Área Temática: GESTÃO TECNOLÓGICA

Título do Trabalho: GERENCIAMENTO DE RISCOS DE TI: AVALIAÇÃO DA ESTRUTURA DE CONTROLES BASEADA NO COBIT®

AUTORES

RENATO PEREIRA DE ALMEIDA

Universidade de São Paulo

rpaeach@gmail.com

EDMIR PARADA VASQUES PRADO

Universidade de São Paulo

eprado@usp.br

RESUMO

Com a crescente evolução da tecnologia de informação e o aumento da competição global, as organizações tornaram-se dependentes dos recursos de tecnologia de informação. Como conseqüência, torna-se imperativo o gerenciamento de riscos inerentes às atividades de tecnologia de informação. Por outro lado, existe uma enorme gama de produtos e metodologias especializados na análise e mitigação de riscos. Em função disso, as empresas encontram dificuldades em escolher qual deve ser sua abordagem para o tema. Considerando essa dificuldade, o presente trabalho visa analisar os controles para a gestão de riscos relacionados à tecnologia de informação. Por meio de um estudo de múltiplos casos, este artigo busca analisar casos de implementação de controles para garantir a integridade da tecnologia de informação na organização. Os dados foram coletados por entrevistas e documentos e sua análise seguiu uma abordagem baseada nos estudos de gestão organizacional. Como resultado, foram identificados doze controles principais, que abrangem os quatro domínios do COBIT® e endereçam dezenove de seus objetivos de controle. Esse controles permite às organizações priorizar os esforços de gerenciamento de riscos associados à tecnologia de informação.

Palavras chave: COBIT®; Tecnologia de Informação; Governança.

ABSTRACT

Organizations have become dependent on IT resources due to increasing development of information technology (IT) and increased global competition. As a result, it becomes imperative to manage risks inherent to IT activities. Moreover, there is a huge range of products and methodologies for risk analysis and mitigation. For this reason, companies have difficulty in choosing what should be their approach to this issue. Considering this difficulty, this paper aims to examine the controls needed to manage IT risks. Through a study of multiple cases, this paper analyzes cases of implementation of controls to ensure the integrity of IT in the organization. Data were collected through interviews and documents and analysis followed an approach based on organizational studies. As a result, we identified 12 key controls that cover the four domains of COBIT and address 19 of their objectives of control.

Key words: COBIT®; Information Technology; Governance.

1 INTRODUÇÃO

Atualmente, diversas empresas, independentemente de seu porte ou mercado de atuação, utilizam recursos de tecnologia da informação (TI) para dar suporte às suas atividades fim. Com a crescente evolução da TI e o aumento da competição global, atualmente disputada em tempo real, as organizações tornaram-se dependentes dos recursos de TI para o gerenciamento e expansão de seus negócios. Segundo Menezes (2005), o atendimento ao cliente, as operações e as estratégias de produto, marketing e distribuição dependem muito, e às vezes totalmente, da disponibilidade de sistemas computacionais.

Nesse cenário, torna-se imperativo o gerenciamento de riscos inerentes às atividades de TI, envolvendo, principalmente, aspectos de segurança da informação, garantia de continuidade das operações e disponibilidade e qualidade dos serviços. Questões relacionadas ao acesso a dados críticos e vulnerabilidades na infra-estrutura física, entre outras, podem interferir diretamente na continuidade dos negócios da empresa, dependendo da intensidade da materialização da falha.

Atualmente, existe uma enorme gama de produtos, metodologias e consultorias especializadas na análise e mitigação de riscos. Em função disso, as empresas freqüentemente encontram dificuldades em escolher qual deve ser sua abordagem para o tema. Considerando essa dificuldade para o controle e monitoramento de tais riscos, o presente trabalho visa analisar os controles para a gestão de riscos relacionados a TI. Dentro desse contexto, este trabalho tem como objetivo analisar casos de implementação de controles para garantir a integridade da TI. Para a consecução desse objetivo, foram estabelecidos dois objetivos específicos: (1) identificar os principais riscos e respectivos controles utilizados pelas organizações; e (2) associar os controles utilizados pelas organizações aos objetivos de controle do COBIT®.

2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica para este trabalho foi construída a partir de uma revisão bibliográfica sobre o *framework* COBIT®. Essa revisão procurou contemplar análises e considerações de diferentes autores e está apresentada em três tópicos: o papel da TI no planejamento estratégico das organizações; modelos utilizados na governança de TI; e o *framework* COBIT®.

