dos serviços tão rápido quanto possível e a diminuição dos efeitos negativos no processo de negócio de forma a garantir a manutenção da disponibilidade e dos melhores níveis de serviço possíveis. Ou seja, objetiva manter os serviços dentro dos limites dos acordos de nível de serviço estabelecidos. A figura 3.4 ilustra o processo de Gerenciamento de Incidentes, apresentado as entradas, saídas e atividades.

Um problema é a causa de um ou mais incidentes. O objetivo do Gerenciamento de Problemas é minimizar o impacto de incidentes e problemas no negócio da organização causados por erros de infra-estrutura de TI. Esta é a abordagem reativa do processo. Pró-ativamente, o Gerenciamento de Problemas atua na prevenção da recorrência destes erros, antes da ocorrência de incidentes. A essência da estratégia é o ataque à causa dos incidentes e a promoção das ações necessárias para melhorar ou corrigir a situação.

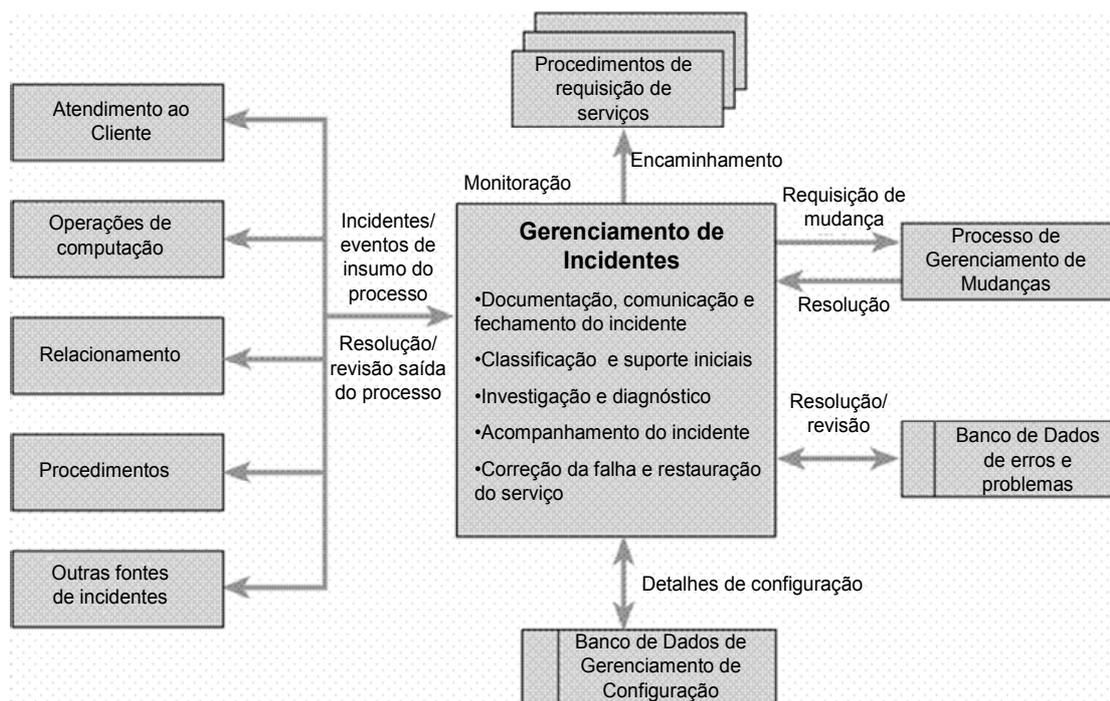


Figura 3.4 – Processo Gerenciamento de Incidentes

Para reduzir o número e a severidade dos incidentes, o Gerenciamento de Problemas garante a documentação das informações, de forma a mantê-la disponível sempre quando necessário. A documentação produzida é um tipo

de Item de Configuração. No ITIL, qualquer objeto componente da infraestrutura de TI é identificado como um item de configuração, seja hardware, software ou mesmo documentos. Requisições de mudança - por exemplo uma solicitação de manutenção evolutiva de um *software* – também são Itens de Configuração.

O Gerenciamento de Configuração é processo responsável por identificar, controlar, manter e verificar as versões dos Itens de Configuração existentes. A ferramenta utilizada para conter as informações desses itens é denominada Banco de Dados de Gerenciamento de Configuração. A figura 3.5 demonstra a relação entre os processos de Suporte de Serviços de TI e o Banco de Dados de Gerenciamento de Configuração.

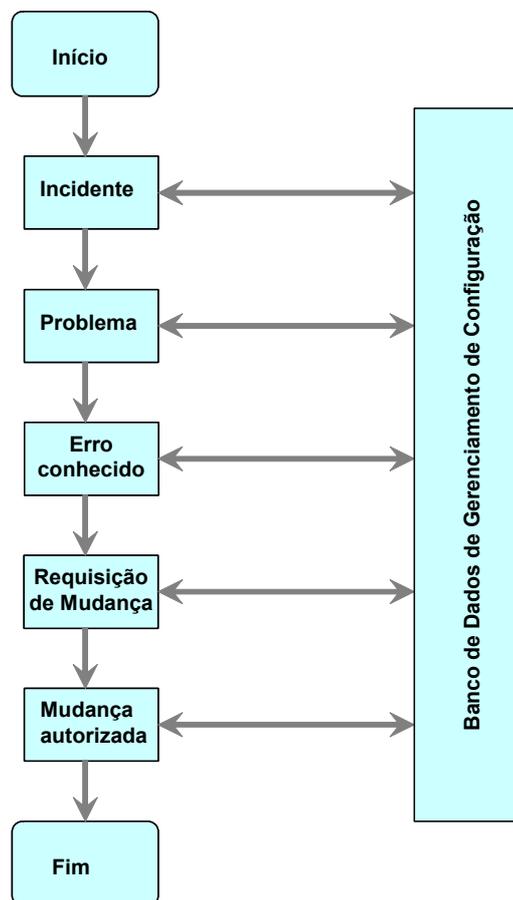


Figura 3.5 – Os processos do Suporte de Serviços de TI e o Banco de Dados de Gerenciamento da Configuração

Normalmente, mudanças ocorrem devido a problemas, entretanto, muitas mudanças podem ocorrer devido ao posicionamento pró-ativo do negócio, ocorrendo, por exemplo, para proporcionar reduções de custo ou a melhoria dos serviços.

O processo de Gerenciamento de Mudanças tem por objetivo garantir a padronização de métodos e procedimentos, visando responder e tratar de forma rápida e eficiente às mudanças.

O efetivo tratamento das requisições de mudanças requer a realização das seguintes atividades:

- Identificar e documentar mudanças;
- Avaliar o impacto, custo, benefícios e riscos da mudança sobre o negócio;
- Justificar e obter a aprovação da mudança;
- Gerenciar e coordenar a execução da mudança;
- Monitorar e relatar a execução e
- Fechar e revisar as requisições de mudança.

Para impedir o impacto negativo de mudanças na qualidade de um serviço, recomenda-se fortemente a realização de testes da manutenção, inclusive de Planos de Contingência quando aplicáveis. Os testes devem incluir aspectos da mudança tais como:

- Desempenho;
- Segurança;
- Manutenibilidade;
- Sustentabilidade;
- Confiabilidade/Disponibilidade;
- Funcionalidade.

Além desses aspectos, devem ser realizados também testes de regressão, com o objetivo de garantir a inexistência de impacto adverso em outras áreas da infra-estrutura.

O gerenciamento e controle de projetos possuem outro processo e não pertence ao escopo do processo de Gerenciamento de Mudanças. Esse último está relacionado com o dia a dia da operação do negócio, diferentemente do foco do Gerenciamento de Projetos. Ainda assim, o impacto de mudanças em projetos e o impacto de projetos em requisições de mudanças devem ser considerados em ambos os processos.

No caso de mudanças emergenciais o processo de Gerenciamento de Mudanças também é seguido. A diferença está na possibilidade de documentar parte dos detalhes após a execução da mudança.

Em ambientes terceirizados é necessária especial atenção ao cumprimento do processo de Gerenciamento de Mudanças por parte dos fornecedores. Sugere-se tratar esse aspecto nos próprios contratos firmados com terceiros.

Uma requisição de mudança autorizada e executada provoca a necessidade da geração de uma versão do conjunto de itens de configuração afetados pela mudança. O processo de Gerenciamento de Versões é responsável por prover uma visão abrangente de uma mudança em um serviço de TI, garantindo atenção aos aspectos técnicos e não técnicos envolvidos. A figura 3.6 apresenta as principais atividades do gerenciamento de versões.

A Biblioteca de Software Definitivo citada na figura 3.6 representa o local onde as versões definitivas de software estão fisicamente armazenadas e protegidas.

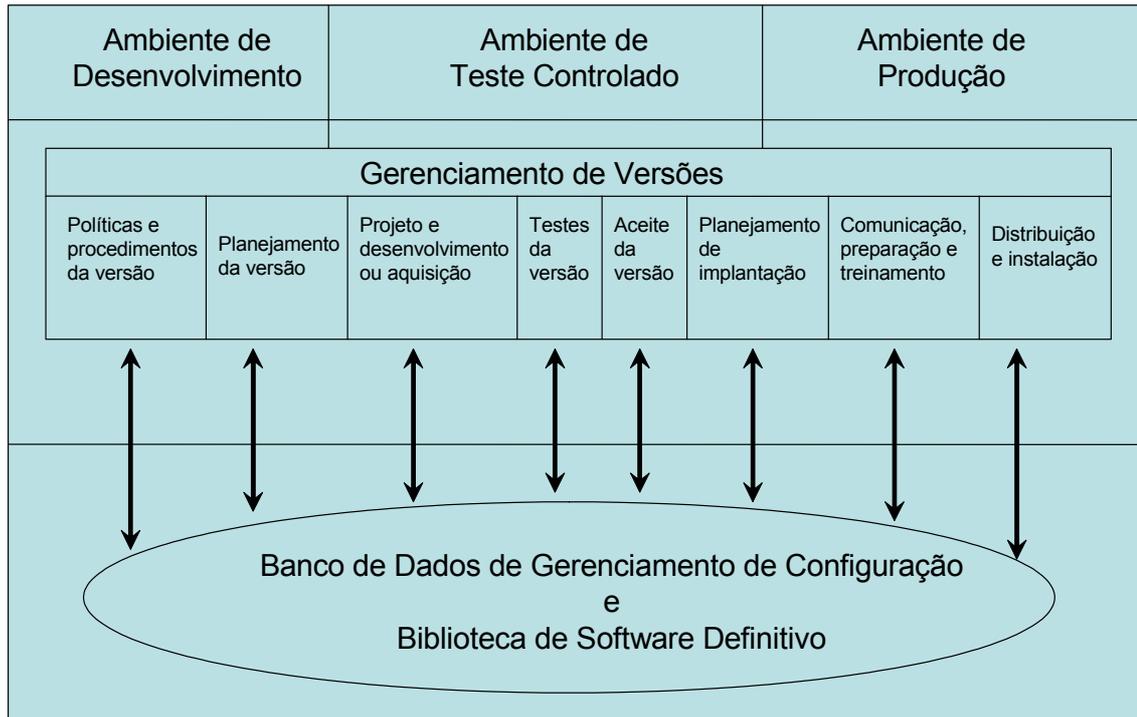


Figura 3.6 – As atividades do Gerenciamento de Versões

3.3 Entrega de Serviços de TI

Enquanto o suporte de serviços possui uma abordagem operacional, com foco no controle da infra-estrutura e ciclos de gerenciamento curtos ou médios; os processos da entrega de serviços de TI são considerados táticos, focados nos requisitos de negócio e possuem ciclos de gerenciamento médios ou longos.

Assim, a entrega de serviços de TI está envolvida com a estruturação dos serviços para atender aos requisitos de negócio e com o alcance do nível de qualidade esperado. Os componentes da entrega de serviços são:

- Gerenciamento do Nível de Serviço
- Gerenciamento Financeiro dos Serviços de TI
- Gerenciamento da Capacidade
- Gerenciamento da Continuidade dos Serviços
- Gerenciamento da Disponibilidade

3.3.1 O Processo de Gerenciamento do Nível de Serviço

O Gerenciamento do Nível de Serviço é considerado um processo essencial na determinação dos níveis necessários para os serviços de TI suportarem o negócio da organização. É o processo relacionado com a monitoração e identificação do alcance – ou não – dos níveis de serviços requeridos. Em caso negativo, é responsável por reconhecer suas razões.

Em uma visão global, um serviço é um conjunto de sistemas desenvolvidos para executar o processo de negócio. Entretanto na realidade existe uma hierarquia de serviços, onde o serviço de negócio – visível para o cliente – é composto por serviços de infra-estrutura, rede, aplicativos – esses invisíveis para o cliente.

Acordos de nível de serviços são os instrumentos utilizados pelo gerenciamento do nível de serviço para definir as metas de desempenho a serem atingidas e pelas quais a área de tecnologia da informação é avaliada.

Desta forma, o objetivo do gerenciamento do nível de serviço é manter e melhorar a qualidade dos serviços de TI através de um constante ciclo: estabelecimento dos acordos seguido pelo monitoramento, relato do desempenho e estímulo de ações para eliminar os serviços de qualidade insatisfatória. Ações estas alinhadas à necessidade do negócio e ao custo associado, visando melhorar o relacionamento entre a área de TI e seus clientes. A figura 3.7 ilustra este processo.

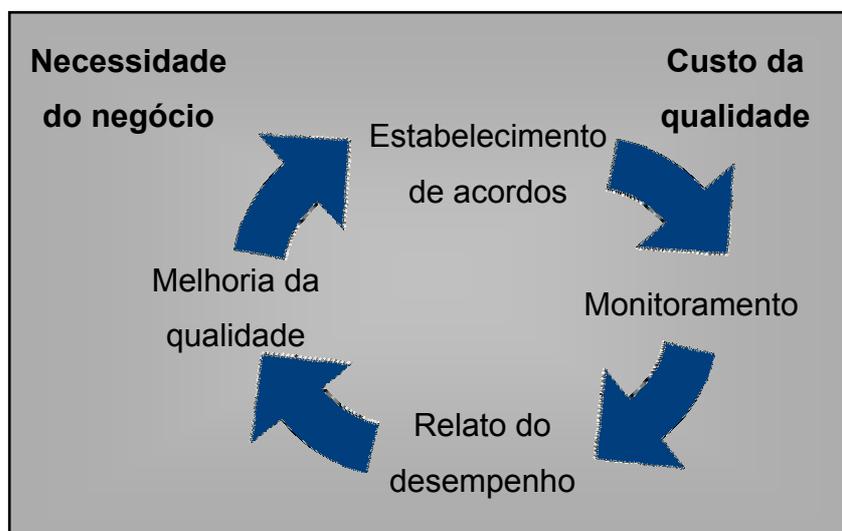


Figura 3.7 – Processo de Gerenciamento do Nível de Serviço

O conteúdo específico e as metas a serem atingidas devem ser negociados. Apesar da dificuldade em pré-determinar os acordos, dadas as singularidades de cada situação, destaca-se um conjunto de características comuns:

- Partes envolvidas – cliente e fornecedor do serviço;
- Título e breve descrição do acordo;
- Assinaturas;
- Datas de início, término e revisão;
- Escopo;
- Responsabilidades do fornecedor e do cliente;
- Descrição dos serviços cobertos pelo acordo.

Um problema comum do gerenciamento do nível de serviço é a identificação do cliente a ser envolvido na definição dos acordos. É necessário reconhecer o “dono” do serviço. Em alguns casos, essa atividade pode ser óbvia, porém, em outros casos, pode ser preciso certa negociação ou para encontrar um voluntário adequado, capaz de expressar o consenso da área representada.

Outra consideração importante é a existência de diferença de objetivos e percepções das pessoas da área cliente do serviço. Por exemplo, um alto executivo pode raramente utilizar um determinado serviço e estar mais interessado em questões tais como produtividade e resultados, enquanto um membro da equipe, usuário do serviço no dia-a-dia, pode preocupar-se com tempos de resposta, usabilidade e confiabilidade. Para um bom gerenciamento do nível de serviço é importante a identificação e incorporação dos requisitos da área cliente em todos os níveis.

Para auxiliar no processo de definição dos acordos de nível de serviço é possível definir diferentes níveis de acordos em uma organização:

- Corporativo: compreende aspectos genéricos dos acordos, adequados para qualquer cliente da organização. Esses

aspectos tendem a ser menos voláteis e conseqüentemente sofrem atualizações com menor freqüência;

- Setorizado: inclui os aspectos relevantes para um grupo de usuários em particular, independentemente do serviço em questão;
- Específico: abrange os aspectos relevantes para serviços específicos dentro de um determinado grupo de clientes.

Outro grupo, além da área cliente, a ser envolvido no processo de definição dos acordos são os representantes do provedor do serviço de TI, seja ele interno à organização ou um fornecedor externo. É necessário alcançar o consenso entre as partes sobre metas realistas, alcançáveis e exeqüíveis.

Nada deve ser incluído em um acordo sem recursos de efetiva monitoração e medição na forma combinada. A inserção de itens cuja monitoração não possa ser efetiva resulta em disputas e eventualmente na perda de confiança no processo.

Existem aspectos cuja monitoração não é possível através procedimentos mecânicos, tais como a satisfação geral do cliente com o serviço. Por exemplo, mesmo com a existência de falhas, o cliente pode manter um sentimento positivo em relação ao serviço por observar a tomada das ações apropriadas para melhorá-lo. Por outro lado, o cliente também pode sentir-se insatisfeito com algumas questões, tais como a forma de atendimento da área de atendimento ao cliente em um contato.

Portanto, é recomendado buscar monitorar a percepção do usuário a respeito de questões desta natureza. Os métodos para realizar esse acompanhamento incluem entrevistas por telefone, questionários periódicos, pesquisas de satisfação, reuniões.

Quando possível, deve-se estabelecer e monitorar a satisfação do usuário através de acordos de nível de serviço. Por exemplo, definir uma meta para o fornecedor do serviço alcançar uma média de 3,5 pontos (em uma escala de 1 a 5 pontos, onde 1 ponto representa um desempenho ruim e 5 pontos representa desempenho excelente).

O estabelecimento de contratos – e por conseguinte de acordos de nível de serviço – com fornecedores da organização é uma atividade obrigatória. Aplicar os acordos internamente, entre as áreas da empresa também é uma iniciativa benéfica.

Para medir a eficiência e eficácia do processo de gerenciamento de nível de serviços pode-se utilizar como indicadores de desempenho:

- Qual o número ou percentual de serviços cobertos por acordos de nível de serviço?
- Os acordos são monitorados e são produzidos relatórios regulares?
- São realizadas e documentadas as reuniões de revisão conforme agendadas originalmente?
- Os acordos estão atualizados? Qual o percentual de acordos com revisão e atualização atrasadas?
- Qual o número ou percentual de metas sendo alcançadas e qual o número e severidade de interrupções de serviços?
- As interrupções de serviço são efetivamente tratadas?
- As estatísticas de percepção do cliente estão melhorando?

Outro aspecto do gerenciamento do nível de serviço é a definição de acordos operacionais para suportar seus objetivos.

Esse tipo de acordo detalha aspectos específicos que afetam o nível de serviço esperado. Um conjunto de acordos operacionais podem ser definidos para auxiliar o processo de gerenciamento do nível de serviço. Esses acordos operacionais, quando estabelecidos junto a terceiros são denominados contratos de apoio. Quando um acordo desta natureza é definido entre áreas de uma mesma organização, é chamado acordo de nível operacional. A figura 3.8 demonstra a relação entre um acordo de nível de serviço, acordos de nível operacional e contratos de apoio.

Assim como os acordos de nível de serviço, os acordos operacionais devem ser monitorados, reportados e avaliados.

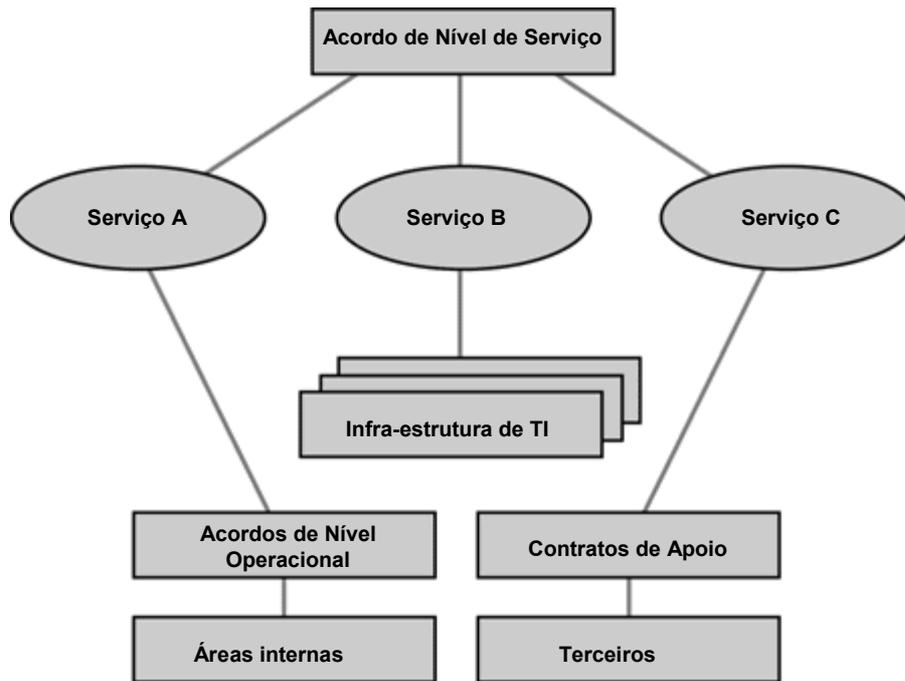


Figura 3.8 – Estrutura de suporte de um Acordo de Nível de Serviço

3.3.2 Os demais processos da Entrega de Serviços de TI

No ambiente atual de alta competitividade e de serviços orientados ao negócio, as organizações são julgadas por sua habilidade em continuar a operar e prover serviços sem interrupções.

O Gerenciamento Financeiro dos Serviços de TI está relacionado com a administração dos custos associados ao provimento dos serviços necessários para atender os requisitos de negócio. Para isso, o processo efetua as atividades de orçamento, contabilização e apropriação dos custos envolvidos demonstradas na figura 3.9.

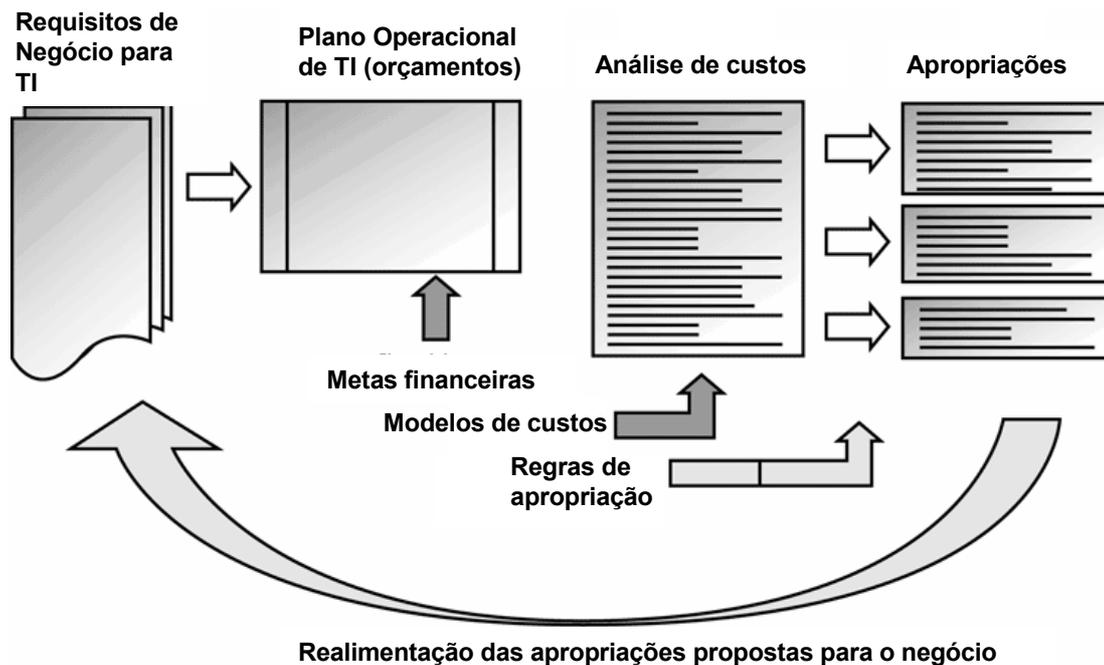


Figura 3.9 – Processo de Gerenciamento Financeiro dos Serviços de TI

O Gerenciamento da Capacidade auxilia as organizações a definir quais componentes atualizar, quando atualiza-los e quanto a atualização custará. É o processo responsável pelo balanceamento do custo e da capacidade com a oferta e a demanda, visando o atendimento das necessidades atuais e futuras do negócio com relação à infra-estrutura. A figura 3.10 representa as entradas, atividades e saídas do processo.

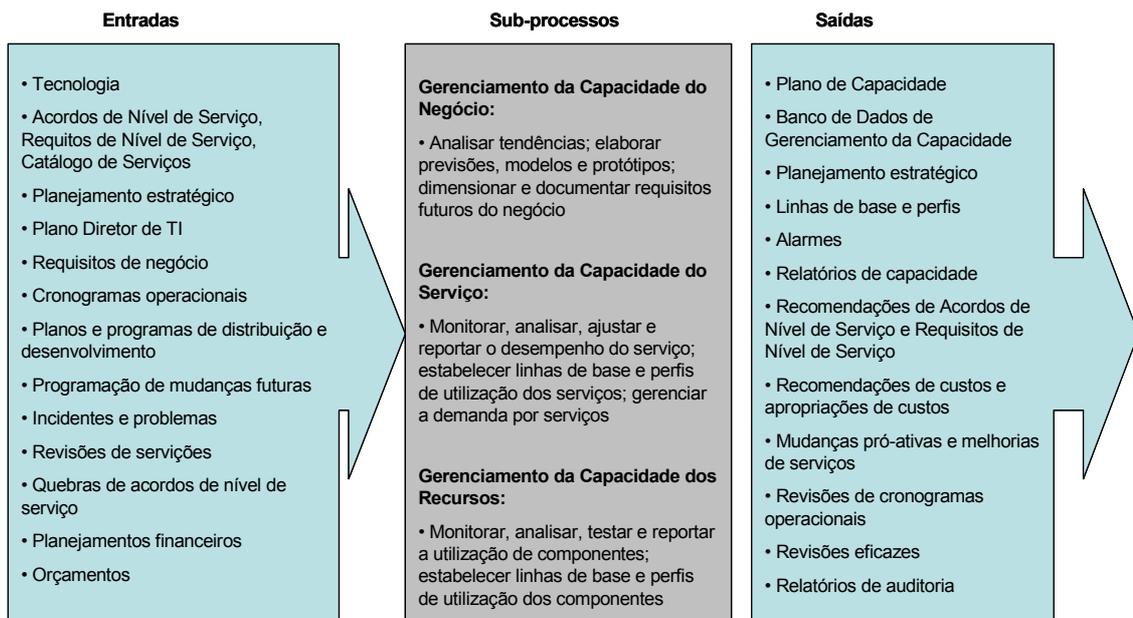


Figura 3.10 – Processo de Gerenciamento da Capacidade

O Gerenciamento da Continuidade dos Serviços está relacionado com a capacidade da organização continuar a prover o nível de serviço pré-determinado e acordado para suportar os requisitos mínimos do negócio no caso de ocorrência de uma interrupção. A figura 3.11 representa o modelo do processo.

O Gerenciamento da Disponibilidade está relacionado com a melhor utilização da capacidade da infra-estrutura de TI e com os serviços e suporte necessários para minimizar a indisponibilidade dos serviços responsáveis pela concretização de requisitos de negócio. A figura 3.12 representa as entradas e saídas do processo.

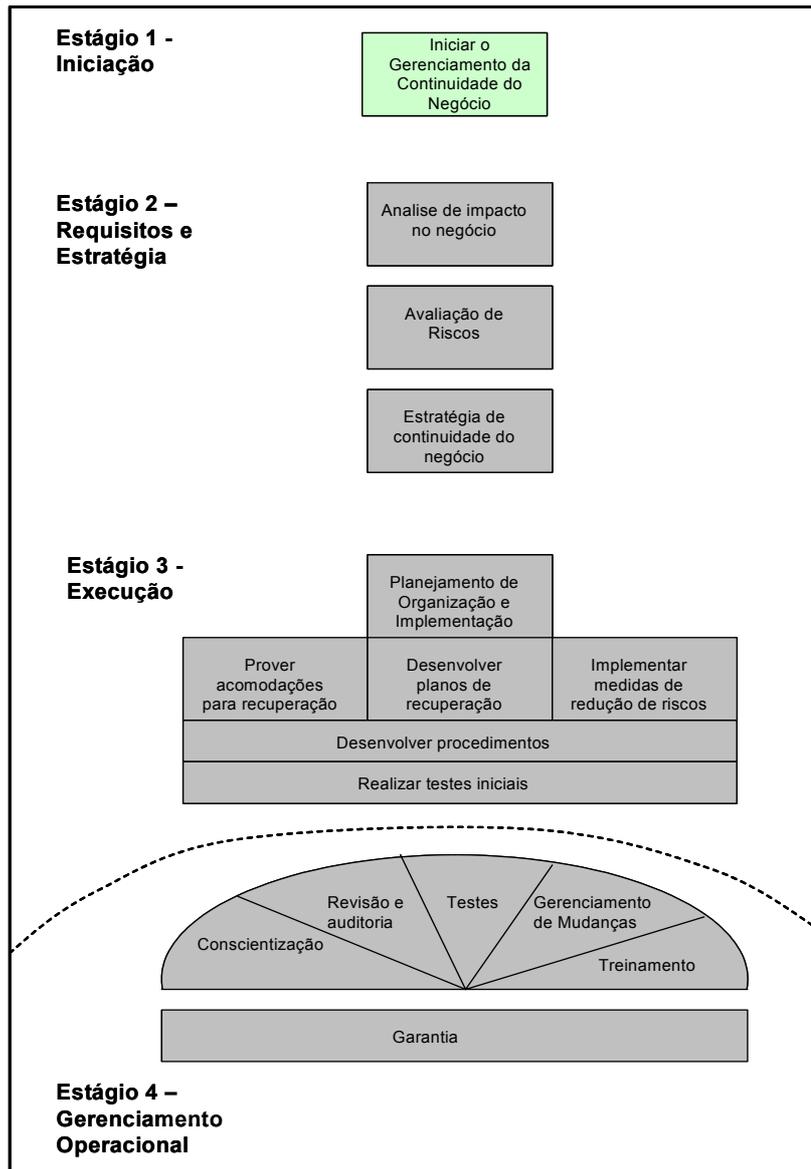


Figura 3.11 – Processo de Gerenciamento da Continuidade dos Serviços de TI

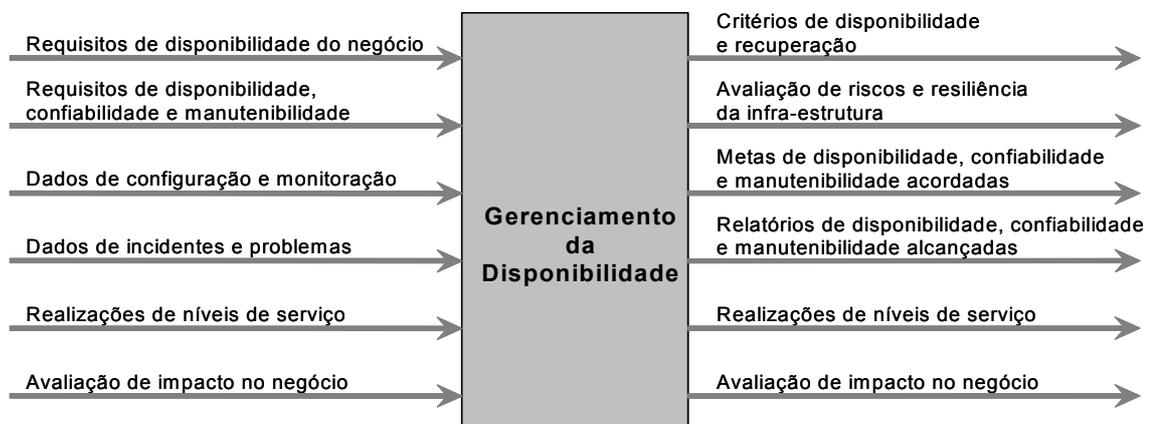


Figura 3.12 – Processo de Gerenciamento da Disponibilidade

4. Padrão IEEE para processos de engenharia de sistemas

Em dezembro de 1998 o *Software Engineering Standards Committee do IEEE Computer Society* publicou o padrão 1220-1998 para aplicação e gerenciamento de processos de engenharia de sistemas.

Este padrão define as tarefas interdisciplinares requeridas durante o ciclo de vida de um sistema para transformar as necessidades do cliente, requisitos e restrições em uma solução de sistema [IEE1998].

Genericamente, existem sistemas biológicos, ecológicos, climáticos, solares etc. Assim, um sistema pode ser visto como um elemento de um sistema maior e o desafio é compreender as fronteiras do sistema, qual é o foco dos esforços de desenvolvimento e o relacionamento entre os sistemas. Um sistema é composto tipicamente de elementos relacionados – subsistemas e componentes – e suas relações.

O ciclo de vida de um sistema – ilustrado na figura 4.1 – é composto por oito processos essenciais para alcançar a satisfação do cliente e a aceitação pública:

- Desenvolvimento: processo relacionado ao planejamento e execução das tarefas de definição do sistema necessárias para transformar as necessidades do cliente em soluções;
- Fabricação: conjunto de tarefas, ações e atividades requeridas para fabricar e montar protótipos e produtos;
- Testes: processo de planejamento e execução das tarefas relacionadas à avaliação da conformidade de uma solução com a especificação realizada durante o processo de desenvolvimento;
- Distribuição: conjunto de tarefas, ações e atividades necessárias para iniciar o transporte, entrega, montagem, instalação, teste e verificação de um produto para transmiti-lo para usuários, operadores ou consumidores;
- Operação: atividades relacionadas com a utilização do produto;

- Suporte: processo relacionado com a manutenção e suporte da operação do produto;
- Treinamento: conjunto de tarefas, ações e atividades requeridas para obter e manter o conhecimento e habilidades necessárias para operar, manter e descartar o produto;
- Descarte: processo relacionado com a garantia de descarte ou reciclagem do produto em acordo com diretrizes e regulamentos ambientais aplicáveis.

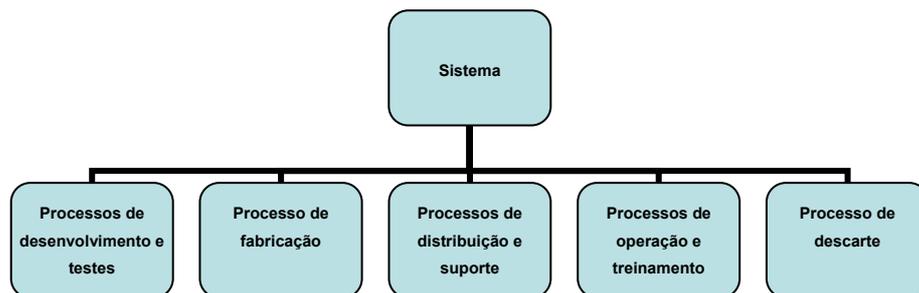


Figura 4.1 – Os processos do ciclo de vida de um sistema no padrão 1220 do IEEE

Os controles e processos de governança descritos em modelos como o CobiT e o ITIL podem ser combinados com o ciclo de vida descrito no padrão do IEEE. Em comum eles possuem a idéia de uma solução – ou serviço – elaborada com o objetivo essencial de atender às necessidades do cliente. Destaca-se a idéia de solução e não apenas de entrega de um produto ao final de seu desenvolvimento ou construção.

Uma solução envolve a percepção de uma necessidade, passa pela elaboração e lapidação da demanda; treinamento, uso do produto, manutenção (suporte, aperfeiçoamento, evolução) e descarte. Os conceitos de governança aliam-se à busca pelo melhor desempenho das atividades do ciclo de vida de uma solução.

Neste trabalho são propostos acordos operacionais aplicáveis a parte dos processos propostos no padrão IEEE, particularmente ao processo de suporte.

4.1 O processo de engenharia de sistemas

O processo proposto pelo IEEE é um modelo genérico para a solução de problemas, provendo os mecanismos necessários para identificar e desenvolver o produto desejado. As atividades componentes do processo e suas interações são apresentadas na figura 4.2.

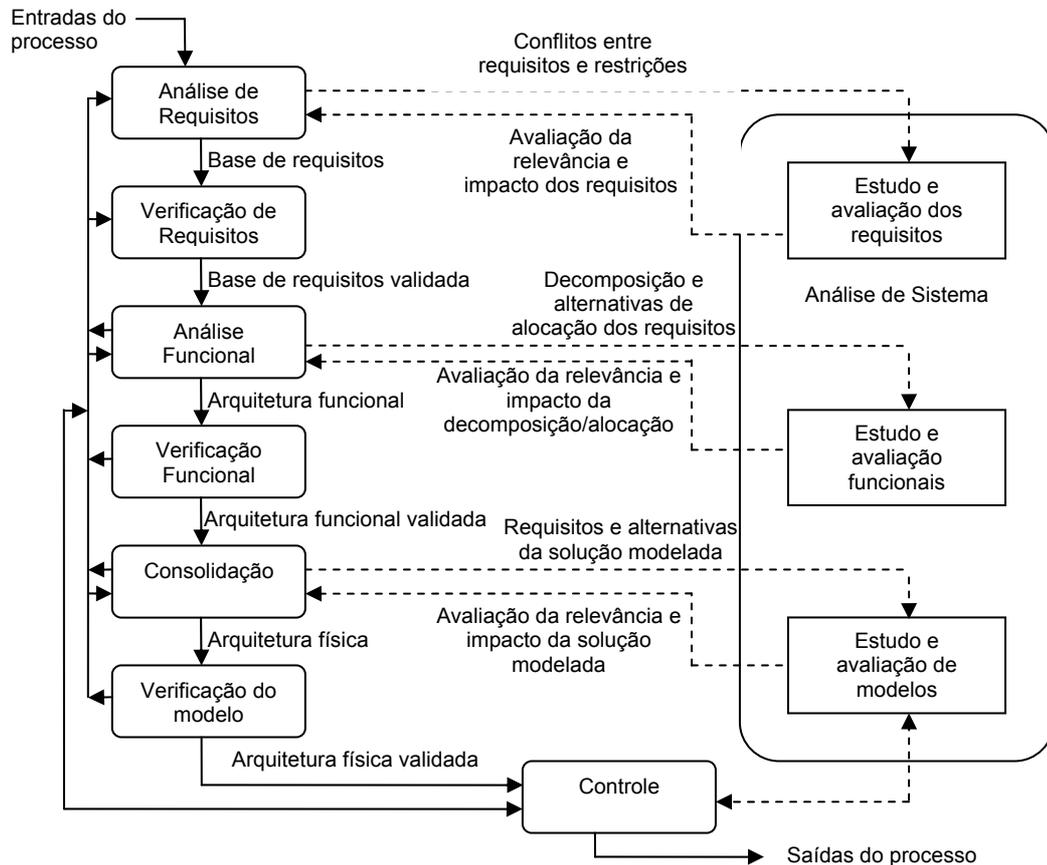


Figura 4.2 – Detalhamento do processo de engenharia de sistemas

4.2 O sub-processo de controle

O sub-processo de Controle, dentro do processo de engenharia de sistemas, tem o objetivo de gerenciar e documentar as atividades do processo de engenharia de sistemas. As atividades de controle são apresentadas na figura 4.3. Saídas e resultados de testes, o planejamento de condução das atividades do processo e os planos técnicos produzidos são controlados pela organização. As atividades do sub-processo de controle proporcionam:

- Uma visão completa e atualizada das atividades e resultados do processo, a serem utilizados como entradas de outras atividades;
- O planejamento e entradas para futuras aplicações do processo;
- Informações para a produção, teste e suporte ao cliente;
- Informações para a tomada de decisões nas revisões técnicas e de projeto.