2.1 O papel da TI no planejamento estratégico das organizações

O planejamento estratégico envolve a tomada de decisões sobre estratégias e objetivos de longo prazo, e possui uma orientação externa forte, envolvendo as principais partes da organização (BATEMAN; SNELL, 2002). Trata-se de uma técnica administrativa ou de um processo gerencial para ordenar as idéias, as ações e os esforços da empresa para atingir a sua meta ou seu objetivo (TSAI, 2006). Robbins (2000) destaca que o planejamento dá direção, reduz o impacto da mudança, minimiza o desperdício e a redundância, e fixa os padrões para facilitar o controle. Isto porque, o planejamento compreende a definição das metas de uma organização, o estabelecimento de uma estratégia global para alcançar estas metas e o desenvolvimento de uma hierarquia de planos abrangente para integrar e coordenar atividades.

Dentro do planejamento estratégico, a TI se encaixa como um instrumento eficaz no auxílio à tomada de decisão, opondo-se a visão de que a tecnologia facilita apenas a automatização de processos. Neste sentido, o correto planejamento e administração dos recursos de TI são fundamentais para o sucesso de uma organização no atual ambiente econômico. De acordo com Albertin (2002), o planejamento, por si só, já pode ser considerado um fator crítico de sucesso para a administração da TI, devido a sua relevância, a sua condição

de base para as demais funções e às características e evoluções do ambiente tecnológico e de negócios.

Porter e Millar (1985) afirmam que a forma como as companhias operam está mudando. Tal fato está afetando a criação de produtos nas empresas, auxiliando na criação de valor, e fazendo com que as organizações sejam divididas em atividades distintas, econômica e tecnologicamente atuantes. Ainda segundo esses autores, nossa economia está passando por uma revolução da informação, e nenhuma organização pode ficar alheia a isso. Reduções dramáticas de custos para obter, processar e transmitir informação estão mudando a forma com que os negócios são realizados.

A TI é vista atualmente como uma das maiores e mais poderosas influências no planejamento das organizações. Ela permite melhorar a qualidade de vários aspectos relacionados ao negócio e tem auxiliado na habilidade de manipular um grande volume de transações num custo unitário médio decrescente, de apoiar operações geograficamente dispersas por intermédio do processamento distribuído e de oferecer novos produtos e canais de distribuição (ALBERTIN, 2001).

Segundo Menezes (2005), a valorização das ações no mercado é influenciada positivamente pelo grau de segurança oferecido pelos direitos concedidos aos acionistas e pela quantidade de informações disponibilizadas pelas organizações. Por este motivo, uma boa administração dos recursos de TI pode permitir à organização uma maior valorização de um de seus ativos mais importantes, sua marca.

A partir dos escândalos corporativos ocorridos nos Estados Unidos, mais especificamente a quebra de empresas como a Enron e a Wordcom, foi criado um conjunto de normas mais rígidas para as empresa de capital aberto. Essas normas ficaram conhecidas como lei Sarbanes & Oxley (SOx). A promulgação da SOx culminou com a criação do PCAOB (*Public Accounting Oversight Board*), órgão responsável pela publicação e atualização das normas definidas pela lei, bem como pela fiscalização das firmas de auditoria independentes que certificam empresas com ações na bolsa de NY. Em seus padrões de auditoria (*Audit Standards*), o PCAOB indica que a área de TI deve fazer parte do esforço contínuo pela transparência e garantias de atendimento (*compliance*) às normas contábeis (PCAOB, 2009). Mais ainda, o PCAOB indica como guia de melhores práticas para a estrutura de controles internos das empresas os *frameworks* COSO e o COBIT®, este último voltado exclusivamente ao ambiente de TI das organizações. Como conseqüência, a TI deve ser considera uma peça chave no planejamento estratégico das empresas, sendo considerada em todos os seus aspectos relevantes – planejamento, monitoramento e controle – para que os objetivos definidos no planejamento sejam plenamente alcançados, com eficiência, eficácia e segurança.

2.2 Modelos utilizados na Governança de TI

Nesta seção será apresentado três das principais metodologias que são comumente utilizadas como aliadas na implementação do *framework* COBIT®. São elas: ITIL, CMMI e PMBOK.

2.2.1 *Information Technology Infrastructure Library* (ITIL)

O *framework* ITIL foi desenvolvido nos anos 80 por um órgão vinculado ao governo britânico (OGC – *Office of Government Commerce*). Sua criação se deu pela necessidade do governo britânico gerenciar seu conjunto de TI que ficava cada vez mais complexo. O ITIL surge como um guia de melhores práticas no Gerenciamento de Serviços de TI. Sua abordagem é basicamente focada na qualidade, eficiência e eficácia de processos (ITGI, 2007). São três as principais áreas de utilização do ITIL, conforme apresenta a Figura1: suporte de

serviço; entrega de serviço e gerenciamento de segurança.

Seu modelo é composto por uma série de documentos públicos, cuja finalidade é apoiar a implementação de uma estrutura adequada à gestão de serviços de TI, definindo o escopo de atuação desta estrutura, bem como os seus serviços.