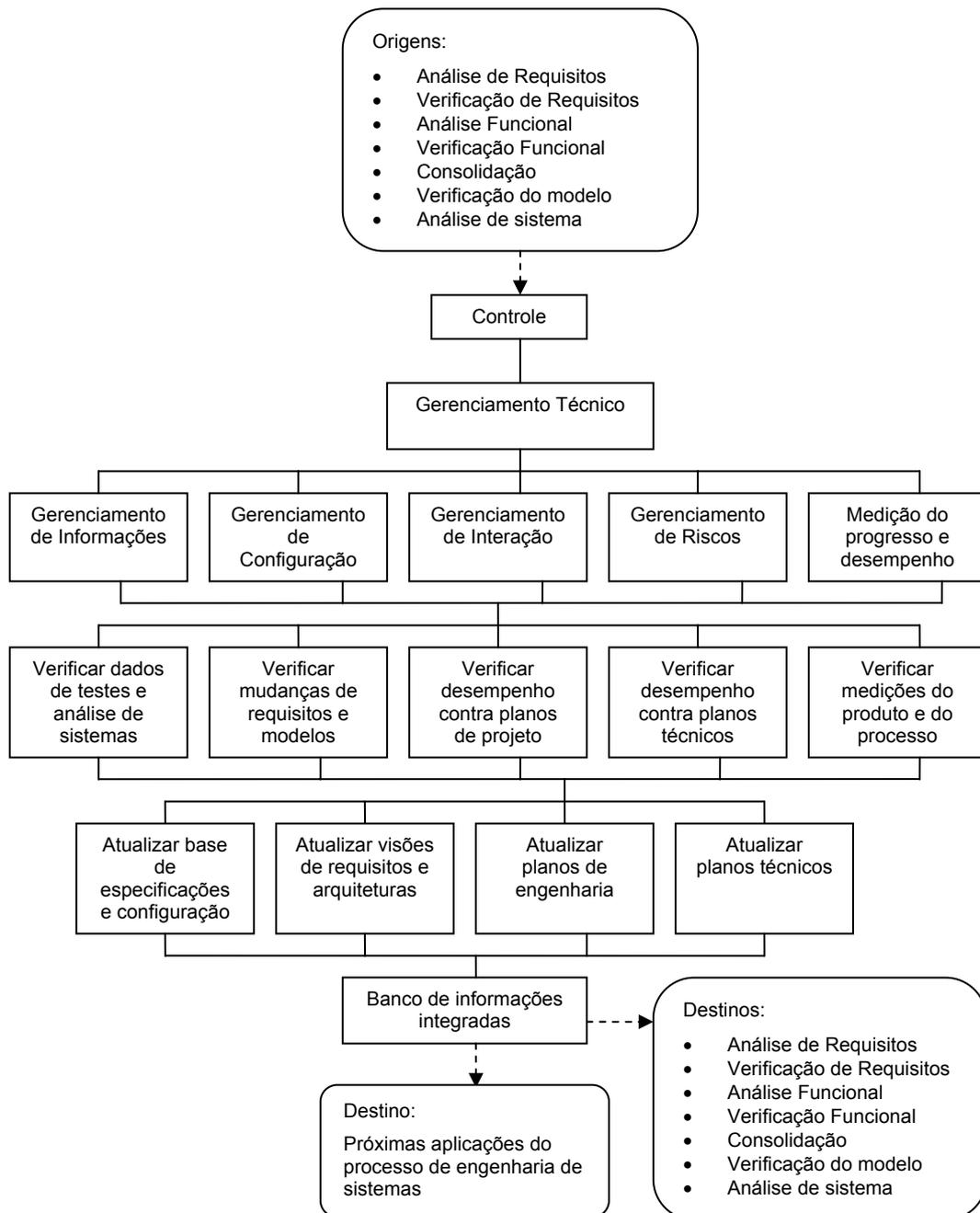


Figura 4.3 – Detalhamento do sub-processo de controle

4.2.1 Gerenciamento técnico

A atividade de gerenciamento técnico envolve o controle das informações produzidas, a configuração das soluções modeladas, interações, riscos e progresso. É necessário manter dimensionados adequadamente a equipe, equipamentos e ferramentas; gerenciar custos e cronogramas; replanejar atividades de desenvolvimento quando for o caso; coordenar interações técnicas com clientes e/ou usuários; garantir o treinamento apropriado da equipe técnicas e demais membros; medir o progresso e coordenar as atividades técnicas e de negócio para realizar as tarefas do processo de engenharia de sistemas.

O gerenciamento técnico é composto por cinco atividades:

- Gerenciamento de informações;
- Gerenciamento de configuração;
- Gerenciamento de interação;
- Gerenciamento de riscos e
- Medição do progresso e desempenho.

O gerenciamento de informações inclui a definição de bancos de dados apropriados e procedimentos para capturar e reter dados, esquemas, ferramentas e modelos. Os dados relativos ao trabalho técnico permanecem acessíveis e atualizados durante o ciclo de vida do sistema.

Deve-se garantir a integridade e segurança das informações através de mecanismos de segurança capazes de prevenir a perda ou modificação indevida de dados.

Outros aspectos relevantes para o gerenciamento da informação são a garantia de reunião, armazenamento, controle e disponibilidade da informação para a realização de um gerenciamento de configuração adequado de modelos, especificações e versões.

O gerenciamento da configuração envolve a identificação dos itens a serem controlados, o controle, acompanhamento e auditoria destes itens e de suas mudanças.

As informações relativas ao gerenciamento da configuração devem permanecer disponíveis durante todo o ciclo de vida do sistema em questão.

O gerenciamento da interação relaciona-se com o planejamento e execução das funcionalidades da interação com o sistema, questões de compatibilidade e coordenação. Assim como no gerenciamento de informações, os dados relativos ao gerenciamento da interação devem estar disponíveis durante todo o ciclo de vida do sistema.

A condução do gerenciamento de riscos de forma sistemática visa controlar as incertezas dos projetos de sistemas com relação aos custos, prazos e desempenho esperados. As ações a serem tomadas envolvem:

- A preparação do gerenciamento de riscos é a atividade de identificar os níveis aceitáveis de risco para cada estágio do desenvolvimento do sistema; levantar fontes potenciais de risco; identificar e avaliar ferramentas e técnicas de gerenciamento de riscos; treinar os membros da equipe para realizar atividades de gerenciamento de riscos.
- A avaliação dos riscos inclui a identificação e descrição das circunstâncias nas quais efeitos adversos podem ocorrer; a quantificação destas circunstâncias para determinar sua probabilidade e custo potencial; a determinação de seus efeitos em prazos e desempenho e a classificação e integração dos riscos identificados para produzir uma avaliação de riscos apropriada para cada etapa do desenvolvimento do sistema.
- A avaliação das estratégias de tratamento de riscos envolve a avaliação de estratégias de tratamento dos riscos com o objetivo de determinar aquelas factíveis e com redução do risco a níveis aceitáveis.
- O controle de riscos relaciona-se com o acompanhamento contínuo dos riscos para prover informações atualizadas e para garantir sua manutenção em níveis aceitáveis.

A última atividade componente do gerenciamento técnico é a medição do progresso e do desempenho. O progresso é medido, avaliado e acompanhado através de cronogramas, medições de desempenho técnico e de custos e prazos e revisões técnicas.

O cronograma permite a identificação de tarefas e atividades e critérios de sucesso associados necessários para satisfazer à especificação de eventos técnicos do processo do ciclo de vida do sistema. Tal ferramenta provê a garantia da conclusão das atividades técnicas requeridas, demonstra o progresso e maturidade atingida, garante a disponibilidade de informações integradas para a tomada de decisões e demonstra o controle de custos, prazos, desempenho e riscos na realização das atividades técnicas, requisitos e objetivos.

Métricas de desempenho técnico, quando apropriadamente escolhidas, representam a chave para avaliar o progresso técnico alcançado. Cada parâmetro técnico crítico deve ser monitorado com relação ao prazo, com datas estabelecidas sobre quando o progresso será verificado e quando a conformidade completa será atingida. Parâmetros técnicos importantes são medidos com relação aos níveis mais baixos dos componentes do sistema através de estimativas, análises ou testes, sendo os valores consolidados nos níveis mais altos (subsistemas e sistemas).

Tais métricas permitem ainda a avaliação da conformidade com requisitos e com os níveis de riscos técnicos, disparam o desenvolvimento de planos de recuperação para as deficiências identificadas e permitem o exame dos benefícios de custo marginais do desempenho relativo a requisitos mais exigentes.

Situações inaceitáveis identificadas através das medições devem ser reportadas para a tomada de ações corretivas.

As métricas de desempenho de custos e prazos avaliam o progresso com base no custo atual do trabalho realizado, o custo planejado para o trabalho realizado e o custo planejado para o trabalho planejado. As variações de custo ou prazo quantificam o efeito dos problemas. Integradas às medições de desempenho técnico é possível prover o impacto do custo, prazo e

desempenho atuais, permitindo a tomada de ações corretivas de forma integrada para as variações identificadas.

Revisões técnicas são realizadas ao final de estágios ou componentes, subsistemas ou sistema com o objetivo de garantir o alcance dos critérios definidos e a rastreabilidade dos requisitos e validar as decisões, avaliações de risco e preparar para o próximo estágio do ciclo de vida do sistema.

4.2.2 Verificar dados de testes e análise de sistemas

A atividade de verificação de dados de testes e análise de sistemas relaciona-se com a coleta, análise e acompanhamento de:

- a) informações dos sistemas analisados com o objetivo de documentar as atividades, recomendações e impactos e
- b) testes visando documentar os resultados, variações e atividades resultantes.

4.2.3 Verificar mudanças de requisitos e modelos

A coleta e organização das informações permitem o acompanhamento de mudanças nos requisitos e modelos, garantindo a identificação da fonte da mudança, seu processamento e aprovação.

4.2.4 Verificar desempenho contra planos de projeto

As informações refletindo as atividades planejadas são coletadas e organizadas. O progresso é avaliado em comparação ao planejamento técnico e cronogramas. Em caso de desvio em relação ao planejamento as mudanças necessárias devem ser solicitadas antecipadamente e realizadas somente após aprovadas.

4.2.5 Verificar desempenho contra planos técnicos

A verificação do desempenho contra planos técnicos relaciona-se com as atividades de:

- a) Coleta e organização das informações refletindo o planejamento de atividades;
- b) Acompanhamento do progresso contra os planos técnicos para determinar desvios dos planos e as mudanças necessárias;
- c) Documentação de mudanças, decisões e realizações.

4.2.6 Verificar medições do produto e do processo

A verificação das métricas do produto e do processo permite:

- a) Determinar áreas técnicas que requerem atenção do gerenciamento de projeto;
- b) Determinar o grau de satisfação do cliente e a aceitação pública;
- c) Prover estimativas de custo e prazo para novos produtos e prover respostas mais rápidas para os clientes.

As métricas são coletadas, acompanhadas e reportadas em pontos de controle pré-estabelecidos durante cada estágio do desenvolvimento visando:

- O estabelecimento de um sistema de qualidade e alcance do uso eficiente dos recursos;
- A avaliação geral da qualidade e produtividade do sistema;
- A comparação com os objetivos e metas planejados;
- A detecção antecipada de problemas e
- A avaliação do processo.

4.2.7 Atualizar base de especificações e configuração

A atualização das bases de especificações e configuração deve refletir todas as mudanças aprovadas. As configurações originais, junto com as

mudanças aprovadas provêm a base para a continuação do trabalho técnico a ser realizado.

4.2.8 Atualizar visões de requisitos e arquiteturas

As visões de requisitos, arquiteturas funcionais, de modelos e de sistemas são atualizadas para refletir as mudanças decorrentes de um cliente, da análise do sistema, da validação e verificação de desvio ou mesmo devido a uma decisão gerencial. A atualização da base de requisitos ou da arquitetura funcional, física ou do sistema é utilizada nas próximas atividades do processo de engenharia do sistema.

4.2.9 Atualizar planos de engenharia

Os planos de engenharia são atualizados para refletir as mudanças decorrentes de um cliente, da análise do sistema, de desvio de custo ou prazo, ou ainda por decisão gerencial. A atualização inclui as atividades planejadas no processo para o próximo estágio do ciclo de vida do sistema.

4.2.10 Atualizar planos técnicos

De forma análoga aos planos de engenharia, os planos de técnicos são atualizados para refletir as mudanças decorrentes de um cliente, da análise do sistema, de desvio do plano de atividades ou por decisão gerencial. A atualização inclui as atividades técnicas planejadas para o próximo estágio do ciclo de vida do sistema.

4.2.11 Banco de informações integradas

Um banco de dados deve ser mantido para armazenar todas as informações pertinentes às demais atividades do sub-processo de controle. Este banco de dados é um repositório para todas as informações utilizadas e

geradas pelo processo e descreve o estágio atual do desenvolvimento do sistema e sua avaliação.

5. Revisão da Bibliografia

O problema abordado neste trabalho é discutido por organizações do mundo todo. As empresas procuram formas de tornar a manutenção de software uma atividade de menor custo e maior qualidade.

A manutenção de *software* é reconhecida como a atividade demandante do maior volume de esforço dentre as atividades de engenharia de *software*. No aspecto financeiro, constitui uma importante parte do custo total do ciclo de vida de um sistema: entre 50 e 80%, segundo alguns autores [PRE2000], [HAN1993], [SNE2003].

Apesar dessa importância, grande parte dos esforços ainda é dirigida para a melhoria dos processos, métodos e ferramentas de desenvolvimento de software. Metodologias e processos – tais como o UP – *Unified Process* e o CMM – *Capability Maturity Model* – são criados para sistematizar e melhorar a qualidade dos produtos do desenvolvimento de software. No entanto, essa prática relega o enorme parque de sistemas legados em funcionamento e sobre os quais são necessárias manutenções para continuarem úteis. Como aplicar um processo de desenvolvimento de software a sistemas desenvolvidos em linguagens como Cobol ou Natural há mais de 15 anos? Como identificar e gerenciar os riscos de um projeto de manutenção?

O valor agregado pela manutenção nem sempre é percebido pelas organizações. Enquanto a introdução de um novo sistema claramente apresenta novos benefícios, o trabalho realizado para manter uma aplicação existente é notado apenas quando apresenta algum problema ou pequenas mudanças são implementadas. Acordos de nível de serviço podem ser utilizados para melhor gerenciar as expectativas dos clientes através da especificação dos resultados do trabalho [APR2000].

Nesse intento, um acordo de nível de serviço é uma ferramenta poderosa tanto para o provedor do serviço quanto para o cliente. Tão importante quanto a instituição de um SLA é gerenciá-lo. Para tanto é necessário estabelecer indicadores atingíveis, mensuráveis, significativos, controláveis e com aceitação mútua.

5.1 Manutenção de software

Manutenção de software, conforme definido por Pressman, é o processo de mudança do software após sua entrega ao cliente. Nele, os requisitos originais são modificados para refletir algum tipo de mudança nas necessidades do usuário, mudança de ambiente, introdução de novo hardware ou *software* ou mesmo correção de erros [PRE2000].

A manutenção de *software* não é uma atividade trivial. O sistema já está em operação e a equipe de manutenção precisa equilibrar as necessidades de mudança com a necessidade de manter o sistema acessível para os usuários [GRU2003]. Além desse fator, outros problemas são frequentemente encontrados nesta atividade:

- Falta de profissionais treinados na equipe com habilidades para manutenção de sistemas;
- Falta de ferramentas apropriadas e de ambiente para apoiar a manutenção;
- Baixa qualidade do sistema a ser mantido;
- Dificuldade de reter pessoas com as habilidades necessárias para manutenção de sistemas.

Pfleeger também destaca outros aspectos [PFL2001]:

- Entendimento limitado do sistema a ser mantido;
- Priorização de soluções emergenciais para resolver os problemas em detrimento de alternativas mais robustas;
- Nível de especificação e tempo para testes inadequados;
- Poucos recursos disponíveis no mercado para manutenção de sistemas;
- Baixa moral da equipe.

E segundo Charrete, dentre os fatores problemáticos da manutenção de software estão [CHA1997]:

- Pouca ou nenhuma documentação;

- Efeitos colaterais das mudanças em outras funcionalidades e sistemas;

Esse conjunto de aspectos responsáveis por tornar a atividade de manutenção de *software* complexa deve ser visto também como fatores de risco associados à atividade.

5.1.1 Os tipos de manutenção

Quanto a sua natureza a manutenção de software é classificada em quatro categorias [PFL2001] [PIG1997]:

- Corretiva: relacionada à identificação e remoção de falhas provenientes do desenvolvimento do *software* ou de manutenções anteriores [BRI1994];
- Adaptativa: causada por fatores tecnológicos tais como um novo sistema operacional ou um novo sistema gerenciador de bancos de dados [HIL1999];
- Perfectiva: implementação de novos requisitos solicitados pelo cliente e
- Preventiva: realizada para melhorar a confiabilidade ou manutenibilidade do *software* ou ainda com o objetivo de oferecer uma base para futuras ampliações.

O padrão ISO para manutenção de software utiliza estas categorias e enquadra-as em duas dimensões: tempo e objetivo, conforme demonstrado no quadro 5.1.

Quadro 5.1 – Categorias de Manutenção de Software (ISO/IEC 14764)

	Corretiva	Evolutiva
Proativa	Preventiva	Perfectiva
Reativa	Corretiva	Adaptativa

Devido às suas características, manutenções preventivas podem ser desenvolvidas sob o mesmo processo definido para novos projetos de desenvolvimento de *software*. Desta forma, os acordos de nível de serviço aplicáveis a manutenções preventivas são análogos aos acordos estabelecidos para novos projetos.

Por outro lado, o processo associado a manutenções corretivas, adaptativas e perfectivas depende de fatores tais como o esforço necessário e o prazo de entrega para ser definido.

O prazo de entrega pode ser agendável, quando tratar-se de uma manutenção sem uma data final pré-determinada. Neste caso, o planejamento e detalhamento do escopo são realizados previamente. Já em manutenções emergenciais a data final é pré-determinada antes mesmo do detalhamento do escopo a ser implementado.

Quanto ao esforço associado, as manutenções são classificadas em relação à quantidade de homens/hora necessários na implementação. São consideradas de pequeno porte aquelas envolvendo menos de 40 homens/hora para sua realização. Acima disto, classificam-se em manutenções de médio ou grande porte.

Submeter uma manutenção a um processo estrutura de desenvolvimento de *software* pressupõe tratá-la como um projeto, com a existência de um planejamento de um período de desenvolvimento. Por outro lado, pequenas requisições de mudança devem seguir um processo de contínuo, adequado à rotina diária [APR2000].

April et al, citando [ABR1993] identifica como características de requisições de mudança:

- Acontecem em intervalos aleatórios de tempo e não podem ser consideradas individualmente em um processo de planejamento estratégico anual;
- São priorizadas no nível operacional da organização, normalmente não requerem o envolvimento da alta direção;

- São gerenciadas através de técnicas de enfileiramento (avaliação e priorização) ao invés de técnicas de gerenciamento de projetos;
- O tamanho e complexidade de cada requisição de mudança costumam ser adequadas à implementação por um ou dois recursos;
- A prioridade de uma mudança pode ser alterada a qualquer momento, por exemplo, uma manutenção corretiva pode ser prioritária sobre qualquer outra manutenção em andamento.

Assim, a combinação das características de cada manutenção específica determinará os acordos de nível de serviço aplicáveis.

5.2 O Gerenciamento de TI

No passado, a área de TI das organizações focava em questões internas, concentrando apenas nos aspectos técnicos de suas atividades. Atualmente, as empresas possuem altas expectativas sobre a qualidade do serviço prestado pela TI e estas expectativas mudam através do tempo. Ou seja, para atender a estas expectativas é necessário concentrar-se na qualidade do serviço e adquirir uma abordagem mais voltada para o cliente de TI [ITI2001].

Por esta razão, o investimento isolado em tecnologia, forma tradicional de gerenciamento da informação mostra-se ineficaz. Segundo Thomas Davenport, esse modelo possui uma abordagem tática de administração: provoca a centralização do poder e implica na implementação de soluções tecnológicas em detrimento de políticas informacionais centradas nas pessoas – esta última representante de abordagem administrativa estratégica. De acordo com Davenport, as constantes – e ainda assim repentinas – mudanças no mercado e na sociedade implicam na necessidade das organizações prepararem-se para a integração do gerenciamento da informação ao restante da empresa: a denominada Ecologia da Informação. O autor propõe a visão da informação integrada à cultura organizacional, à própria tecnologia, às

políticas de intercâmbio e ao comportamento e processos de trabalho [DAV1994].

Em um ambiente de integração da informação ao restante da organização, o “ecologista” passa a fazer parte de atividades tais com definição de atribuições, obtenção de recursos e estabelecimento de um padrão cultural adequado para a empresa. Esse novo contexto provoca a necessidade de alinhamento das políticas de tecnologia da informação de negócios da empresa.

Este trabalho trata as atividades informacionais relacionadas à manutenção de *software* a serem alinhadas aos objetivos da organização.

5.3 Governança

Em tempos de crescimento das economias e dos negócios internacionais e locais o tema de governança vem à tona. Devido à sua importância, órgãos internacionais como o FMI e o Banco Mundial têm empreendido esforços e divulgação de políticas e recomendações da necessidade da governança corporativa como uma prática até mais importante em comparação com os aspectos financeiros das relações comerciais [FIG2006].

O termo Governança Corporativa, conforme a definição utilizada pela Organização para Cooperação e Desenvolvimento Econômico (OECD – *Organization for Economic Cooperation and Development*) é de um sistema pelo qual as corporações de negócio são dirigidas e controladas. A estrutura da governança corporativa especifica a distribuição das responsabilidades e dos direitos entre os diversos participantes da corporação, tais como o conselho consultivo, os gerentes, os acionistas e outros colaboradores, e dita as regras e os procedimentos para tomar decisões em assuntos corporativos. Ao fazer isto, também provê a estrutura através da qual os objetivos da companhia são estabelecidos, bem como os meios de obter tais objetivos e monitorar o desempenho [OEC2004].

Os princípios da governança estão orientados à transparência dos riscos da organização e à proteção do investimento do acionista. A utilização

da tecnologia para atender a estes princípios tornou-se inevitável, causando uma dependência crítica da tecnologia da informação. Essa realidade resultou na necessidade de uma abordagem com foco específico em governança da tecnologia da informação [BBI2003].

Desta forma, a Governança de Tecnologia da Informação está relacionada com uma estrutura de relacionamentos e processos para dirigir e controlar a organização no alcance dos objetivos desta organização, adicionando valor e equilibrando os riscos em relação ao retorno da tecnologia da informação e seus processos [COB2005].

De fato, para muitas organizações, a informação e a tecnologia associada representam seu maior valor, mas são frequentemente pouco compreendidas. Empresas de sucesso reconhecem os benefícios da tecnologia da informação e a utilizam para agregar valor. Estas empresas também compreendem e gerenciam os riscos associados, tais como a maior necessidade da existência de controles – a exemplo da SOX – e a crítica dependência dos processos de negócio em relação à informação e à tecnologia associada. Assim, o valor agregado, os riscos e o controle representam a essência da Governança de TI.

Ao avaliar o impacto da informação sobre o sucesso de uma organização espera-se identificar a forma de utilizá-la para aumentar a vantagem competitiva da organização. Mais especificamente, procura-se saber se a informação é gerenciada de forma a:

- Atender os objetivos de negócio (estratégicos) da organização;
- Ser compreensível e adaptável a mudanças de ambiente;
- Permitir a identificação de oportunidades de negócio e agir sobre elas.

É de responsabilidade da alta direção e dos executivos da organização a instituição da governança de TI através de sua liderança e da implantação de estruturas e processos organizacionais capazes de sustentar as estratégias e objetivos do negócio. A utilização de modelos de governança orienta a identificação dos processos e estruturas apropriados.

Existem vários modelos e metodologia para auxiliar a efetivação da governança de TI nas empresas. Além do CobiT e ITIL – objeto de estudo deste trabalho – modelos (normas, metodologias, padrões) tais como a ISO 17799, COSO *Report*, CMM, BSC, RUP e o PMBoK tratam de assuntos integrantes da governança de TI.

5.3.1 ISO 17799

A norma ISO 17799 define um conjunto de boas práticas de gestão da segurança, servindo de base para o estabelecimento de políticas e realização de auditorias de segurança de informações nas organizações [NBR2001]. É composta pelos seguintes módulos:

- Política de Segurança
- Organização da Segurança
- Classificação e Controle de Ativos
- Segurança de Pessoal
- Segurança Física e Ambiental
- Gerenciamento de Comunicações e Operações
- Controle de Acesso
- Desenvolvimento e Manutenção de Software
- Planejamento de Continuidade de Negócios
- Conformidade

5.3.2 COSO *Report*

A metodologia publicada pelo COSO - *Committee of Sponsoring Organizations of the Treadway Commission* - identifica os objetivos essenciais do negócio de uma dada instituição e define o Controle Interno e seus componentes, fornecendo critérios a partir dos quais os sistemas de controle podem ser avaliados [GHE2005].

Segundo o COSO, Controle Interno é um processo, tornado efetivo através das pessoas, as quais devem assegurar com razoável grau de segurança o alcance dos seguintes objetivos, fundamentais a qualquer negócio:

- Economia e eficiência das operações, incluindo o alcance dos objetivos em termos de performance e segurança dos ativos contra perdas;
- Veracidade das demonstrações financeiras;
- Conformidade com as normas e legislação locais.

Em 2001, o COSO associou-se à *Pricewaterhouse-Coopers* para desenvolver o projeto de um modelo adequado para efetivamente identificar, avaliar e gerenciar riscos. Mais adiante, foi publicado o *Enterprise Risk Management* (ERM), o qual é composto por 8 componentes inter-relacionados, a saber:

- Ambiente de Controle: contempla o tom de uma instituição, e se configura como a base de como o risco é percebido e tratado pelas pessoas envolvidas, considerando a filosofia de gestão de riscos e a tolerância a riscos, a integridade e os valores éticos, e o ambiente operacional. O Ambiente de Controle é a base para todos os demais componentes.
- Definição de Objetivos: garantia de adoção de um processo para definir objetivos e de que os objetivos selecionados suportam e estão alinhados à missão da instituição e são consistentes com a tolerância a riscos.
- Identificação de Eventos: devem ser identificados todos os tipos de eventos internos e externos que podem afetar o alcance dos objetivos da instituição, devendo ser distinguidos os riscos das oportunidades.
- Avaliação de Riscos: os riscos internos e externos à instituição são analisados, considerando a probabilidade e a severidade

das ameaças, como base para determinar os riscos relevantes e como estes devem ser gerenciados.

- Tratamento dos Riscos: seleção da opção adequada - evitar, aceitar, reduzir ou compartilhar riscos - desenvolvendo uma série de ações (controles) para alinhar os riscos com a tolerância a riscos.
- Atividades de Controle: definição e implementação de políticas e procedimentos para ajudar a garantir a realização do tratamento correto do risco, de forma a alcançar os objetivos estratégicos estabelecidos.
- Informação e Comunicação: identificação, captura e comunicação de informações relevantes para possibilitar o recebimento do nível de conteúdo apropriado pelas pessoas necessárias para permitir a execução de suas atividades.
- Monitoração: a gestão de riscos corporativa é monitorada em âmbito global e as alterações são feitas quando necessário. A monitoração é feita por atividades contínuas de gestão, por auditorias internas ou externas (periódicas ou especiais), ou por ambas.

5.3.3 *Capability Maturity Model*

O CMM – *Capability Maturity Model* – ou Modelo de Maturidade da Capacitação para Software, desenvolvido pelo *Software Engineering Institute*, é um modelo aplicado com o objetivo de medir o nível de maturidade das organizações no processo de desenvolvimento de *software* [CMM2002].

Neste modelo é proposto um caminho gradual para aprimorar continuamente as organizações na busca de uma solução própria para os problemas inerentes ao desenvolvimento sistemático de *software*. Este caminho gradual é apresentado através de 5 níveis de maturidade. No estágio inicial – nível 1 - a improvisação rege o processo de desenvolvimento. No nível 5 – o mais alto da escala do CMM – o foco é a melhoria sistemática do

processo. Cada nível possui áreas-chaves de processo, visando atingir uma meta de melhoria do processo através de um conjunto de atividades realizadas para este fim (práticas chave). A figura 5.1 ilustra os cinco níveis do modelo.

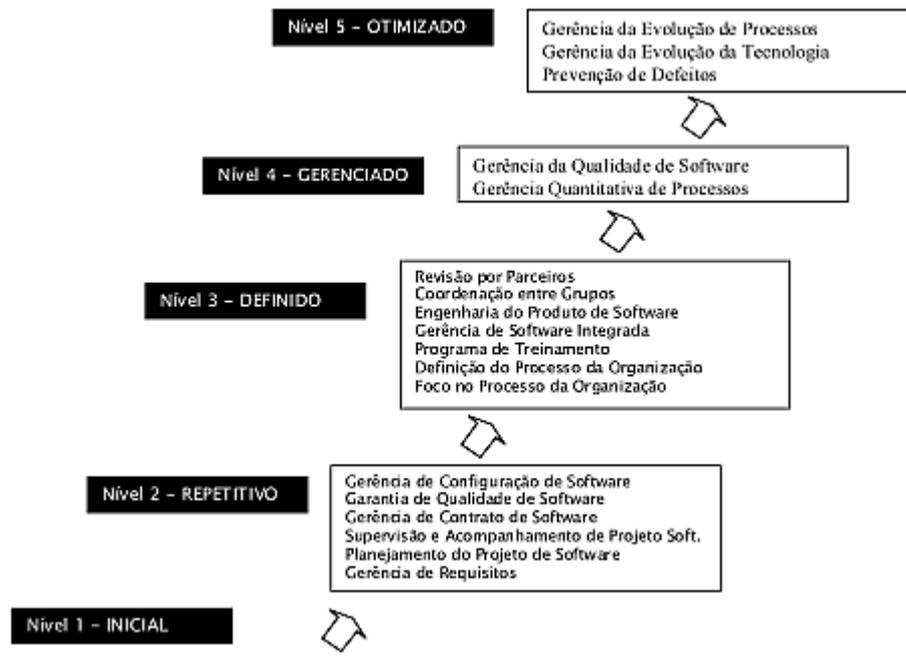


Figura 5.1 – As áreas chaves de processos do CMM [PAU1995]

5.3.4 *Balanced Scored Card*

Kaplan e Norton, autores modelo BSC – *Balanced Scored Card*, propõem a avaliação das organizações através de quatro perspectivas com interação entre si, focando a ligação do sistema de medição à estratégia da empresa [KAP1997]. A figura 5.2 ilustra a interação das quatro perspectivas do *Balanced Scored Card*.

O BSC reflete o equilíbrio entre objetivos de curto e longo prazos, entre medidas financeiras e não-financeiras, entre indicadores de tendências e ocorrências e, ainda, entre as perspectivas interna e externa de desempenho. Este conjunto abrangente de medidas serve de base para o sistema de medição e gestão estratégica por meio do qual o desempenho organizacional é mensurado de maneira equilibrada sob as quatro perspectivas. Desta forma, contribui para que as empresas acompanhem o desempenho financeiro,

monitorando, ao mesmo tempo, o progresso na construção de capacidades e na aquisição dos ativos intangíveis necessários para o crescimento futuro.

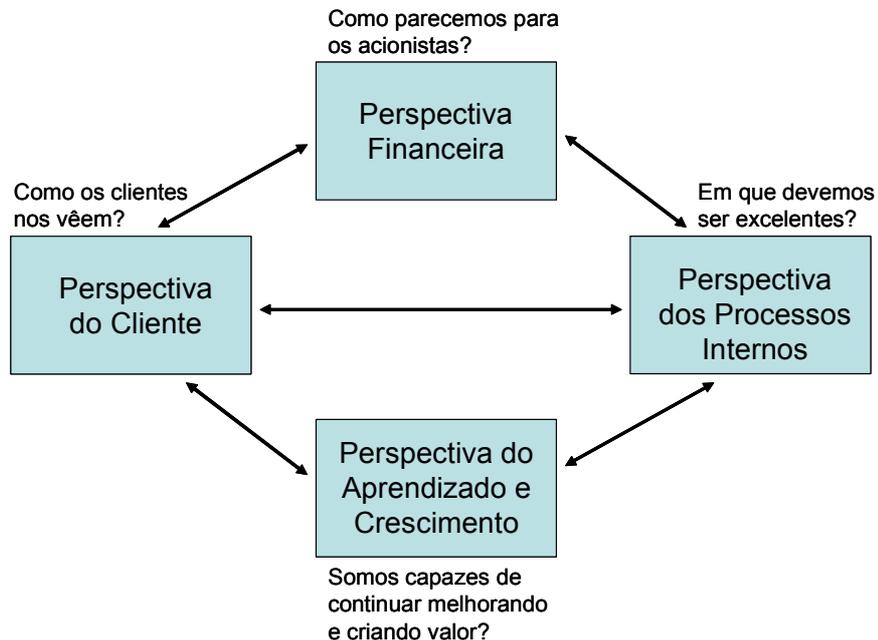


Figura 5.2 – As perspectivas do Balanced Score Card [KAP1992]

5.3.5 Rational Unified Process

O RUP – *Rational Unified Process* – é um processo de desenvolvimento de *software* iterativo, centrado em arquitetura e dirigido por casos de uso. Oferece uma abordagem baseada em disciplinas para atribuir tarefas e responsabilidades dentro de uma organização de desenvolvimento, visando garantir a produção de *software* de alta qualidade e atendendo às necessidades dos usuários dentro de um orçamento e cronograma previsíveis [RUP2001].

A figura 5.3 apresenta os elementos básicos do RUP. Nesta metodologia, um projeto de desenvolvimento de *software* passa por 4 fases :

- Iniciação: entendimento da necessidade e visão do projeto;
- Elaboração: especificação e abordagem dos pontos de maior risco;
- Construção: desenvolvimento principal do sistema;

- Transição: ajustes, implantação e transferência de propriedade do sistema.

Cada fase é composta de uma ou mais iterações, normalmente de curta duração e abordando um pequeno conjunto de funções do sistema. Desta forma, o processo proposto pelo RUP reduz o impacto de possíveis mudanças. Além das fases e iterações, o RUP propõe uma abordagem das disciplinas participantes do ambiente de desenvolvimento de sistemas em uma seqüência de tarefas encadeadas e relacionadas. A figura 5.3 mostra a ênfase de cada disciplina em cada fase do projeto.

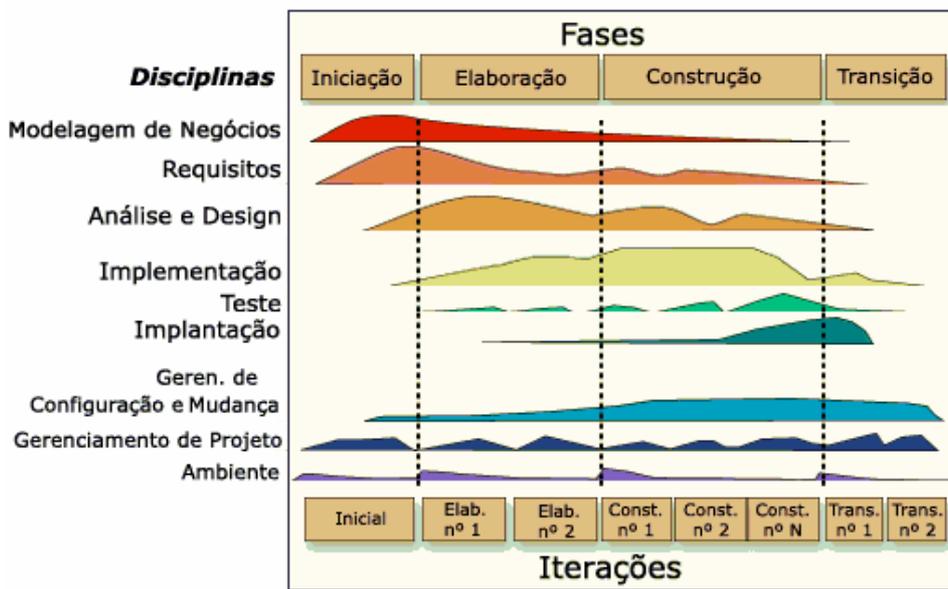


Figura 5.3 – Fases e disciplinas do RUP

5.3.6 Project Management Body of Knowledge

O gerenciamento de projetos integra a governança corporativa e a governança de tecnologia da informação. O PMBoK - *Project Management Body of Knowledge* – é um guia de boas práticas de gerenciamento de projetos publicado pelo *Project Management Institute*. Nele, o ciclo de vida de um projeto é composto por 5 grupos de processos:

- Iniciação: definição e autorização do projeto ou de uma fase do projeto;

- Planejamento: definição e refinamento dos objetivos e planejamento das ações necessárias para atingi-los;
- Execução: integração de pessoas e demais recursos para realizar as ações definidas na etapa de planejamento;
- Controle: medição e monitoração regular do progresso do projeto, visando a tomada de ações corretivas quando necessário;
- Encerramento: formalização e aceitação do produto.

Dentro desses grupos estão distribuídos processos de 9 áreas de conhecimento: Escopo, Tempo, Custo, Qualidade, Recursos Humanos, Riscos, Comunicações, Aquisições e Integração [PMI2004].

5.4 Lei Sarbanes-Oxley

A Lei *Sarbanes-Oxley* – SOX – foi promulgada pelo governo dos Estados Unidos em decorrência a escândalos financeiros ocorridos em grandes organizações, entre as quais a Enron, WorldCom e Tyco. Composta de onze títulos, a lei define requisitos rígidos para a contabilidade de companhias públicas e transforma a indústria da contabilidade pública. Reformando procedimentos de demonstração e governança corporativa, os diversos títulos e seções da SOX definem as responsabilidades de gerenciamento nos relatórios anuais e semestrais, o ambiente do controle, gerenciamento de risco e o monitoramento e a medição das atividades de controle. O quadro 5.2 apresenta os assuntos tratados pela lei em seus onze títulos. [STI2005].

A SOX é uma lei é voltada principalmente para companhias de capital aberto com ações nas bolsas de valores ou com negociação na Nasdaq. Muitas de suas regulamentações dizem respeito à responsabilidade corporativa pela veracidade de conteúdo dos relatórios financeiros produzidos e pelo gerenciamento e avaliação dos controles internos.

A lei prevê inclusive penas de multas ou prisão para os executivos da companhia no caso de apresentação de informações incorretas ou imprecisas.

Apesar de sua abrangência restrita, a SOX passou no entanto a ser referência para todas as grandes empresas que hoje já demonstram preocupação com a aderência aos padrões de governança.

Quadro 5.2 – Os títulos da lei Sarbanes-Oxley

Conteúdo	Título do Assunto
Título I	Comitê de Supervisão da Contabilidade da Companhia Pública
Título II	Independência do auditor
Título III	Responsabilidade corporativa
Título IV	Aumento de demonstrações financeiras
Título V	Conflitos de interesse do analista
Título VI	Recursos e autoridade da comissão
Título VII	Estudos e relatórios
Título VIII	Prestação de contas corporativas e fraude criminosa
Título IX	Aprimoramento das penalidades contra os crimes do colarinho branco
Título X	Retorno de impostos corporativos
Título XI	Fraude corporativa e prestação de contas

No Brasil, o tema da governança corporativa avança, forçado inclusive pela crescente pressão do mercado. Aqui, assim como em outros lugares do mundo, a Lei *Sarbanes-Oxley* é utilizada como uma diretriz para organizar e controlar o ambiente corporativo. Assim, em 1995 foi fundado o IBGC - Instituto Brasileiro de Governança Corporativa, focado especificamente nesta questão.

A Lei *Sarbanes-Oxley*, na seção 404, Avaliação dos Controles Internos pela Gerência afirma:

“(a) RULES REQUIRED--The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S. C 78m or 78o(d) to contain an internal control report, which shall-- (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, or the effectiveness of the internal control structure and procedures of the issuer for financial reporting.” [SOX2002]

A sessão 404 da lei refere-se aos controles necessários para manter a integridade do processamento e reporte de dados financeiros. Deve-se examinar e estabelecer controles sobre qualquer processo ou sistema, visando garantir sua integridade.

Desta forma, com relação à área de Tecnologia da Informação, algumas questões devem ser respondidas pelas organizações na busca da conformidade com a lei:

- Qual o impacto da tecnologia da informação sobre os objetivos do negócio?
- Os níveis de serviço de TI para os processos de negócio mais importantes são efetivamente monitorados?
- A área de TI provê métricas de nível de serviço visíveis para a alta administração?
- A TI possui insumos para prover a visibilidade necessária?

A figura 5.4 demonstra o sentido de atuação para a área de TI garantir a conformidade com a SOX [ITC2004].