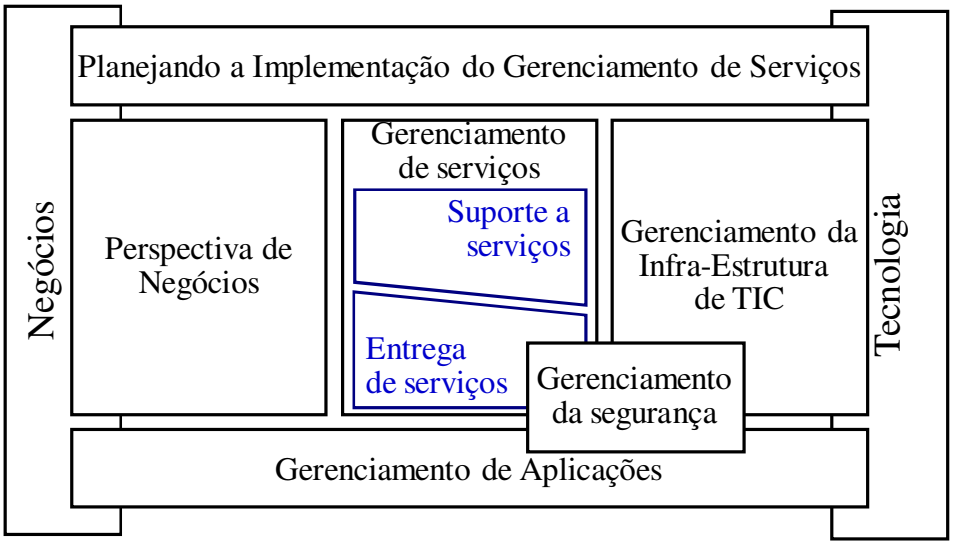

Figura 1 – Categoria de Processos CMMI.
Fonte: Adaptado de Fernandes e Abreu (2006).

2.2.2 *Capability Maturity Model Integration* (CMMI)

O CMMI é um conjunto de modelos que fornece às empresas um guia para organizar seus processos de desenvolvimento e manutenção de software, bem como para evoluir em

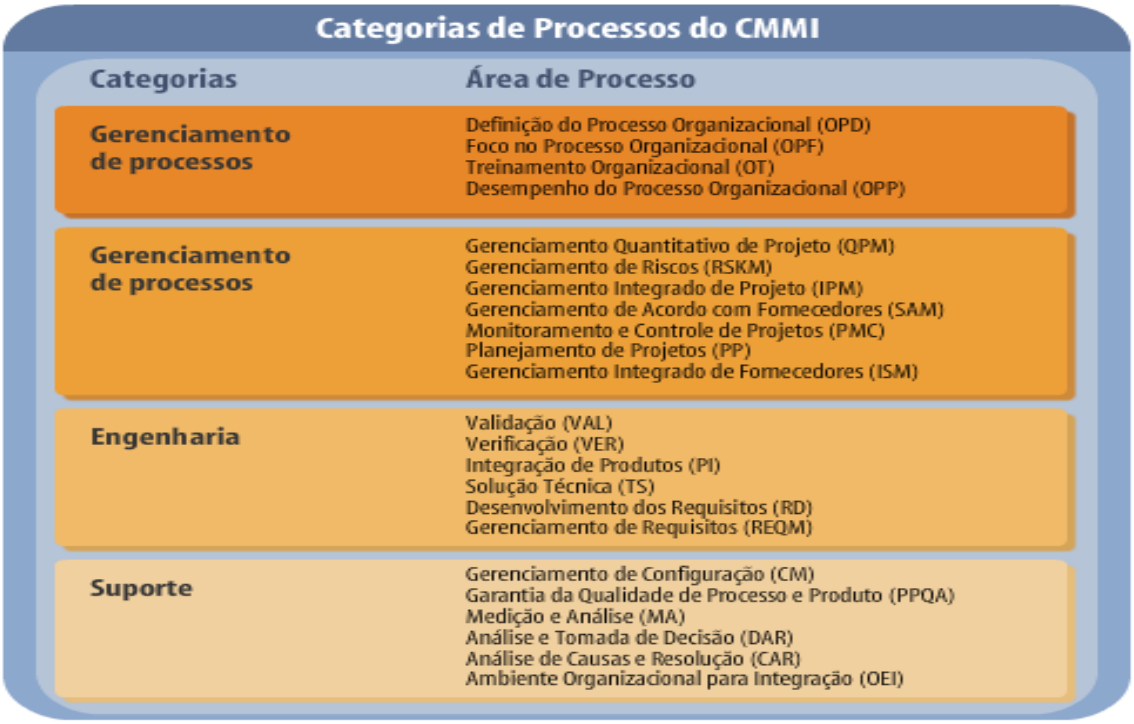

Figura 2 – Categoria de Processos CMMI.
Fonte: Adaptado de SEI (2007).

direção a uma excelência em cultura de engenharia de software (SEI, 2007). Esse *framework*,

desenvolvido pela SEI (*Software Enginnering Institute*) e pela Universidade *Carnegie Mellon,* provê um guia para melhoria dos processos de uma organização e sua habilidade de gerenciar o desenvolvimento, aquisição e manutenção de produtos ou serviços. Ele objetiva a avaliação e a melhoria da capacitação de uma organização, ajudando a garantir processos maduros, estáveis e capazes. O CMMI está estruturado em 5 níveis de maturidade, abrangendo 25 áreas de processo, divididas em 4 categorias: gerenciamento de projetos, gerenciamento de processos, engenharia e suporte. A Figura 2 ilustra as categorias de processos do CMMI.

2.2.3 *Project Management Body of Knowledge* (PMBOK)

O PMBOK é um guia que contempla boas práticas reconhecidas internacionalmente no gerenciamento de projetos. Este guia foi desenvolvido pelo PMI (*Project Management Institute*) e encontra-se atualmente em sua terceira versão (PMI, 2009). De acordo com o PMI, projeto é um conjunto não repetitivo de atividades inter-relacionadas que, mediante a combinação temporária de recursos, têm por finalidade alcançar um objetivo pré-determinado num prazo definido e com recursos limitados.

O PMBOK inclui melhores práticas comprovadas no gerenciamento de projetos, bem como práticas inovadoras desenvolvidas para a profissão, além de fornecer uma linguagem comum para os profissionais da gestão de projetos. O Guia PMBOK está organizado em 44 processos de gerenciamento de projetos, divididos em nove áreas do conhecimento, conforme ilustrado na Figura 3.

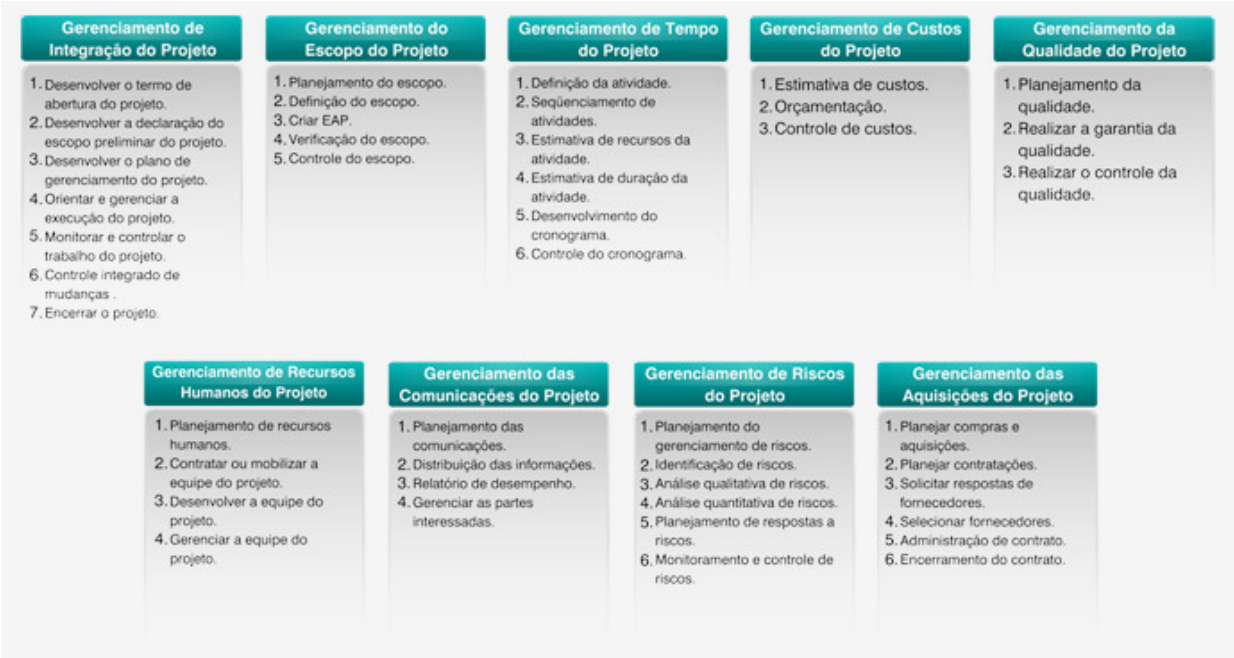

Figura 3 – Áreas do conhecimento do PMBOK.
Fonte: Adaptado de PMI (2004).

2.3 O *Framework* COBIT®

Este tópico tem por objetivo expor os principais aspectos relacionados ao *framework* COBIT®. O COBIT é uma estrutura de gerenciamento que se dedica ao ciclo de vida completo do investimento de TI. A estrutura suporta as realizações de TI e as metas corporativas, garantindo o alinhamento de TI com os objetivos organizacionais e melhorando a eficiência e a produtividade de TI (ITGI, 2007).