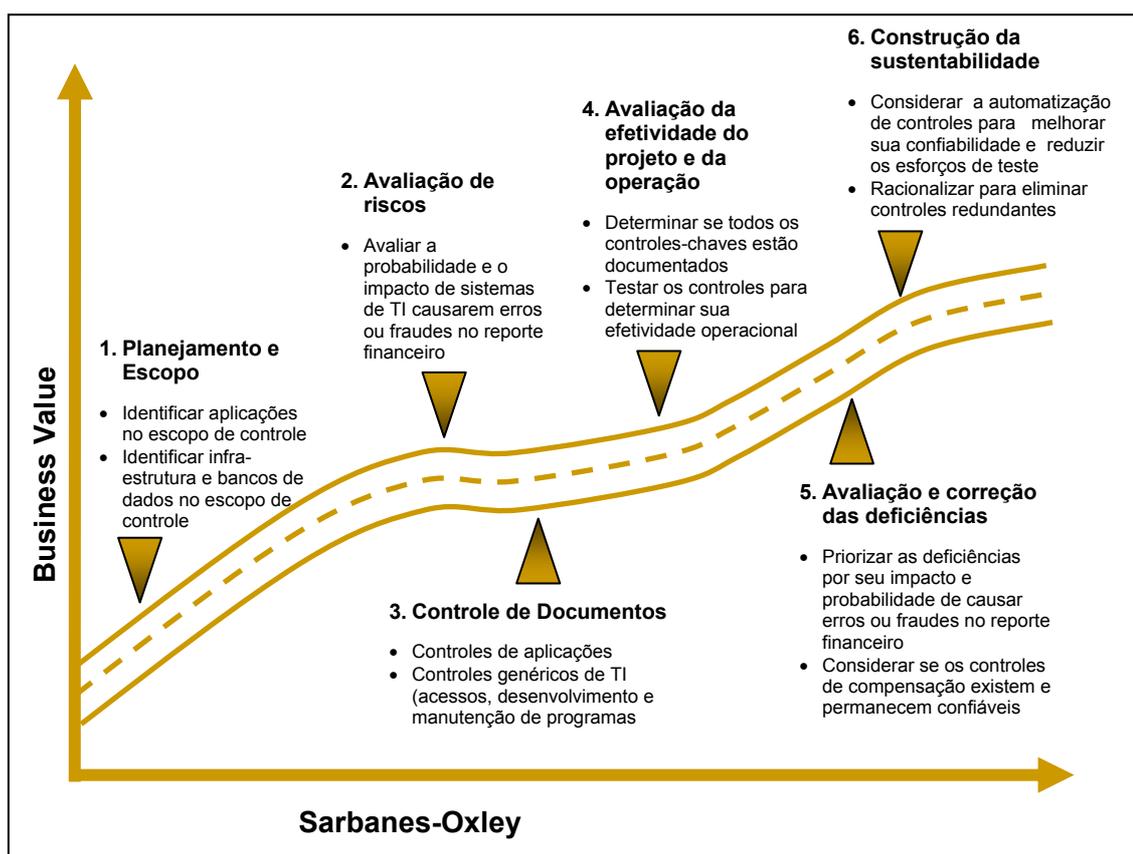


Figura 5.4 – Atividades de TI para aderência à SOX [ITC2004]

A avaliação dos controles de TI inclui cinco processos considerados críticos para a integridade dos processos, sistemas e informações

relacionados à produção de relatórios financeiros precisos e confiáveis [BMC2004]:

- Administração da segurança: garantia de acesso a dados, aplicativos, bancos de dados, sistemas operacionais e redes apenas às pessoas apropriadas.
- Gerenciamento de mudanças: alterações de aplicativos ou na infra-estrutura tecnológica impactam na integridade das informações financeiras. É necessário estabelecer procedimentos efetivos de gerenciamento, garantindo a realização de testes consistentes e a aprovação da mudança antes de sua entrada em ambiente de produção.
- Gerenciamento de dados e recuperação de desastres: garantia da integridade dos dados quanto à sua precisão, autorização e validade. Inclui atividades de *backup* e recuperação e restauração dos dados. Em caso de desastres, recuperação e execução de planos de continuidade.
- Gerenciamento de problemas e operações: auxiliar na garantia da integridade de informações e transações financeiras. Habilidade em responder a falhas e interrupções de sistemas de forma a garantir as operações, transações e integridade de dados. Estabelecimento de acordos de nível de serviços para alcançar os objetivos de negócio, o desempenho e capacidade dos sistemas. Habilidade para prevenir, minimizar e responder a eventos responsáveis por interromper a operação normal dos serviços.
- Gerenciamento de recursos: controle dos recursos de TI, desde sua requisição e recepção para instalação e manutenção, até sua inutilização.

Nos acordos de nível de serviço propostos no capítulo sete são apresentados os relacionamentos entre os acordos e os cinco controles de TI responsáveis pela integridade do processo.

5.5 Relatório de pesquisa global sobre governança

Em 2003, o ITGI – *IT Governance Institute*, criador do CobiT, encomendou à empresa *PricewaterHouseCoopers* a condução de uma pesquisa com o intuito de avaliar a percepção e aplicação dos conceitos e modelos de governança de tecnologia da informação no mundo. Em 2005, foi realizada uma segunda pesquisa, com o mesmo propósito. De forma detalhada, os objetivos da pesquisa foram:

- Pesquisar e analisar o grau em que o conceito de governança de TI é reconhecido, estabelecido e aceito dentro das organizações;
- Determinar o nível de conhecimento sobre governança de TI e quais modelos são conhecidos e adotados e
- Medir a extensão de percepção e utilização do CobiT.

A pesquisa envolveu 695 organizações de diferentes tamanhos e áreas de atuação (empresas de telecomunicações, instituições financeiras, indústrias, varejo e setor público) em todo o mundo.

Dentre as principais descobertas da pesquisa está crescente importância da tecnologia da informação para as organizações. Para oitenta e três por cento dos participantes, a tecnologia da informação é classificada entre importante e muito importante para a realização da estratégia e da visão corporativas. A seguir são apresentados os resultados de três questões levantadas pela pesquisa.

O percentual de organizações empregadoras de modelos de governança é menor em 2005 com relação a 2003. Por outro lado, o percentual daquelas sem intenção de adotá-los também é menor. Este fato pode ser explicado pelo fato da implantação da governança não ser tão trivial quanto se imaginou originalmente. O estado da adoção de modelos de governança nas organizações é demonstrado na tabela 5.1.

O objetivo das organizações com a implantação de soluções parciais de governança foi abordado na pesquisa. A principal motivação é melhorar o gerenciamento de custos da área de tecnologia da informação. Em seguida,

as empresas buscam melhorar o gerenciamento de recursos (financeiros, humanos, sistemas) e gerenciar os riscos da área. A tabela 5.2 demonstra o cenário desta questão.

Tabela 5.1 – Situação da implementação de Governança de TI

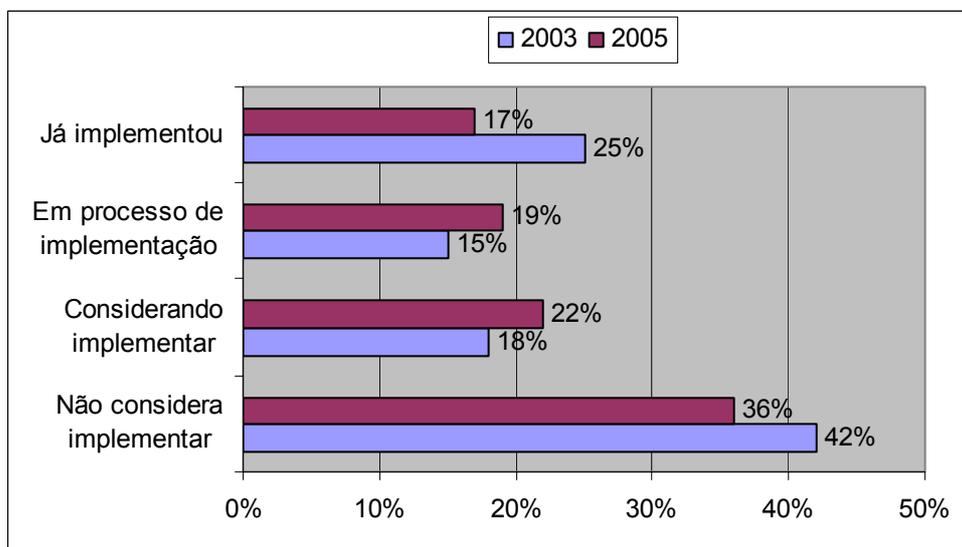
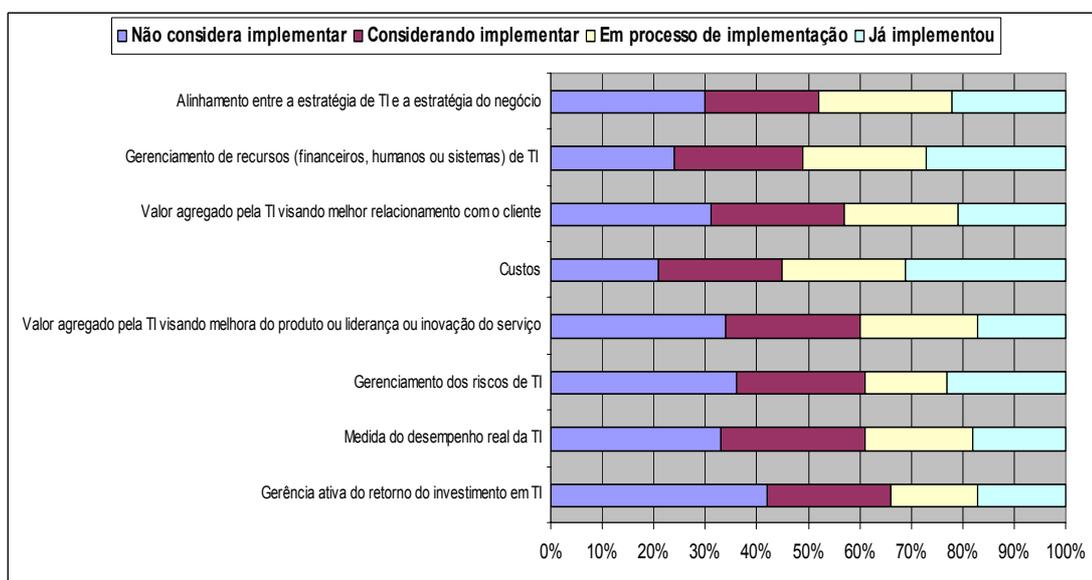


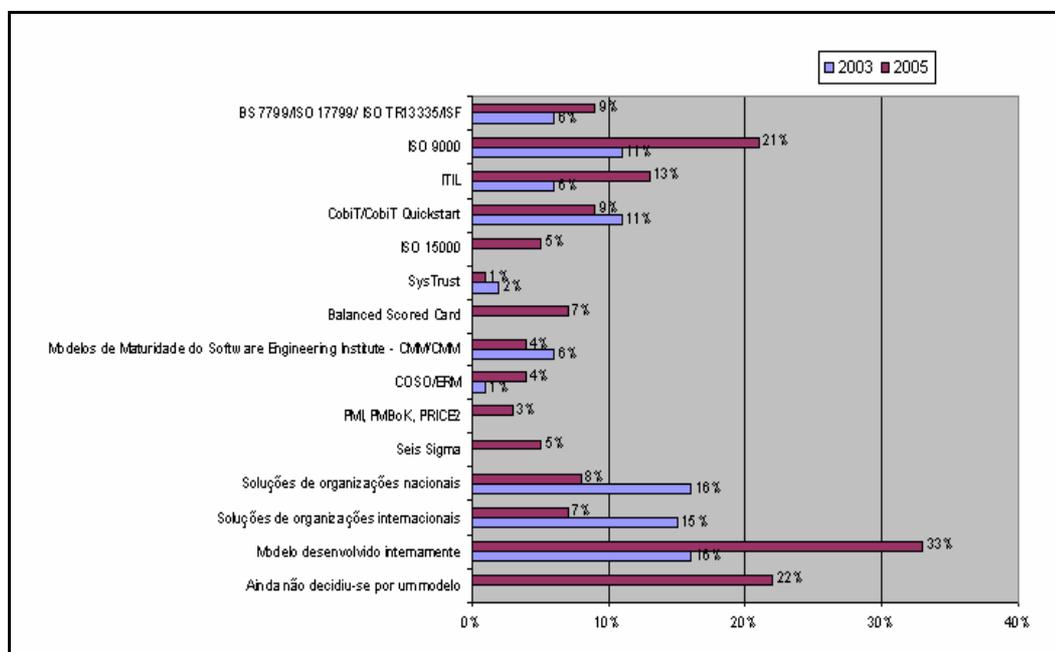
Tabela 5.2 – Situação da implementação parcial de Governança



A terceira questão destacada da pesquisa, sobre qual (ou quais) modelo as organizações utilizam – ou pretendem utilizar – para implementar a governança é apresentada na tabela 5.3. Um terço dos participantes utiliza ou

pretende utilizar um modelo desenvolvido internamente e aproximadamente um quarto deles ainda não se decidiu por qual modelo adotar.

Tabela 5.3 – Modelos de Governança utilizados



5.6 Casos

O professor Henrique Brodbeck relata, em palestras e aulas de cursos de Gestão Empresarial da Universidade Federal do Rio Grande do Sul, experiências da utilização dos modelos de Governança Corporativa [BRO2004].

A *Procter&Gamble* adotou o modelo proposto pelo ITIL em 1997. Segundo Brodbeck, com esta iniciativa a empresa economizou quinhentos milhões de dólares em quatro anos, cortou seus custos operacionais na faixa de seis a oito por cento e reduziu entre quinze e vinte por cento a equipe de tecnologia.

O governo de Ontário, no Canadá, adotou o ITIL para melhorar a prestação de serviços a vinte e cinco mil usuários em cerca de mil localidades. Criou uma área de Atendimento ao Usuário – para aperfeiçoar o atendimento – e reduziu os custos com chamados em quarenta por cento.

Brodbeck relata também a experiência do Estado de Kansas, nos Estados Unidos: utilização dos padrões do CobiT na estratégia de governo virtual para redução de custos e manutenção do nível de serviço.

Já a Dell Computer utiliza o CobiT como parte de sua política corporativa para manter o alto grau de qualidade de seus produtos.

No Brasil, o Banco ABN Amro iniciou a implantação do ITIL em 2001. Centralizou o atendimento a usuários e os chamados cresceram de vinte mil para sessenta mil devido ao aumento de controle dos processos. O tempo de atendimento foi reduzido em vinte por cento e o volume de reclamações em oitenta por cento. Noventa e quatro por cento dos atendimentos passaram a ser completados em menos de vinte segundos.

A Revista Info Corporate em sua trigésima edição traz relatos das experiências de empresas tais como Roche Brasil e Carrefour com os modelos ITIL e CobiT, ressaltando redução de custos e aumento de eficiência [OSS2006].

O crescente aumento de automatização dos processos no segmento bancário tem mobilizado as autoridades. O crescente investimento realizado pelo Sistema Financeiro Brasileiro em tecnologia da informação requer uma atenção dos dirigentes de TI na governança de TI. Segundo a Revista Banco Hoje, essa demanda visa adequar os custos de TI aos investimentos de forma a implementar os conceitos de governança aos serviços prestados de tecnologia da informação aos negócios da empresa [FIG2006].

Em 2001 foi criado pela Bovespa “um seguimento de listagem destinado à negociação de ações emitidas por empresas que se comprometem, voluntariamente, com a adoção de práticas de governança corporativa”. O resultado foi a valorização acima da média dessas ações no mercado e o anúncio do lançamento de um novo segmento com o objetivo de incentivar a ida de pequenas e médias empresas “firmemente comprometidas com o seu crescimento, com boas práticas de governança corporativa e com a busca da liquidez das suas ações no mercado secundário” [BOV2001].

Especificamente com relação à lei *Sarbanes-Oxley*, a revista Exame de fevereiro de 2006 relata a experiência de organizações onde a implantação

dos procedimentos exigidos pela lei propiciou a melhoria dos controles, auxílio na gestão e até mesmo corte de custos [EXA2006]:

- A empresa Siemens reduziu de trinta para cinco por cento os problemas em suas compras, tais como diferenças de preço, quantidade e características da mercadoria e o tempo de processamento caiu de cinco dias para quarenta e oito horas;
- O Banco ABM Amro Real – cuja experiência com o ITIL também foi relatada acima neste trabalho – baixou de oito para quatro dias úteis o prazo para fechamento das demonstrações contábeis mensais;
- A operadora de TV a cabo Net reduziu de onze para quatro as versões de cada documento legal a ser encaminhado ao mercado e cortou pela metade o prazo para consolidar suas demonstrações contábeis.

6. Acordos de nível de serviço

De forma genérica, um serviço é caracterizado por [APR2000]:

- Ênfase em venda direta ao cliente;
- Contato direto com o cliente;
- Geração e entrega por demanda;
- Menor tempo de conclusão;
- Não é necessariamente representado por um produto físico;
- Nem sempre pode ser transportado ou armazenado;
- Menor padronização em comparação com mercadorias;
- Concorrência de produção e consumo.

Uma manutenção de *software* pode ser definida como um serviço, dado seu menor tempo de execução – em comparação com o desenvolvimento de um novo sistema – e por não ser uma atividade padronizada. Por outro lado, uma das principais diferenças está na tangibilidade do produto percebido pelo usuário. O resultado de uma manutenção de *software* pode ser inspecionado e testado antes de ser entregue ao usuário (cliente).

A forma de demonstrar a contribuição das manutenções de software ao negócio é a utilização de acordos de nível de serviço, criando a percepção para o cliente, do serviço prestado.

A proposição de um modelo para acordos de nível operacional para controle do processo de manutenção de *software* alinhado às teorias de Governança de Tecnologia da Informação permite beneficiar a organização em diferentes aspectos: confiabilidade, avaliação de desempenho, previsões e análises de tendências.

Acordos de nível de serviço têm por objetivo prover garantias, dentro de determinados parâmetros, sobre um serviço; definir penalidades por não atingimento dessas garantias e possivelmente recompensar sua superação [SAL2003].

Os parâmetros a serem estabelecidos nos acordos normalmente relacionam-se a uma dentre as quatro seguintes características: prazo, custo, qualidade e flexibilidade.

Um contrato de manutenção de *software*, assim como em qualquer outro tipo de contrato regido por acordos de nível de serviço, deve capturar claramente as relações de dependência – conseqüências positivas e negativas – existentes nas cláusulas contratuais.

Em [BOU1999], Bouman apresenta diferentes formas de estruturação de um acordo de nível de serviço. Em uma delas, propõe-se fundamentá-los em resultados ao invés de esforços. Nestes casos, é imprescindível a descrição apropriada e o consenso entre as partes (fornecedor e cliente) sobre dos resultados a serem alcançados.

Outra estruturação proposta por Bouman é a elaboração de um inventário com um conjunto de orientações padronizadas para especificação dos acordos. Uma destas orientações é a identificação das partes relacionadas com o serviço a ser prestado. Deve-se também explicitar as expectativas ou requisitos de cada serviço.

No caso de acordos de nível de serviço internos, Bouman destaca as expectativas e requisitos:

- O cliente deseja concentrar-se em seu próprio trabalho e espera um serviço homogêneo da área de TI da organização, permitindo-o interagir com um conjunto de sistemas de informação. A forma de composição desses sistemas e serviços tem importância menor para o cliente. Estas circunstâncias devem ser refletidas nos acordos de nível de serviço estabelecidos de forma a descrever o desempenho e a qualidade dos sistemas, e não de seus componentes;
- A área de manutenção de sistemas deve prover o cliente de uma imagem real sobre quais expectativas ter, ou seja, deve fornecer uma percepção clara quanto a qualidade do serviço a ser entregue. A equipe de manutenção, durante uma implementação, deve focalizar principalmente a estabilidade e

manutenibilidade do sistema, ao invés da funcionalidade a ser modificada.

Em [SAL2003], Sallé alerta também para a necessidade de ligação entre os papéis (por exemplo compradores e provedores de serviços) presentes no contrato e pessoas reais para exercê-los. Devido à natureza dinâmica das interações de negócios modeladas, nem todas as obrigações especificadas nos contratos estão ativas em um determinado momento de sua vigência. Algumas delas tornar-se-ão ativas com o passar do tempo, enquanto outras podem até nem serem ativadas, como no caso de penalidade nunca materializadas. Quando a análise do contrato for concluída, apenas as obrigações ativas e suas conseqüências são levadas em conta.