2.3.1 Visão Geral

O modelo COBIT® foi desenvolvido pela ISACA (*Information Systems Audit and Control Association*) em 1996. A ISACA é uma entidade privada e voluntária, reconhecida como líder mundial em governança em TI, e com foco em controles, voltados principalmente para questões de segurança da informação e auditoria de processos.

Desenvolvido para ser o modelo para governança de TI no mercado, o COBIT® passou a ser difundido mundialmente, principalmente a partir dos padrões editados pelo PCAOB. Como conseqüência, o COBIT® passou ser o modelo de governança escolhido como ideal para estabelecer controles internos relativos à área de TI das organizações, devido principalmente à sua grande relevância e ao direcionamento nas questões de auditoria e segurança.

Segundo Silva (2007), as organizações têm cada vez mais acesso aos mesmos recursos tecnológicos. Porém, é na maneira como as aplicações de TI estão alinhadas aos negócios que se podem obter vantagens estratégicas. O *framework* COBIT® contribui para o alinhamento da TI necessário para alcançar um diferencial competitivo, e está focado fortemente no alto nível das organizações, inserindo uma cultura de governança de TI, alinhada com os objetivos de negócio da corporação.

2.3.2 Motivação para a Adoção

Atualmente, devido à grande velocidade com que a TI se desenvolve, bem como a grande dificuldade enfrentada pelas corporações para controlar os riscos presentes em sua estrutura de TI, faz-se necessária adoção de uma estrutura de governança de TI, alinhada ao modelo de governança corporativa e aos objetivos de negócio da empresa. Conforme Corrêa (2006), existem várias mudanças em TI que mostram a necessidade de um melhor gerenciamento dos riscos envoolvidos. Segundo o ITGI (2007), para muitas organizações a informação e a tecnologia que a suportam, representa seu mais valioso ativo, porém o menos freqüentemente entendido. Organizações de sucesso reconhecem os benefícios da TI e a usam para dirigir os valores de seu *stakeholders*.

Existem algumas vantagens na adoção de um modelo de governança de TI. No caso específico do *framework* COBIT®, pode-se destacar algumas vantagens que motivam a sua adoção: definição das responsabilidades na área de TI; especificação dos riscos e controles atrelados aos objetivos organizacionais; modelo de boas práticas conhecido, claro e comumente aceito; e a facilidade para a auto-avaliação, medição de metas de desempenho e *benchmarking* da organização de TI.

2.3.3 Estrutura

O *framework* COBIT® é formado por quatro domínios: planejamento e organização; aquisição e implementação; entrega e suporte; e monitoramento e controle. Ele abrange 34 processos de domínio, subdivididos em 210 objetivos de controle (ITGI, 2007). A Figura 4 expõe o inter-relacionamento entre os objetivos de negócio, a Governança e TI e a estrutura do COBIT®.

- **Planejamento e Organização.** Abrange estratégias e táticas, e diz respeito à identificação de como TI pode melhor contribuir para a realização dos objetivos de negócio. É de suma importância que neste ponto sejam alinhadas as estratégias de TI com as estratégias de negócio da corporação, pois as demais fases de implantação do modelo de governança de TI dependem fundamentalmente da boa execução desta fase inicial de planejamento. Os processos deste domínio são: PO01 - definição do plano estratégico de TI; PO02 - definição da arquitetura de informação; PO03 - determinação da direção tecnológica; PO04 - definição dos relacionamentos, organização e processos

de TI; PO05 - gerenciamento do investimento de TI; PO06 - comunicação da direção e objetivos gerenciais; PO07 - gerenciamento dos recursos humanos; PO08 - gerenciamento da qualidade; PO09 - avaliação e gerenciamento de riscos de TI; e PO10 - gerenciamento de projetos.

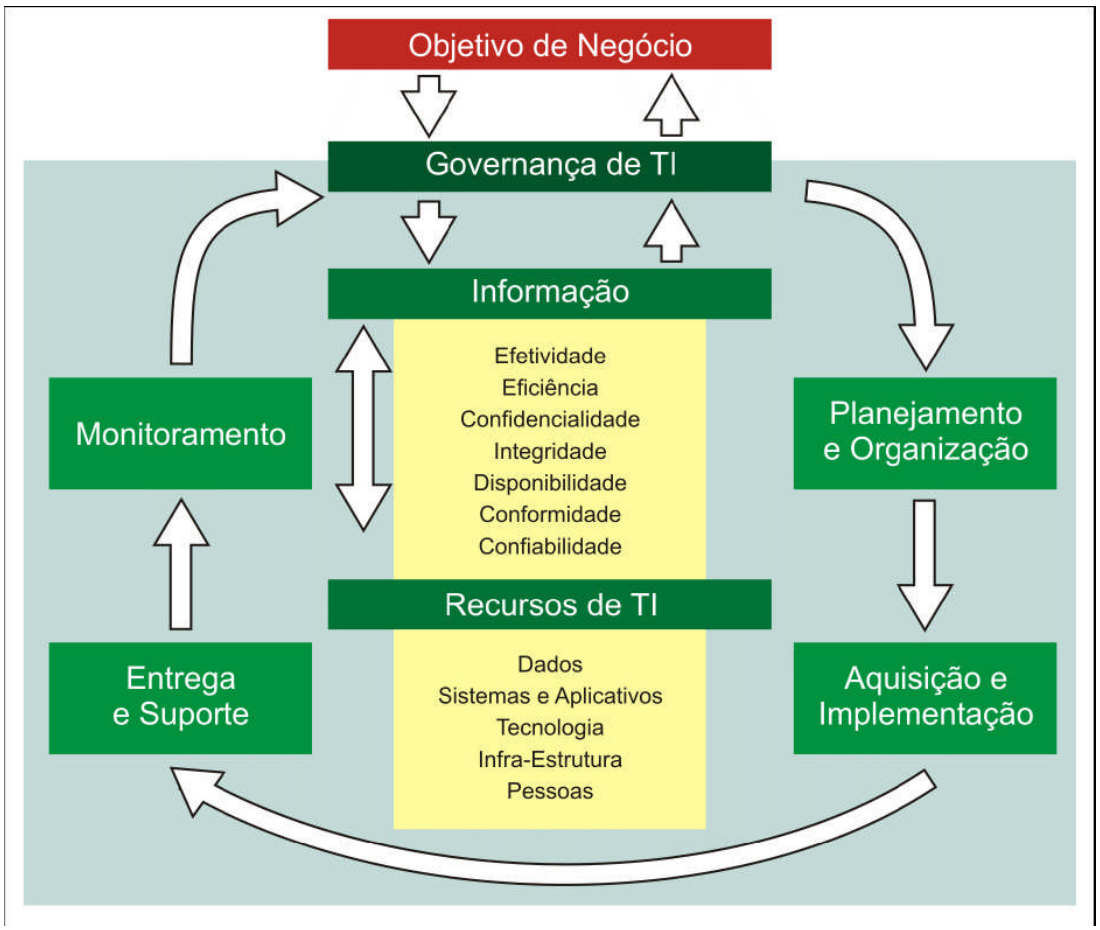

Figura 4 – Visão geral do *framework* COBIT®.
Fonte: Adaptado de Menezes (2005).

- **Aquisição e Implementação.** Para atingir a estratégia de TI, a equipe de suporte deve identificar, adquirir, implementar e integrar as estratégias de TI aos processos de negócio. Adicionalmente, mudanças e manutenções nos sistemas existentes devem continuar alinhadas as estratégias de negócio da empresa. Este domínio possui sete processos: AI01 - identificação de soluções automatizadas; AI02 - aquisição e manutenção do software aplicativo; AI03 - aquisição e manutenção da infra-estrutura tecnológica; AI04 - habilitação da operação e utilização; AI05 - aquisição dos recursos de TI; AI06 - gerenciamento de mudanças; e AI07 - instalação e aprovação de soluções e mudanças.
- **Entrega e suporte.** Este domínio diz respeito às requisições e às entregas de serviço, ao gerenciamento da segurança e continuidade das operações, e ao serviço de suporte aos usuários. Os processos ligados a este domínio são: DS01 - definição e gerenciamento de níveis de serviço; DS02 - gerenciamento de serviços de terceiros; DS03 - gerenciamento de performance e capacidade; DS04 - garantir serviço contínuo; DS05 - garantir a segurança dos sistemas; DS06 - identificação e atribuição de custos; DS07 - educação e treinamento de usuários; DS08 - gerenciamento de incidentes e

service desk; DS09 - gerenciamento de configuração; DS10 - gerenciamento de problemas; DS11 - gerenciamento de dados; DS12 - gerenciamento do ambiente físico; DS13 - gerenciamento das operações.

- **Monitoramento e Controle.** Com exceção do domínio Planejamento e Organização, talvez este seja o tópico mais importante do *framework* COBIT®. Este ponto trata do monitoramento e avaliação da estrutura de TI, sendo validada através de testes dos controles internos mapeados, realizando a adequação aos pontos regulatórios, tais como leis ou acordos de boas práticas, além de prover a governança, ou seja, o controle e gerenciamento dos produtos de TI. Este domínio é composto de quatro processos: M01 - monitorar e avaliar o desempenho de TI; M02 - monitorar e avaliar os controles internos; M03 - garantir atendimento a questões regulatórias; e M04 - prover a governança de TI.