Neste trabalho são propostos acordos operacionais para compor acordos de nível de serviços adequados considerando-se parâmetros de qualidade, custo e prazo. A relevância dos acordos operacionais para controle do processo de manutenção de *software* propostos neste trabalho são abordados nas próximas seções.

6.1 Gerenciar Riscos

De acordo com Webster em [WEB2005], o gerenciamento de riscos tem ganho grande importância na área de engenharia de *software*. Neste contexto várias abordagens de processos de gerenciamento de riscos são encontradas na literatura. No entanto, existe um consenso entre os processos de identificação e análise de riscos. Alguns autores consideram esta disciplina a primeira dentre as melhores práticas de gerenciamento de projetos. No entanto poucos estudos foram desenvolvidos para manutenção de sistemas, dentre eles a adaptação de atividades de gerenciamento de riscos de desenvolvimento para manutenção de *software*. Por outro lado, a manutenção de sistemas é um dos grandes desafios da engenharia de *software*, pelo fato de corresponder até 70% dos custos de um sistema de *software*. Isto é demonstrado claramente pelo tempo gasto e pelo esforço requerido para manter *software*.

Riscos sempre existem em qualquer atividade entretanto deve-se buscar diminuir a probabilidade e/ou o impacto da sua ocorrência.

A Lei *Sarbanes-Oxley* reforma procedimentos de demonstração e governança corporativa e em seus títulos e seções define as responsabilidades da organização em relação ao gerenciamento de risco. Entretanto, por ser uma lei e não uma norma, a SOX define o que deve ser feito, mas não fornece diretrizes sobre como fazê-lo. Muitas companhias estão adotando a estrutura de gerenciamento de risco do Comitê de Organizações Patrocinadoras da Comissão *Treadway* (COSO) como uma norma de conformidade com a SOX [STI2005].

Em seu artigo sobre controles internos, Gherman afirma: “O CobiT, por sua vez, procura ocupar o espaço entre a Gestão de Riscos voltada para o Negócio (atendida, por exemplo, pelo COSO), a Gestão de Serviços em TI (por exemplo, por meio do ITIL) e a Gestão da Segurança da Informação (por exemplo, tratada pela BS7799)”. A figura 6.1 ilustra a interação dos modelos de gestão citados.

Ainda segundo Gherman: “Dessa forma, o COBIT permite alinhar os objetivos dessas áreas de conhecimento às estratégias e aos princípios de governança corporativa, garantindo, assim, a sistematização dos processos e atividades desempenhadas pelas respectivas áreas e funções para o alcance dos objetivos do negócio e redução dos riscos operacionais” [GHN2005].

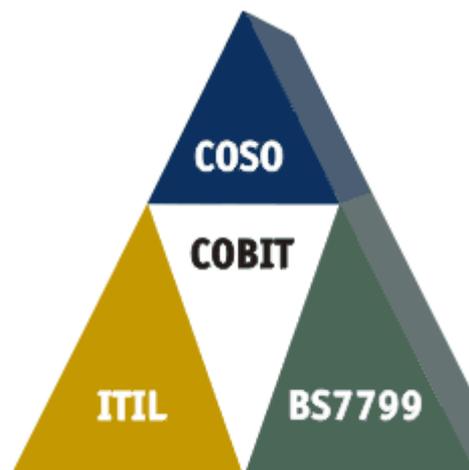


Figura 6.1 – A interação dos modelos de gestão COSO, ITIL, BS7799 e COBIT [GHN2005]

De acordo com Alberto Bastos, sócio-fundador da consultoria Módulo (empresa atuante na área de Segurança da Informação), conhecer o risco (exato) de um servidor parar; de um determinado dado ser roubado de um local seguro; de um usuário burlar um processo; de um sistema ser invadido; de uma infra-estrutura física de TI ser vulnerável a incêndio, umidade ou goteira representam ações de gestão de riscos na área de TI. Como a TI hoje é o suporte para muitos negócios, saber tudo isso é primordial, pois vários desastres na tecnologia significam desastre nos negócios. Robson Calil Chaar, gerente-sênior de riscos empresariais da Deloitte do Brasil, diz mais: gestão de riscos é trocar o instinto por ações planejadas. Nas suas palavras, significa abandonar de vez a correria desesperada para colocar no ar um servidor parado ou subir os sistemas de *backup* urgentemente para recuperar arquivos de extrema importância apagados por descuido. Gestão de risco na TI significa não querer mais apagar incêndios na TI, e sim evitá-los. E, no caso das situações fora de controle, como o surgimento de pragas digitais mais potentes e destruidoras, aprender a gerenciar e conviver com o risco.

Frederico José de Souza Burgos, chefe da divisão de segurança do departamento de TI do Banco Central, afirma seguir algumas práticas para mitigar alguns riscos nos sistemas do Bacen; e elaborar, de fato, planos de continuidade de negócios. Por exemplo: todo programa robusto usado pelo Bacen tem o código analisado por uma equipe de segurança ao ser finalizado, publicado ou migrado de um servidor para outro. Apesar desta ação representar uma pequena parcela de um modelo de gestão de riscos, Alberto Bastos enaltece a preocupação de Burgos: "os processos podem ser burlados, e um código prejudicial pode ser colocado no programa, de propósito ou não" [INF2006].

6.2 Gerenciar o prazo e o custo e garantir a qualidade da manutenção

O gerenciamento do prazo e do custo das atividades relacionadas à manutenção de software está diretamente ligado ao gerenciamento da qualidade do produto gerado e por conseguinte, ligados ao serviço prestado.

É critério integrante da avaliação por parte do cliente o atendimento aos prazos e orçamentos propostos para a manutenção. Satisfazer ou exceder as necessidades do cliente envolve equilibrar questões de escopo, tempo, custo e qualidade.

Cada vez mais, exige-se qualidade nos serviços prestados pela área de Tecnologia da Informação das organizações. A qualidade dos serviços de TI é medida através do atendimento às necessidades do cliente e pela qualidade do processo de desenvolvimento dos produtos integrantes do serviço prestado. Por outro lado, a qualidade dos processos é mensurada principalmente através do cumprimento entre outros requisitos, do prazo de conclusão e do custo de desenvolvimento do serviço.

De acordo com o CobiT, a garantia da qualidade é alcançada através de ações tais como a definição de padrões de qualidade, a monitoração e revisão do desempenho quanto aos padrões estabelecidos e através da busca da melhoria contínua da qualidade.

A aplicação de acordos de nível de serviço ao processo de manutenção de *software* visa garantir a qualidade do produto através da qualidade no processo de manutenção.

Um efetivo gerenciamento de mudanças, conforme descrito no ITIL produz benefícios tais como:

- Melhora no alinhamento dos serviços de TI aos requisitos do negócio;
- Aumento da visibilidade e comunicação tanto para o negócio quanto para a equipe de suporte de serviços;
- Melhora na avaliação de riscos;
- Redução de impactos negativos da mudança na qualidade dos serviços;
- Melhora na avaliação do custo de mudanças propostas antes de serem executadas;
- Diminuição do número de mudanças canceladas no momento da implantação;

- Melhora do gerenciamento de problemas e disponibilidade através da utilização de informações obtidas e acumuladas com o processo de gerenciamento de mudanças;
- Aumento da produtividade dos usuários devido à diminuição de interrupção e serviços de maior qualidade.

6.3 Gerenciar o desempenho da manutenção

No CobiT, o gerenciamento do desempenho dos serviços de TI satisfaz o objetivo de garantir o desempenho dos sistemas aplicativos e soluções técnicas organização e, sob a ótica dos objetivos da organização, permite diminuir o custo do processo. Para isso, a atividade deve focar nos requisitos de tempo de resposta, minimizar o tempo de interrupções e prover a melhoria contínua do desempenho através de monitoração e medição.

Dentre os benefícios apontados no ITIL para os processos de gerenciamento da capacidade, processo este relacionado com o desempenho dos serviços, estão:

- Aumento da eficiência e redução de custos;
- Redução de riscos;
- Previsões da capacidade de infra-estrutura adequada mais confiáveis;

O gerenciamento do desempenho de um serviço está ligado ainda com a sua disponibilidade, ou seja, com a habilidade de realizar sua função em um determinado instante ou período de tempo. E esta propriedade está diretamente ligada a um dos mais importantes resultados esperados dos serviços de TI: a satisfação do cliente com o serviço prestado;

6.4 Garantir a continuidade

A garantia da continuidade, segundo o CobiT, propicia o menor impacto para o negócio em caso de ocorrência de uma interrupção em um serviço. Para isso, o processo concentra-se em construir soluções automatizadas

robustas e no desenvolvimento, manutenção e teste de planos de continuidade.

O ITIL descreve diferentes possíveis impactos para o negócio devido a interrupções de serviços de TI:

- Perda de receita;
- Custos adicionais;
- Perda de participação no mercado – momentânea ou a longo prazo;
- Não conformidade com leis, regulamentos, padrões ou ainda com responsabilidade moral;
- Riscos a segurança pessoal;
- Embaraço político, corporativo ou pessoal;
- Perda de benefícios, credibilidade, boa imagem ou reputação;
- Perda de capacidade operacional.

6.5 Garantir a segurança

A garantia da segurança está associada à necessidade de manter a integridade da informação e de proteger os bens de TI. Este processo, tanto no modelo definido no CobiT quanto na norma ISO 17799, inclui o estabelecimento e manutenção de regras de segurança e responsabilidades, políticas, padrões e procedimentos. Envolve também a realização de monitoração da segurança, testes e implementação de ações corretivas para as fragilidades identificadas. Desta forma, o efetivo gerenciamento da segurança garante a aderência aos controles impostos pela Lei *Sarbanes-Oxley* e sobretudo alinha a área de tecnologia da informação às diretrizes de governança corporativa, protegendo os bens de TI e minimizando o impacto de vulnerabilidades de segurança e de incidentes no negócio.

6.6 Treinar usuários

O efetivo treinamento de todos os usuários de sistemas, requer a identificação das necessidades de treinamento de cada grupo de usuário. Além de identificar as necessidades, o CobiT propõe a definição e execução de uma estratégia para o treinamento efetivo e medição de resultados. Um programa de treinamento adequado aumenta a utilização da tecnologia através da redução de erros de usuários e aumento da produtividade. Para isso, é necessário o estabelecer o conteúdo do treinamento, organizar, realizar, monitorar e reportar sua efetividade.

Dentre as atividades propostas para o gerenciamento de problemas no ITIL, o treinamento de usuários é uma forma de tratá-los pró-ativamente. Os benefícios desta iniciativa são:

- O aumento da qualidade do serviço;
- Redução do volume de incidentes e
- Melhora na aprendizagem e conhecimento organizacional.

6.7 Gerenciar versões

Conforme as organizações tornam-se mais dependentes da tecnologia da informação, o controle e segurança de seus sistemas de informação assumem maior importância. É necessário preparar-se para lidar com freqüentes liberações de novas versões de equipamentos e sistemas sem sacrificar a qualidade do serviço prestado. Os controles e mecanismos propostos no ITIL para o gerenciamento de versões auxiliam a suportar este requisito de forma eficiente e econômica.

Os principais benefícios do gerenciamento de versões – combinado com o efetivo gerenciamento de mudanças – são:

- Uma alta taxa de sucesso em liberação de versões de *hardware* e *software* e conseqüentemente um aumento na qualidade dos serviços oferecidos à organização;

- Consistência nos processos de versionamento de plataformas de *hardware* ou de ambientes de *software*;
- Diminuição de interrupções de serviços através da sincronização de versões em pacotes envolvendo componentes de diferentes plataformas e ambientes;
- Garantia de utilização de equipamentos e sistemas de qualidade em produção, devido à construção apropriada de versões com componentes submetidos a controle de qualidade e testes;
- Ambientes de teste e produção estáveis devido à combinação de mudanças em versões, reduzindo o número de implementações individuais;
- Melhor utilização do tempo do usuário em decorrência da combinação dos esforços de testes realizados em versões;
- Criação de expectativas positivas com a divulgação antecipada de uma programação de liberação de versões;
- Redução de erros devido ao controle de versões dos ambientes de teste e produção, evitando a incorporação de versões incorretas;
- Manutenção de um registro completo das mudanças ocorridas em ambiente de produção, permitindo a realização de trilhas de auditoria;
- Controle e proteção apropriados dos componentes, dos quais a organização pode ser altamente dependente;
- Habilidade em absorver freqüentes alterações nos sistemas sem afetar a qualidade do serviço através do agrupamento de mudanças em versões únicas, bem compreendidas e controladas;

O crescimento da eficiência e efetividade do gerenciamento de versões implica no crescimento da produtividade da equipe envolvida. Ainda mais importante, os benefícios desta produtividade chegam aos usuários finais,

conforme novas versões tornem-se menores e melhor planejadas, com o treinamento apropriado e com documentação de alta qualidade.

7. O modelo de acordos operacionais para controle do processo de manutenção de *software*

A proposição de modelos para acordos operacionais visa, em primeira análise, tornar a manutenção de *software* uma atividade de menor custo e maior qualidade.

O alcance deste objetivo através destes acordos implica em ações a serem tomadas, tais como a formalização das expectativas de usuários e clientes da área de tecnologia da informação.

A busca pela satisfação das expectativas de clientes, redução de custos e aumento da qualidade também proporciona outros benefícios. Avaliações de desempenho, possibilidade de realização de previsões e análises de tendências auxiliam as organizações na tomada de decisões estratégicas.

A análise dessas expectativas e benefícios demonstra a necessidade de serviços adequados, eficazes, confiáveis e disponíveis. Tal fato aponta para a aplicação dos conceitos propostos pelos modelos de governança, onde se destaca o alinhamento da tecnologia da informação à necessidade do negócio.

Dentre as atividades envolvidas na governança de TI destacam-se:

- Garantir suporte aos objetivos e estratégias da organização;
- Controlar, medir e auditar a execução e a qualidade dos serviços;
- Viabilizar o acompanhamento de contratos internos e externos;
- Definir condições para o exercício eficaz da gestão com base em conceitos consolidados de qualidade;
- Especificar como as decisões são tomadas e executadas;
- Identificar os responsáveis por cada um dos processos de TI.

Acordos de nível de serviço – e conseqüentemente acordos operacionais – possuem importante papel dentro do acompanhamento de contratos internos e externos da área de tecnologia da informação: eles são responsáveis por formalizar as expectativas e responsabilidades dos envolvidos.

A utilização de modelos para definição de acordos de nível de serviço em contratos de manutenção de *software* busca a melhor aplicação dos recursos das organizações, cada vez mais dependentes dos seus sistemas de *software* para executar suas atividades fins ou periféricas. O alinhamento aos preceitos de governança reforça sua adequação.

O processo Gerenciamento do Nível de Serviço do modelo de governança de TI proposto no ITIL orienta a definição de todos os acordos operacionais deste modelo. Conseqüentemente, a própria utilização de acordos de nível de serviço já configura um indicativo de governança.

Assim como o gerenciamento do nível de serviço está presente no ITIL, também consta do CobiT. Em ambos, a noção de avaliação do acordo estabelecido, seu monitoramento e aperfeiçoamento são essenciais. O fundamento básico é o entendimento do princípio – o que não é medido não é gerenciado. Acompanhar para medir, medir para controlar, controlar para gerenciar, e gerenciar para fazer os ajustes necessários. O processo é constante; o ciclo sempre termina onde começa. É, portanto, dinâmico e contínuo. As verificações da aplicabilidade e dos parâmetros dos acordos estabelecidos compõem o processo de melhoria contínua da organização. Os acordos aqui propostos devem ser aperfeiçoados a cada repetição do ciclo, garantindo sua adequação.

A lei *Sarbanes-Oxley*, mesmo não sendo um modelo de processos de governança, impulsiona as organizações no sentido de organizar e controlar o ambiente corporativo. Os controles da tecnologia de informação alinhados à lei e sobre os quais é estabelecida a relação com os acordos de nível de serviço são:

- Administração da segurança;
- Gerenciamento de mudanças;
- Gerenciamento de dados e recuperação de desastres;
- Gerenciamento de problemas e operações e
- Gerenciamento de recursos

Esse conjunto de controles é abordado em detalhes na revisão bibliográfica, dentro da seção 4.5, onde a Lei *Sarbanes-Oxley* é descrita.

Os acordos operacionais propostos no modelo são compostos de:

- Descrição da manutenção a ser implementada;
- Partes envolvidas – cliente e fornecedor do serviço;
- Tipo do acordo: interno e/ou externo. Um determinado acordo pode ser aplicável apenas internamente (entre a área de TI e outra área da organização), apenas externamente (entre a organização e um fornecedor externo) ou em ambos casos;
- Tipo da manutenção: corretiva, perfectiva, adaptativa ou preventiva. Os acordos propostos não necessariamente são aplicáveis a todos os tipos de manutenção;
- Atividade a ser verificada;
- Descrição da atividade: explica as ações a serem executadas para alcançar o nível definido;
- Objetivo a ser alcançado com a realização das atividades;
- Indicadores: definem métricas para demonstrar o alcance do nível acordado;
- Meta a cumprir: aplicação de valores concretos a serem alcançados em cada indicador. O modelo destaca esses valores, podendo ser alterados conforme a natureza do negócio;
- Processo IEEE: indica, dentro do processo de engenharia de sistemas, sub-processo de controle do padrão IEEE, qual atividade relaciona-se com o acordo operacional proposto;
- Governança: nesta seção são apresentadas as referências aos modelos de governança, demonstrando a relação entre o acordo e o processo específico dos modelos de governança citados. Quando aplicável, também é apresentada a correlação com a Lei *Sarbanes-Oxley* ou o guia do gerenciamento de projetos – PMBoK.

No apêndice é apresentada uma figura demonstrando o mapeamento de cada acordo de nível de serviço proposto com os processos de governança do CobiT e do ITIL e com os controles de TI integrantes da Lei *Sarbanes-Oxley*.

7.1 Gerenciar riscos

O objetivo do estabelecimento de acordos operacionais relacionados ao gerenciamento de riscos está relacionado com a necessidade de uma manutenção de *software* ser acompanhada da análise dos possíveis impactos de sua implementação sobre os processos e objetivos do negócio.

Esta atividade permite reduzir a ocorrência de incidentes causados pela manutenção do sistema, além de viabilizar uma avaliação do custo da implementação de planos de contingência. Esta abordagem em acordos operacionais garante a pró-atividade, o domínio sobre os eventos com possível impacto sobre o negócio.

A definição do percentual de riscos a serem mitigados está relacionada com o seu impacto sobre o negócio. Riscos de alto impacto e/ou probabilidade de ocorrência devem sempre possuir uma estratégia de tratamento, seja através de uma contingência ou redução de impacto ou probabilidade. Acordos de níveis de serviço para manutenções realizadas em sistemas pertencentes a processos de negócio não essenciais para a organização podem estabelecer percentuais de metas de gerenciamento de riscos mais flexíveis.

No ciclo de vida de engenharia de sistemas proposto pelo IEEE, dentro da etapa de suporte – relacionada com a manutenção de sistemas – no processo de controle, a atividade de gerenciamento de riscos está presente. Esta atividade é composta por ações tais como a preparação do gerenciamento de riscos, avaliação de riscos, avaliação das estratégias de tratamento de riscos e controle de riscos.

Além dos modelos de governança CobiT e ITIL, o PMBoK trata estratégias e atividades a serem realizadas para um efetivo gerenciamento de riscos. Conforme a Lei *Sarbanes-Oxley*, o gerenciamento de riscos demonstra o domínio da organização sobre seus processos negócio.

Acordo Operacional	
Serviço de Manutenção de Software	
Descrição:	{ Descrição detalhada da manutenção }
Envolvidos	
Cliente:	{ Área cliente do serviço }
Fornecedor:	{ Fornecedor do serviço }
Aplicabilidade	
Tipo do Acordo:	(X) Interno (X) Externo
Tipo da Manutenção:	(X) Corretiva (X) Perfectiva (X) Adaptativa (X) Preventiva
Nível da Atividade	
Atividade:	Gerenciar riscos
Descrição:	Realização de atividades objetivando reduzir a probabilidade e o impacto dos riscos da manutenção. O impacto deve ser avaliado tanto na TI quanto no negócio. Avaliação da probabilidade e impacto, elaboração de planos de respostas a riscos.
Objetivo:	Mitigar os riscos da manutenção de software
Indicadores de Nível Operacional	
INS1	Percentual de riscos concretizados e mitigados
Meta a cumprir:	Mitigação de riscos de alto impacto: <u>100%</u> Mitigação de riscos de médio impacto: 80%
Processo IEEE	

Controle	Gerenciamento de Riscos
Governança	
COBIT	Processo PO9 – Avaliar e gerenciar os riscos da área
ITIL	Suporte de Serviços de TI – Gerenciamento de Mudanças
SOX	Controle – Gerenciamento de Mudanças
PMBok	Área de conhecimento – Gerenciamento do risco

7.2 Gerenciar o prazo da manutenção

O estabelecimento de mecanismos de controle do prazo de uma manutenção de *software* aproxima-se das diretrizes de gerenciamento de prazo em projetos. O PMBoK possui uma área de conhecimento orientada às atividades de gerenciamento de prazos.

O controle do prazo de implementação de uma manutenção através de acordos operacionais visa, em primeira instância, atender às expectativas dos envolvidos com relação à entrega do produto.

É o atendimento dessa expectativa um dos responsáveis pela percepção de qualidade do produto a ser entregue. (Outros parâmetros de qualidade são a custo dentro do orçamento e conformidade com o requisito).

O percentual de desvio do prazo de entrega da manutenção deve ser definido de acordo com a criticidade da manutenção envolvida. Uma alteração em um sistema responsável pelo serviço prestado ao cliente final, por exemplo, sugere um desvio aceitável menor em comparação com uma manutenção em um sistema periférico e utilizado por um usuário interno à organização.

No processo de controle do IEEE, a atividade de medição do progresso e desempenho destaca a necessidade de demonstração do acompanhamento dos prazos planejados e concretizados durante o processo. Medições do desempenho dos prazos permitem avaliar o progresso da manutenção, através, por exemplo, da análise de valor agregado: esforço planejado em comparação ao esforço realmente agregado.

Acordo Operacional		
Serviço de Manutenção de Software		
Descrição:	<i>{ Descrição detalhada da manutenção }</i>	
Envolvidos		
Cliente:	<i>{ Área cliente do serviço }</i>	
Fornecedor:	<i>{ Fornecedor do serviço }</i>	
Aplicabilidade		
<i>Tipo do Acordo:</i>	<input checked="" type="checkbox"/> <i>Interno</i>	<input checked="" type="checkbox"/> <i>Externo</i>
<i>Tipo da Manutenção:</i>	<input type="checkbox"/> <i>Corretiva</i>	<input checked="" type="checkbox"/> <i>Perfectiva</i>
	<input checked="" type="checkbox"/> <i>Adaptativa</i>	<input checked="" type="checkbox"/> <i>Preventiva</i>
Nível da Atividade		
Atividade:	Gerenciar o prazo da manutenção	
Descrição:	Em manutenções tratadas como projetos – normalmente nos casos de manutenções evolutivas, elaborar o cronograma e atualizar o andamento das atividades.	
Objetivo:	Garantir a entrega da manutenção no prazo acordado Garantir a qualidade da manutenção	
Indicadores de Nível Operacional		
INS1	Desvio do período (meses, dias, horas) de entrega da manutenção	
Meta a cumprir:	Atraso na entrega inferior a <u>10%</u> do prazo acordado	
Processo IEEE		
Controle	Medição do progresso e desempenho	

Governança

COBIT

Processo – PO10 Gerenciar projetos

Processo – PO8 Gerenciar a qualidade

PMBok

Área de conhecimento Gerenciamento do prazo

7.3 Gerenciar o custo da manutenção

Acordos operacionais relacionados ao gerenciamento de custos justificam-se de forma análoga aos acordos estabelecidos para o gerenciamento de prazo: visam atender às expectativas dos envolvidos com relação à entrega do produto e contribuir para a percepção de qualidade do produto a ser entregue.

No processo de controle do IIEEE, a atividade de medição do progresso e desempenho também se refere à necessidade de demonstração do acompanhamento dos custos do processo.

Diferentemente, o percentual de desvio do custo da manutenção deve ser definido de acordo com o risco envolvido na manutenção. Atividades com alto risco possuem maior possibilidade de estouro de custos devido à eventual necessidade de implementação de planos de contingência. Por outro lado, manutenções com baixo risco sugerem uma margem menor de variação dos custos.

O PMBoK possui uma área de conhecimento orientada às atividades de gerenciamento de custos em projetos aplicáveis a manutenções evolutivas.

COBIT	Processo – PO10 Gerenciar projetos Processo – PO8 Gerenciar a qualidade
ITIL	Suporte de Serviços de TI – Gerenciamento de Mudanças
PMBok	Área de conhecimento Gerenciamento do custo

7.4 Gerenciar o desempenho da manutenção

A garantia do desempenho adequado do sistema após a implantação da manutenção está relacionada com o atendimento do requisito do negócio, com a expectativa de nível serviço prestado. Um acordo operacional associado ao desempenho da manutenção busca manter a disponibilidade dos serviços e permite a avaliação da adequação da infra-estrutura disponível.

As metas de tempos de resposta (segundos, milissegundos etc) devem ser estabelecidas com base na necessidade do negócio, ou seja, na importância do processo de negócio afetado com a manutenção, visando garantir a satisfação do cliente final.

Acordos operacionais com indicadores e metas baseados na análise de picos de carga buscam garantir a disponibilidade dos serviços através de uma implementação compatível com a infra-estrutura de TI disponível.

O percentual de crescimento do pico de carga aceitável deve ser estabelecido com base nos recursos de TI disponíveis e no volume de transações ou submissões esperadas para os serviços afetados pela manutenção.

Informações de utilização da infra-estrutura permitem a realização de previsões de necessidades de atualizações futuras de equipamentos. A aplicação de conceitos de engenharia econômica tais como depreciação, retorno de investimento e taxa interna de retorno orientam essas análises.

O controle sobre a satisfação dos requisitos e objetivos da organização são os aspectos presentes na atividade de medição do progresso e desempenho, processo de controle do IEEE, relacionados com a atividade de gerenciamento de desempenho proposta neste acordo.

Acordo Operacional	
Serviço de Manutenção de Software	
Descrição:	{ Descrição detalhada da manutenção }
Envolvidos	
Cliente:	{ Área cliente do serviço }
Fornecedor:	{ Fornecedor do serviço }
Aplicabilidade	
<i>Tipo do Acordo:</i>	(X) Interno (X) Externo
<i>Tipo da Manutenção:</i>	(X) Corretiva (X) Perfectiva
	(X) Adaptativa (X) Preventiva
Nível da Atividade	
Atividade:	Gerenciar o desempenho da manutenção
Descrição:	Definir, documentar e prover o tempo de resposta esperado nas funcionalidades em manutenção. Definir e documentar a infra-estrutura necessária – capacidade – para suportar a manutenção.
Objetivo:	Garantir o desempenho adequado do sistema após a implantação da manutenção
Indicadores de Nível Operacional	
INS1	Percentual de tempos de resposta esperados não atingidos
Meta a cumprir:	Tempo de resposta menor que <u>x segundos (milissegundos, minutos etc)</u> em <u>99%</u> das transações/submissões
INS2:	Picos de carga
Meta a cumprir:	Crescimento inferior a <u>1%</u> em picos de carga com a implantação da manutenção, durante <u>x meses (dias, horas)</u>

após a implantação	
Processo IEEE	
Controle	Medição do progresso e desempenho
Governança	
COBIT	Processo – ES3 Gerenciar desempenho e capacidade
ITIL	Entrega de Serviços de TI – Gerenciamento da Capacidade Entrega de Serviços de TI – Gerenciamento de Disponibilidade

7.5 Garantir a continuidade

O estabelecimento de um acordo operacional para garantir a continuidade do serviço visa proporcionar o menor impacto em caso de interrupção de serviço decorrente da implantação da manutenção.

No processo de controle do IEEE, o desenvolvimento de planos de contingência e recuperação para as deficiências identificadas compõem a atividade de medição do progresso e desempenho da etapa de suporte (assim como das demais etapas) do ciclo de vida de engenharia de sistemas.

A disponibilidade dos serviços associados aos processos de negócio críticos para a organização pode ser traduzida claramente em possibilidade de aumento de receita e em satisfação do cliente.

A elaboração de planos de contingência para manutenções realizadas sobre sistemas dos processos de negócio críticos visa garantir a resistência e recuperação de falhas devido a um erro ou falha na manutenção. Quanto mais crítico for considerado um processo, maior a necessidade de elaboração de um plano de contingência. Desta forma, a meta dos processos de negócio a serem cobertos pelos planos de contingência deve levar em conta a importância dos processos envolvidos para a organização.

Indicadores associados à duração ou ao volume de interrupções na ponta também avaliam a disponibilidade do serviço. Acordos operacionais para manutenções efetuadas em serviços cuja interrupção causa impacto para os objetivos do negócio devem estabelecer metas mais rígidas.

Um indicador operacional associado ao volume de incidentes visa garantir a satisfação do usuário ou cliente do serviço afetado pela manutenção. A meta para esse indicador deve ser baseada em critérios tais como a visibilidade e importância do usuário ou cliente do sistema ou serviço afetado pela manutenção de *software*.

Acordo Operacional	
Serviço de Manutenção de Software	
Descrição:	{ Descrição detalhada da manutenção }
Envolvidos	
Cliente:	{ Área cliente do serviço }
Fornecedor:	{ Fornecedor do serviço }
Aplicabilidade	
<i>Tipo do Acordo:</i>	(X) Interno (X) Externo
<i>Tipo da Manutenção:</i>	(X) Corretiva (X) Perfectiva
	(X) Adaptativa (X) Preventiva
Nível da Atividade	
Atividade:	Garantir a continuidade
Descrição:	Elaborar, testar e treinar a aplicação de Planos de Contingência.
Objetivo:	Garantir o menor impacto em caso de interrupção de serviço decorrente da implantação da manutenção
Indicadores de Nível Operacional	
INS1	Percentual de processos de negócio críticos cobertos pelos Planos de Contingência
Meta a cumprir:	Tratamento de <u>100%</u> dos processos de negócio críticos associados à manutenção
INS2	Duração de interrupções na ponta
Meta a cumprir:	Interrupções com impacto inferior a <u>x segundos (minutos, horas)</u> para o usuário

INS3	Volume de interrupções na ponta
Meta a cumprir:	Ocorrência de <u>Q</u> interrupções na ponta devido à implantação da manutenção durante <u>x meses (dias, horas)</u>
INS4	Volume de incidentes
Meta a cumprir:	Ocorrência de <u>Q</u> incidentes devido à implantação da manutenção durante <u>x meses (dias, horas)</u>
Processo IEEE	
Controle	Medição do progresso e desempenho
Governança	
COBIT	Processo – ES4 Garantir a continuidade dos serviços
SOX	Controle – Gerenciamento de Mudanças Controle – Gerenciamento de Problemas e Operações
ITIL	Suporte de Serviços de TI – Gerenciamento de Mudanças Suporte de Serviços de TI – Gerenciamento da Continuidade dos Serviços

7.6 Garantir o controle da qualidade

Qualidade é o atendimento das necessidades do cliente. Um acordo de nível de serviço para garantir a qualidade da manutenção deve ser aplicado ao processo de desenvolvimento: utilização de padrões, elaboração, execução e documentação de planos de testes.

O PMBoK possui uma área de conhecimento orientada às atividades de gerenciamento da qualidade em projetos aplicáveis ao processo de manutenção de *software*.

Padrões e normas ISO para desenvolvimento de *software* também podem ser utilizados.

A avaliação da qualidade de um produto através de acordos de nível de serviço pode ser considerada subjetiva. Desta forma, é necessário transformar os requisitos de qualidade do cliente em itens concretos através de documentação e aceite entre as partes. O percentual de requisitos a serem atendidos deve ser crescente a cada interação entre o cliente do serviço com o seu fornecedor, buscando a melhoria contínua da qualidade.

Outro indicador possível de estabelecimento de acordo de nível de serviço relacionado à qualidade de uma manutenção de sistema é o percentual de atividades de testes documentadas em planos de testes. Sugere-se a documentação e execução de testes de todas as funcionalidades envolvidas ou afetadas pela manutenção.

Acordo de Nível Operacional	
Serviço de Manutenção de Software	
Descrição:	{ Descrição detalhada da manutenção }
Envolvidos	
Cliente:	{ Área cliente do serviço }
Fornecedor:	{ Fornecedor do serviço }
Aplicabilidade:	(X) Interna (X) Externa
Aplicabilidade	
Tipo do Acordo:	(X) Interno (X) Externo
Tipo da Manutenção:	(X) Corretiva (X) Perfectiva (X) Adaptativa (X) Preventiva
Nível da Atividade	
Atividade:	Garantir o controle da qualidade
Descrição:	Elaborar e aplicar um Plano de Gerenciamento da Qualidade. Elaborar e executar Planos de Testes incluindo aspectos de funcionalidade, desempenho, segurança, confiabilidade/disponibilidade. Elaborar e executar testes de regressão.
Objetivo:	Garantir o controle, a continuidade e o crescimento da qualidade do <i>software</i> em manutenção
Indicadores de Nível Operacional	
INS1	Percentual de atividades de testes documentadas em Planos de Testes
Meta a cumprir:	Documentação de atividades de testes de <u>100%</u> das funcionalidades em manutenção

INS2	Percentual de atendimento aos requisitos de qualidade
Meta a cumprir:	Atendimento mínimo de <u>90%</u> dos requisitos de qualidade identificados
Processo IEEE	
Controle	Medição do progresso e desempenho
Governança	
COBIT	Processo – PO8 Garantir a qualidade
ITIL	Suporte de Serviços de TI – Gerenciamento de Mudanças
PMBok	Área de conhecimento Gerenciamento da qualidade

7.7 Garantir a segurança

Acordos operacionais de garantia da integridade das informações e redução do impacto de vulnerabilidades de segurança visam permitir o acesso aos dados apenas a usuários autorizados e reduzir o número de incidentes provocadas pela manutenção do sistema.

Desta forma é possível fornecer a garantia de proteção contra acessos não autorizados às informações críticas e confidenciais para a organização. Por outro lado, a garantia de segurança objetiva propiciar a disponibilidade de serviços através da resistência e recuperação a falhas e ataques.

Os indicadores estabelecidos neste acordo convertem-se nos objetivos descritos acima. Deve-se garantir nenhuma ocorrência de acesso não autorizado às funcionalidades envolvidas na manutenção. Qualquer lacuna neste aspecto representa falha de segurança.

A ocorrência de incidentes com impacto público na reputação da empresa é medida através de notificações de empresas reguladoras. O número de notificações aceitável deve ser estabelecido de acordo com o porte da empresa.

Assim como requisitos de qualidade, os requisitos de segurança devem ser transformados em itens concretos através de documentação e classificação (imprescindível ou desejável).

O aceite deve ser formalizado entre as partes. Todos os requisitos de segurança considerados imprescindíveis devem ser atendidos. Requisitos de segurança considerados desejáveis permitem maior flexibilidade.

Existem requisitos de segurança genéricos para manutenções de sistemas, tais como controle de acesso, integridade de dados, criptografia e cópias de segurança. Por outro lado, há requisitos específicos da área de atuação da organização. Por exemplo, em telecomunicações, a confidencialidade dos registros de ligações. Tanto requisitos genéricos quanto requisitos específicos devem ser identificados, documentados e categorizados.

A atividade de gerenciamento de informações previsto no processo de controle proposto pelo IEEE destaca a necessidade de iniciativas relacionadas

à garantia da segurança e integridade de dados para prevenir a perda ou alteração indevida de dados.

A norma ISO 17799 possui diretrizes de gestão da segurança e pode ser utilizada para orientar a definição de requisitos de segurança.

Acordo Operacional	
Serviço de Manutenção de Software	
Descrição:	{ Descrição detalhada da manutenção }
Envolvidos	
Cliente:	{ Área cliente do serviço }
Fornecedor:	{ Fornecedor do serviço }
Aplicabilidade	
<i>Tipo do Acordo:</i>	(X) Interno (X) Externo
<i>Tipo da Manutenção:</i>	(X) Corretiva (X) Perfectiva
	(X) Adaptativa (X) Preventiva
Nível Operacional	
Atividade:	Garantir a segurança
Descrição:	Identificar os requisitos de segurança, vulnerabilidades e ameaças à manutenção do sistema
Objetivo:	Garantir a integridade das informações e minimizar o impacto de vulnerabilidades de segurança provocadas pela manutenção do sistema
Indicadores de Nível Operacional	
INS1	Acessos não autorizados
Meta a cumprir:	Ocorrência de <u>0</u> casos de acesso não autorizados aos dados ou funcionalidades envolvidos na manutenção
INS2	Número de incidentes com impacto público na reputação da empresa
Meta a cumprir:	Ocorrência de menos de <u>x</u> notificações de empresas reguladoras (<i>Ex, Procon</i>) devido a incidente causado pela manutenção durante <u>x meses (dias, horas etc)</u> após a

implantação	
INS3	Percentual de atendimento aos requisitos de segurança
Meta a cumprir:	Atendimento mínimo de <u>100%</u> dos requisitos de segurança identificados como imprescindíveis
	Atendimento mínimo de <u>80%</u> dos requisitos de segurança identificados como desejáveis
Processo IEEE	
Controle	Gerenciamento de Informações
Governança	
COBIT	Processo – ES5 Garantir a segurança dos sistemas
SOX	Controle – Administração da Segurança

7.8 Treinar usuários

Um acordo operacional baseado em treinamento de usuários tem por objetivo alcançar a satisfação do usuário com o serviço prestado no qual a manutenção de *software* está envolvida.

A transferência do conhecimento para usuários garante a utilização efetiva e eficiente das funcionalidades da manutenção e a disseminação das políticas e procedimentos envolvidos.

Um indicador de nível de serviço baseado na satisfação do usuário deve definir um percentual capaz de estimular a excelência na realização do treinamento pelo fornecedor.

A perda de horas de trabalho de usuário interno devido a treinamento insuficiente é outro indicador, identificado de duas formas. A primeira é a análise da produtividade dos usuários dos serviços afetados pela manutenção. A segunda é a realização de pesquisas de avaliação do treinamento dias (ou semanas) após a conclusão do treinamento e após a utilização das funcionalidades pelos mesmos usuários.

A meta a ser estabelecida neste caso deve ser baseada no período de tempo necessário para realizar as atividades antes de a manutenção ser implantada. A pesquisa de avaliação necessita explicitar a perda de produtividade devido à deficiência do treinamento.

O terceiro indicador proposto para o acordo operacional de treinamento de usuários, baseado no registro de dúvidas com relação às funcionalidades envolvidas no treinamento, demonstra a eficiência do treinamento.

A meta a ser atingida para este indicador deve ser estabelecida com base na complexidade da manutenção. Pequenas alterações em um número reduzido de funcionalidades permitem menor volume de registro de dúvidas comparativamente a alterações essenciais ou em maior número de funcionalidades.

No padrão IEEE, o treinamento de usuários encaixa-se na etapa de Treinamento, enquanto os demais acordos aqui propostos relacionam-se diretamente à etapa de Suporte. Ainda de acordo com o padrão, o mesmo

processo de engenharia é aplicado às diferentes etapas do ciclo de vida de sistemas. Assim, no sub-processo de controle, a atividade de medição do progresso e desempenho trata o treinamento de usuários ao abordar a necessidade de atendimento aos requisitos e de demonstração da maturidade e resultados progressivos.

	falhas ou insuficiência do treinamento
INS3	Volume de dúvidas
Meta a cumprir:	Registro de dúvidas com relação às funcionalidades envolvidas na manutenção inferior a <u>x</u> ocorrências durante <u>x</u> <i>meses (dias, horas etc)</i> após a implantação
Processo IEEE	
Controle	Medição do progresso e desempenho
Governança	
COBIT	Processo – ES7 Educar e treinar usuários
ITIL	Suporte de Serviços de TI – Gerenciamento da Problemas

7.9 Gerenciar versões

A manutenção da estabilidade e integridade dos ambientes de teste e produção visa reduzir os erros de implantação de versões, garantindo o controle sobre esses ambientes e possibilitando a realização de trilhas de auditoria. Desta forma, um acordo de nível de serviço baseado no gerenciamento de versões resulta no crescimento da produtividade da equipe envolvida.