2.3.4 Graus de Maturidade

Para que sejam criadas estruturas de controles internos adequadas aos objetivos de negócio das organizações, faz-se necessária a realização de uma análise do nível de maturidade no gerenciamento dos riscos e governança de TI atual e desejado, levando-se sempre em consideração os objetivos de negócio da organização. Segundo o ITGI (2007), o grau de maturidade da área de TI de uma organização, pode ser classificado em cinco níveis:

- **Não Existente (nível 0)**. Não há processo de governança em TI e a organização não reconhece sua importância e não tem interesse em implementá-lo.
- **Inicial ou *Ad-Hoc* (nível 1)**. Existem processos ocorrendo, contudo não estão formalizados, e as ações são tomadas conforme a necessidade.
- **Repetitiva (nível 2)**. Os processos de governança de TI estão em desenvolvimento e já existe uma preocupação neste sentido em alguns setores da organização. Todavia, as ações são centralizadas em algumas pessoas e as medidas de desempenho não são completamente utilizadas.
- **Processo Definido (nível 3)**. A alta gerência já reconhece a importância da governança e existem indicadores confiáveis de desempenho que conectam os processos aos objetivos de negócio da empresa.
- **Gerenciado e Medido (nível 4)**. Todas as áreas da organização estão empenhadas no processo de governança e os processos são informados por meio de treinamento formal. Métricas são estabelecidas e medidas por acordos de níveis de serviço (SLA). Porém, o uso de tecnologia no nível tático ainda é limitado.
- **Otimizado e Automático (nível 5)**. Há total conhecimento da governança em todos os níveis, e a melhoria de processos é feita através de *benchmarking*. O levantamento de riscos é constante e informado a toda a organização.

No COBIT® a ferramenta de análise de maturidade auxilia os gestores de TI a identificar como estão posicionados os macro controles de TI em relação aos padrões esperados de mercado e às suas próprias expectativas e objetivos. O COBIT®, por focar principalmente na estrutura de governança de TI, comumente necessita ser implementado em conjunto com outra metodologia, sendo normalmente combinado com os *frameworks* ITIL, CMMI e PMBOK.

3 METODOLOGIA DA PESQUISA

Este trabalho se caracteriza como um estudo qualitativo e de caráter exploratório. Segundo Richardson (1999), a pesquisa qualitativa é adequada para descrever a complexidade

de uma determinada situação e compreender seus processos dinâmicos. Como conseqüência, esse tipo de pesquisa é adequada a este trabalho, pois se busca identificar os principais riscos aplicados à área de TI e descrever os principais controles utilizados pelas organizações brasileiras para reduzir esses riscos.

Segundo Gil (2002), não há consenso por parte dos pesquisadores quanto às etapas a serem seguidas no desenvolvimento de um estudo de caso. Em função disso, utilizou-se a seguinte seqüência para elaboração desta pesquisa: definição do problema de pesquisa; estratégia da pesquisa; definição do escopo e das unidades de análise; coleta e análise dos dados.

3.1 Problema de Pesquisa

O problema básico de pesquisa deste trabalho é analisar casos de implementação de controles para garantir a integridade da TI. Para atingir esse objetivo procurou-se responder às seguintes perguntas:

- Quais os principais controles utilizados pelas organizações brasileiras de médio e grande porte?
- Quais as associações existentes entre os controles utilizados pelas organizações e os objetivos de controle do COBIT®?

Ao responder a essas perguntas, deseja-se melhorar o entendimento sobre os riscos relacionados a TI, contribuindo para que: as áreas de TI possam focar seus esforços nos riscos mais relevantes para as organizações; e os provedores de serviço de TI possam aprimorar suas metodologias, de modo a contemplar um conjunto mínimo de controles que enderecem os riscos mais relevantes.

3.2 Estratégia da Pesquisa

O estudo de caso é um método de pesquisa empírica que investiga fenômenos contemporâneos em seu contexto real, quando os limites entre o fenômeno e o contexto não estão claramente definidos e quando existem mais variáveis de interesse do que pontos de dados (YIN, 2005). Em um estudo de caso uma unidade de análise corresponde a um caso. Pode ser um evento, uma entidade, um indivíduo, ou até mesmo um processo de implantação em uma organização. Neste trabalho, a unidade de análise é o processo de controle de riscos relacionados a TI, implementado nas organizações.

A estratégia de pesquisa adotada neste trabalho foi o estudo de múltiplos casos. Segundo Yin (2005), o estudo de múltiplos casos aumenta a confiança nas evidências em relação ao estudo de um único caso, pois permite a comparação das diferenças e similaridades entre eles.

3.3 Definição do Escopo e das Unidades de Análise

O escopo desta pesquisa abrange organizações do setor privado com negócios e operações no mercado brasileiro e de médio e grande porte. Isto porque, nas empresas de médio e grande porte a avaliação de risco possui uma relevância maior e é conduzida por processos mais formais.