Por outro lado, o gerenciamento de versões gera expectativas positivas junto ao cliente do serviço, com a divulgação antecipada de uma programação de liberação de versões.

Indicadores apropriados para avaliar o gerenciamento de versões apresentam o percentual de documentações, itens de *hardware* e *software* afetados pela manutenção identificados e com análise de impacto. Tal levantamento está diretamente relacionado com a redução de erros na implantação de manutenções de *software*.

Como meta, deve-se identificar e analisar o impacto de implantação da manutenção sobre todos os itens de hardware e software afetados. A percepção da ausência do levantamento completo do item de *hardware* ou *software* afetado pela manutenção ocorre no momento da implantação e ou com o início de operação do serviço associado.

Itens de documentação, com impacto menor sobre a disponibilidade de serviços permitem metas de nível de serviço relativamente mais flexíveis. A identificação de documentos não atualizados pode ocorrer no momento da implantação ou mesmo em manutenções futuras.

A ocorrência de cancelamentos de implantação de versões devido a incompatibilidade de versões de itens de hardware ou software também é um indicador de gerenciamento de versões. Uma implantação cancelada durante sua realização explicita a existência de falhas no processo de gerenciamento de versões. A quantidade de cancelamentos a ser estabelecida como nível de serviço aceitável deve ser baseada na criticidade do processo de negócio envolvido na manutenção.

A atividade de gerenciamento da configuração do processo de controle do padrão IEEE define, dentre outras ações, a necessidade de planejar e implementar o controle sobre os itens a serem alterados durante o processo de engenharia de sistemas.

Acordo Operacional		
Serviço de Manutenção de Software		
Descrição:	{ Descrição detalhada da manutenção }	
Envolvidos		
Cliente:	{ Área cliente do serviço }	
Fornecedor:	{ Fornecedor do serviço }	
Aplicabilidade		
<i>Tipo do Acordo:</i>	(X) Interno	(X) Externo
<i>Tipo da Manutenção:</i>	(X) Corretiva	(X) Perfectiva
	(X) Adaptativa	(X) Preventiva
Nível da Atividade		
Atividade:	Gerenciar versões	
Descrição:	Identificar itens de <i>hardware</i> , <i>software</i> e documentos afetados pela manutenção e avaliar o impacto. Elaborar plano de versão ou implementação e documentar procedimentos de cancelamento da implantação em caso de falha	
Objetivo:	Garantir a estabilidade e integridade dos ambientes Garantir a qualidade da manutenção	
Indicadores de Nível Operacional		
INS1	Percentual de itens de <i>hardware</i> afetados identificados	
Meta a cumprir:	Identificação e avaliação de impacto de <u>100%</u> dos itens de <i>hardware</i> efetivamente afetados pela manutenção	
INS2	Percentual de itens de <i>software</i> afetados identificados	
Meta a cumprir:	Identificação e avaliação de impacto de <u>100%</u> dos itens de	

<i>software</i> efetivamente afetados	
INS3	Percentual de documentos afetados identificados
Meta a cumprir:	Identificação e avaliação de impacto de <u>90%</u> dos documentos efetivamente afetados pela manutenção
INS4	Número de ocorrências de cancelamento da implantação devido a incompatibilidade de versões de itens de <i>hardware</i> ou <i>software</i>
Meta a cumprir:	Ocorrência inferior a <u>1</u> cancelamento da implantação devido a incompatibilidade de versões de itens de <i>hardware</i> ou <i>software</i>
Processo IEEE	
Controle	Gerenciamento de Configuração
Governança	
ITIL	Suporte de Serviços de TI – Gerenciamento de Mudanças Suporte de Serviços de TI – Gerenciamento de Versões

8. Conclusões

A utilização dos conceitos de governança em tecnologia da informação para estabelecimento de acordos operacionais para o controle do processo de manutenção de *software* é adequada. Inclusive em organizações onde a implantação de sua estrutura e processos não faça parte de seu planejamento.

A estrutura de relacionamentos e os processos componentes dos princípios de governança dão flexibilidade às organizações em situações de mudança. Permitem o direcionamento e controle de metas e objetivos estratégicos, adicionam valor e mantêm a continuidade de negócios, enquanto auxiliam no equilíbrio dos riscos em relação ao retorno de TI e seus processos.

A implementação de procedimentos de controle em processos de TI para alcance dos objetivos da organização compreende o estabelecimento de acordos de nível de serviço bem como de acordos operacionais para suportá-los.

Por outro lado, a importância da atividade de manutenção de *software* é inegável. A necessidade de adaptações devido a novos requisitos, mudanças no ambiente de negócio, novas oportunidades de mercado ou atualização tecnológica é cotidiana nas empresas.

A aplicação de um processo estruturado para a manutenção torna a atividade passível de controle. O processo de engenharia de sistemas do padrão 1220 do IEEE apresenta as atividades necessárias para realizar esse controle.

Assim, o retrato do processo de manutenção de *software* das organizações atuantes no mercado competitivo mundial emoldurado por acordos operacionais para controle do processo de manutenção segundo o padrão IEEE de engenharia de sistemas, orientados à governança proporciona um bela paisagem.

A relação de benefícios do modelo proposto nesta pesquisa permeia os próprios benefícios da governança e de acordos de nível de serviço.

A implementação de práticas de governança produzem:

- O alinhamento da estratégia de TI à estratégia do negócio;
- O aumento da capacidade e agilidade para novos modelos de negócios ou ajustes dos modelos atuais;
- Explicita a relação entre o aumento nos custos de TI e o aumento no valor da informação para o negócio da organização;
- Mantém os riscos do negócio sob controle;
- Externa a importância da TI na continuidade dos negócios;
- Mede e melhora continuamente o desempenho de TI.

No CobiT destacam-se como indicativos de alcance dos requisitos do negócio a disponibilidade, integridade da informação a eficiência financeira dos processos e sua confiabilidade, eficácia e adequação.

De forma complementar, as práticas propostas no ITIL buscam otimizar a utilização de recursos, reduzir os custos; aumentar a disponibilidade, ajustar a capacidade, aumentar o desempenho e melhorar a escalabilidade dos sistemas.

Por outro lado, a efetivação de práticas de governança requer atenção para fatores tais como:

- O conhecimento dos processos e não apenas da tecnologia;
- Indispensabilidade de uma visão de negócios e ampla disseminação das metas e objetivos da organização;
- Utilização de metodologias de controle e melhoria contínua da qualidade dos processos;
- Priorização da capacitação e retenção dos profissionais.

O outro componente da moldura, o estabelecimento de acordos operacionais para controle do processo de manutenção, provê a garantia de serviços realizados dentro de parâmetros pré-determinados. Este trabalho propõe a definição dos acordos e seus parâmetros baseada nas teorias de governança.

Assim, resgatando a hipótese apresentada no início deste trabalho, conclui-se pela adequação e viabilidade de um modelo para acordos operacionais para controle do processo de manutenção de *software* alinhado às teorias de governança de tecnologia da informação.

8.1 Recomendações para trabalhos futuros

O estudo realizado para propor um modelo de acordos operacionais para controle do processo de manutenção de *software* orientados a aspectos de governança de tecnologia da informação demonstra a sua aplicabilidade nas organizações. Assim, sugerem-se como trabalhos futuros complementares:

1. Desenvolvimento de um sistema computacional para manter dados reais de indicadores de níveis operacional e de serviço apurados em uma organização e prover relatórios gerenciais para a tomada de decisões, análise de tendências e realização de previsões;
2. Aplicação, acompanhamento e avaliação do modelo em organizações de diferentes tamanhos e naturezas;
3. Ampliação dos acordos e/ou dos indicadores propostos para a atividade de manutenção de *software*;
4. Proposição de um modelo de acordos operacionais para processos de outras naturezas, por exemplo em projetos de desenvolvimento de sistemas.

9. Referências Bibliográficas

- [ABR1993] ABRAN A.; Nguyenkim H. Measurement of the Maintenance Process from a Demand-based Perspective. Journal of Software Maintenance: Research and Practice, Vol 5 n. 2, 1993 p. 63-90.
- [APR2000] APRIL A. et all. Software Maintenance in Service Level Agreement: Controlling the Customers Expectations. FESMA-AEMES Software Measurement Conference 2000. Madri, 2000.
- [BBI2003] INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. Board Briefing on IT Governance, 2nd Edition. Illinois: IT Governance Institute, 2003.
- [BMC2004] BMC Software. Sarbanes-Oxley Section 404: How BMC IT Service Support Express Addresses General IT Control Requeriments. Disponível em <http://documents.bmc.com/products/documents/14/71/61471/61471.pdf>. Acesso em 20 Mar. 2006.
- [BOV2001] BOVESPA – Bolsa de Valores de São Paulo. Novo Mercado. Disponível em <http://www.bovespa.com.br> Acesso em 20 Mar. 2006.
- [BRI1994] BRIAND L. C. et all. A Change Analysis Process to Characterize Software Maintenance Projects. International Conference on Software Maintenance. Victoria, 1994.
- [BRO2004] BRODBECK H. J. Governança de TI. Disponível em <http://www.inf.ufrgs.br/~brodbeck/palestras/Governanca-TI.ppt> Acesso em 26 Dez. 2005.
- [CHA1997] CHARETTE R. N.; ADAMS K. M.; WHITE M. B. Managing Risk in Software Maintenance. Los Alamitos: IEEE Computer Society Press, 2003.
- [CMM2002] CMMI - CAPABILITY MATURITY MODEL INTEGRATION. Software Engineering Institute, v 1.1, Mar. 2002.
- [COB2005] ISACA – INFORMATION SISTEMS AUDIT AND CONTROL ASSOCIATION. Control Objectives for Information and related Technology (CobiT). Illinois: Information Systems Audit and Control Association, 2005.

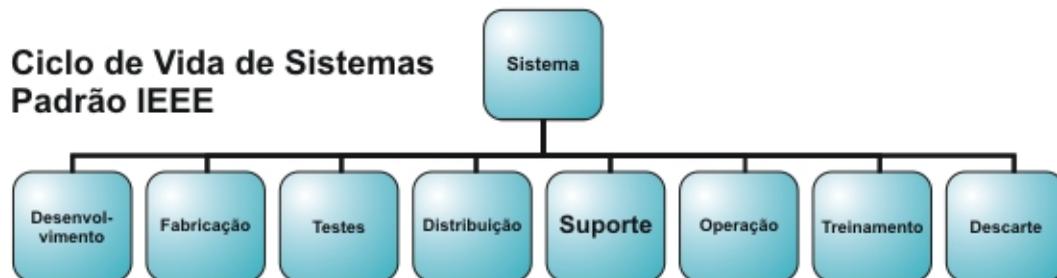
- [DAV1994]** DAVENPORT T. Saving IT's soul: Human-centered information management. Boston: Harvard Business Review, 1994.
- [DIN2003]** DINSMORE C. P. Como se tornar um profissional em gerenciamento de projetos. 1ª. Edição. Rio de Janeiro: Qualitymark, 2003.
- [EXA2006]** Os ganhos com a Sarbanes-Oxley – Revista Exame, Fev. 2006.
- [FIG2006]** FIGUEIREDO Fo. A. C. Governança Corporativa e de TI – Revista Banco Hoje, Jan. 2006.
- [GHE2005]** GHERMAN M. Controles Internos – Buscando a solução adequada – Parte II Disponível em http://www.modulo.com.br/checkuptool/artigo_06.htm. Acesso em 26 Dez. 2005.
- [GHN2005]** GHERMAN M. Controles Internos – Buscando a solução adequada – Parte V. Disponível em http://www.modulo.com.br/checkuptool/artigo_10.htm. Acesso em 26 Dez. 2005.
- [GRU2003]** GRUBB P.; TAKANG A. A. Software Maintenance: Concepts and Practice. Danvers: World Scientific, 2003.
- [HAN1993]** HANNA M. Maintenance Burden Begging for Remedy. Software Magazine, Abr.1993 p. 53-63.
- [HIL1999]** HILBURN T. B. et all. A Software Engineering Body of Knowledge. Software Engineering Institute, v 1.0, Abr. 1999.
- [ISO1999]** ISO/IEC 14764 Software Engineering - Software Maintenance. Genebra: Internationa Organization for Standardization, 1999.
- [IEE1998]** IEEE – INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. Standard for Application and Management of the Systems Engineering Process (Std 1220-1998). Nova York, 1998.
- [INF2006]** Gestão de Riscos: só o pessimista salva – Revista Informática Hoje, Jan. 2006.

- [ITC2004]** INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. IT Control Objectives for Sarbanes-Oxley. Illinois: IT Governance Institute, 2004.
- [ITI2001]** OGC – BRITISH OFFICE OF GOVERNMENT COMMERCE. Information Technology Infrastructure Library (ITIL). London: Office of Government Commerce, 2001.
- [KAP1992]** KAPLAN R. S.; NORTON D. P. The Balanced Score Card – Measures that Drive Performance. Boston: Harvard Business Review, 1992.
- [KAP1997]** KAPLAN R. S.; NORTON D. P. A Estratégia em Ação: Balance Scorecard. Rio de Janeiro: Campus, 1997.
- [LAK2003]** LAKATOS E. M.; MARCONI M. A. Fundamentos de Metodologia Científica. São Paulo: Atlas, 2003.
- [NBR2001]** NBR ISO/IEC 17799 Tecnologia da Informação – Código de prática para gestão da segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2001.
- [OEC2004]** ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. OECD Principles of Corporate Governance. Paris: Organization for Economic Co-operation and Development, 2004.
- [OSS2005]** OSSAMU C. ITIL é a solução para gerir TI? – Revista Info Corporate, Mai. 2006.
- [PAU1995]** PAULK M. C. The Capability Maturity Model: guidelines for improving the software process. Boston: Addison Wesley, 1995.
- [PFL2001]** PFLEEGER S. L. Software Engineering: Theory and Practice. 2nd Edition. New-Jersey: Prentice Hall, 2001.
- [PIG1997]** PIGOSKI T. M. Practical Software Maintenance: Best Practices for Software Investment. Nova York: Wiley Computer Publishing, 1997.
- [PMI2004]** PMI - PROJECT MANAGEMENT INSTITUTE. A Guide to the Project Management Body of Knowledge 3rd Edition (PMBok). Maryland: Project Management Institute Inc., 2004.

- [PRE2000]** PRESSMAN R. S. Software Engineering: a practitioner's approach. Nova York: MacGrawHill, 2000.
- [RUP2001]** RUP – RATIONAL UNIFIED PROCESS. Rational Software Corporation, v 2001.03.00, 2001.
- [SAL2003]** SALLÉ M.; BARTOLINI C. Management by Contract. Disponível em <http://www.hpl.hp.com/techreports/2003/HPL-2003-186R1.pdf> Acesso em 26 Dez. 2005.
- [SOX2002]** H.R. 3763, The Sarbanes-Oxley Act of 2002, 10º. Congresso dos Estados Unidos da América. Washington DC, 23 de janeiro de 2002.
- [SNE2003]** SNEED H. M. Critical Success Factors in Software Maintenance. International Conference on Software Maintenance. Amsterdã, 2003.
- [STI2005]** STIMSON A. W. Sarbanes-Oxley e ISO 9000 – Revista Quality Progress, Mar. 2005 p. 24-29.
- [WEB2005]** WEBSTER K. P. B. Riscos para manutenção de software: taxonomia e priorização. Dissertação (Mestrado) – Universidade Católica de Brasília, 2005.

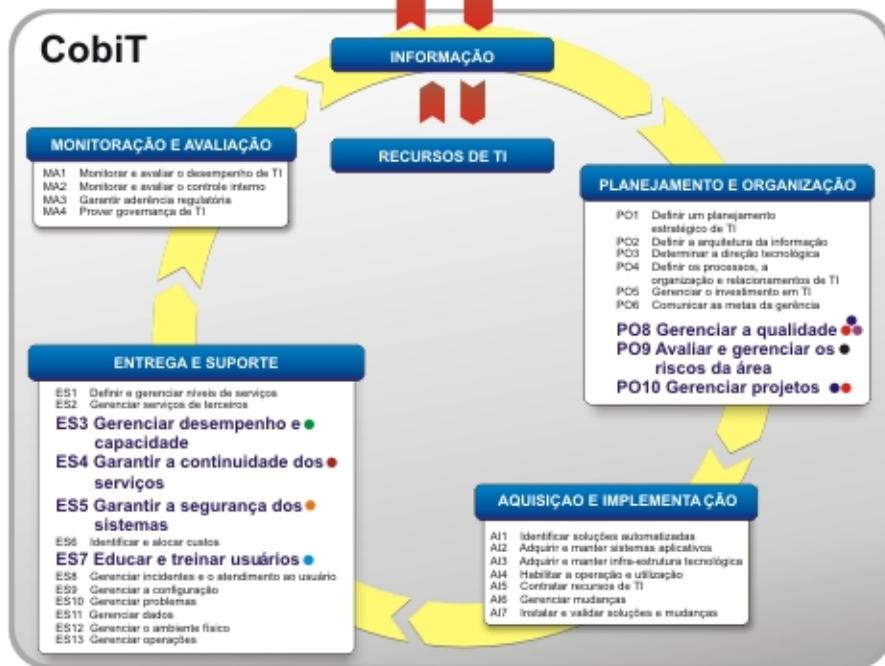
APÊNDICE

Ciclo de Vida de Sistemas Padrão IEEE



OBJETIVOS DO NEGÓCIO Os processos e controles de governança de TI associados a cada nível de serviço são destacados com as cores marcadoras de cada acordo

OBJETIVOS DE GOVERNANÇA



Lei Sarbanes - Oxley

Conteúdo	Título do Assunto
Título I	Comitê de Supervisão da Contabilidade da Companhia Pública
Título II	Independência do auditor
Título III	Responsabilidade corporativa
Título IV	Aumento de demonstrações financeiras
Título V	Conflitos de interesse do analista
Título VI	Recursos e autoridade da comissão
Título VII	Estudos e relatórios
Título VIII	Prestação de contas corporativas e fraude criminosas
Título IX	Aprimoramento das penalidades contra os crimes de colarinho branco
Título X	Retorno de impostos corporativos
Título XI	Fraude corporativa e prestação de contas



Planejamento de Gerenciamento de Serviços



Livros Grátis

(<http://www.livrosgratis.com.br>)

Milhares de Livros para Download:

[Baixar livros de Administração](#)

[Baixar livros de Agronomia](#)

[Baixar livros de Arquitetura](#)

[Baixar livros de Artes](#)

[Baixar livros de Astronomia](#)

[Baixar livros de Biologia Geral](#)

[Baixar livros de Ciência da Computação](#)

[Baixar livros de Ciência da Informação](#)

[Baixar livros de Ciência Política](#)

[Baixar livros de Ciências da Saúde](#)

[Baixar livros de Comunicação](#)

[Baixar livros do Conselho Nacional de Educação - CNE](#)

[Baixar livros de Defesa civil](#)

[Baixar livros de Direito](#)

[Baixar livros de Direitos humanos](#)

[Baixar livros de Economia](#)

[Baixar livros de Economia Doméstica](#)

[Baixar livros de Educação](#)

[Baixar livros de Educação - Trânsito](#)

[Baixar livros de Educação Física](#)

[Baixar livros de Engenharia Aeroespacial](#)

[Baixar livros de Farmácia](#)

[Baixar livros de Filosofia](#)

[Baixar livros de Física](#)

[Baixar livros de Geociências](#)

[Baixar livros de Geografia](#)

[Baixar livros de História](#)

[Baixar livros de Línguas](#)

[Baixar livros de Literatura](#)
[Baixar livros de Literatura de Cordel](#)
[Baixar livros de Literatura Infantil](#)
[Baixar livros de Matemática](#)
[Baixar livros de Medicina](#)
[Baixar livros de Medicina Veterinária](#)
[Baixar livros de Meio Ambiente](#)
[Baixar livros de Meteorologia](#)
[Baixar Monografias e TCC](#)
[Baixar livros Multidisciplinar](#)
[Baixar livros de Música](#)
[Baixar livros de Psicologia](#)
[Baixar livros de Química](#)
[Baixar livros de Saúde Coletiva](#)
[Baixar livros de Serviço Social](#)
[Baixar livros de Sociologia](#)
[Baixar livros de Teologia](#)
[Baixar livros de Trabalho](#)
[Baixar livros de Turismo](#)