Os estudos de caso foram conduzidos em oito organizações, clientes de uma grande consultoria com operações internacionais e de renomada atuação na área de auditoria de sistemas da informação, avaliação de estrutura de governança e de controles internos das áreas de TI. As organizações foram selecionadas em função de possuírem as melhores estruturas de controles internos, avaliadas pela consultoria no período de 2006 e 2008. Um resumo das

características de cada uma das oito organizações selecionadas pode ser visto no Quadro 1.

Quadro 1 – Características das organizações estudadas.

Setor de atuação	Ramo de atuação	Porte das organizações
Industrial	Cosméticos	Grande
	Siderúrgica	Grande
	Química	Médio
	Autopeças	Médio
Serviços	Energia elétrica	Grande
	Informações financeiras	Médio
Comércio	Móveis	Grande
	Rede de drogarias	Médio

Fonte: próprio autor.

3.4 Coleta e Análise de Dados

O instrumento de coleta de dados utilizado foi a entrevista. Elaborou-se inicialmente um roteiro de perguntas, que foi aplicado pessoalmente a cada um dos entrevistados. As entrevistas foram conduzidas no primeiro semestre de 2009 com os gestores de projetos em cada uma das oito organizações selecionadas. O roteiro foi constituído de várias perguntas em torno de três tópicos básicos: as premissas utilizadas na definição dos riscos relevantes da área de TI; o alinhamento entre a área de TI e as áreas de negócio para a manutenção de uma estrutura de controles internos efetiva; e a utilização do COBIT® durante a definição dos principais riscos e controles desenvolvidos.

Além de entrevistas com os gestores de projetos, a pesquisa utilizou para análise os documentos elaborados pela consultoria externa que prestou serviço a essas organizações.

4 RESULTADOS DA PESQUISA

Os dados obtidos nas entrevistas com os gestores foram muitos semelhantes. Isso evidencia a existência de uma metodologia utilizada por essas organizações, fruto do *framework* COBIT®. Entretanto, observaram-se algumas diferenças:

- **Premissa utilizada na definição dos riscos**. Para os oitos gerentes entrevistados o ponto de partida na definição dos riscos relevantes aplicáveis á área de TI é a análise dos riscos de negócio da organização, ou seja, os riscos definidos pela alta administração, os quais poderiam impactar negativamente o atingimento das metas estabelecidas pela companhia em sua estratégia.
- **Alinhamento entre a área de TI e as áreas de negócio**. Para seis dos gestores entrevistados existia um alinhamento adequado entre a área de TI e as áreas de negócio na manutenção e otimização dos controles internos de TI. No entanto, em dois casos, a área de TI enfrentava grandes dificuldades em manter os controles implementados de forma efetiva. Isto porque, existia certa dificuldade entre as áreas de negócio no que diz respeito às regras de prazo, documentação, testes formais de aceitação, abertura de chamado para todos os pedidos, entre outras. Tais dificuldades foram relatadas nos casos das organizações varejista de móveis e na rede de drogarias, sendo uma de médio e outra de grande porte, e ambas do setor de comércio.
- **Utilização do *framework* COBIT®**. Em todos os oito casos analisados, o COBIT® foi utilizado como guia na identificação e mitigação dos principais riscos de TI e controles desenvolvidos.

  Na segunda etapa da pesquisa foram analisadas as documentações existentes nas oito

organizações, cujas cópias também estão presentes, em formato eletrônico, nas bases de dados da consultoria. Com base na análise desses documentos foram identificados os principais riscos e controles em execução nas organizações. A relação de riscos e respectivos controles está apresentada no Quadro 2.

Quadro 2 – Principais riscos e controles identificados nas organizações.

Riscos		Controles	
N°	Descrição	N°	Descrição
1	Acesso não autorizado aos sistemas pode afetar a disponibilidade, confiabilidade e integridade dos dados	3	No desligamento de um empregado, seus acessos aos sistemas e rede interna são imediatamente bloqueados
		11	Acesso de usuários à rede e aos sistemas é aprovado formalmente pelo gestor responsável pela área
2	Acesso não autorizado à base de dados pode causar violações de integridade e confidencialidade dos dados	4	Senhas de acesso a rede e sistemas estão parametrizados com tamanho mínimo, tempo de expiração, complexidade e bloqueio por número de tentativas de acesso inválidas
		5	Somente usuários autorizados possuem acesso direto ao banco de dados da companhia e as parametrizações de acesso possuem mecanismos de segurança.
3	Dano à estrutura física dos servidores pode ocorrer, e comprometer a integridade e continuidade das operações	7	Acesso à sala dos servidores é restrito ao pessoal autorizado, e possui bloqueio. O ambiente possui dispositivos de segurança, tais como, extintores e alarmes de incêndio, piso falso e temperatura constante
4	Ausência de alinhamento entre os investimentos na área TI e a estratégia de negócio da empresa	9	Existe Comitê de TI formado pela alta administração que atua na definição das políticas e acompanhamento dos projetos relacionados aos recursos de TI da empresa
		10	Área de TI é periodicamente avaliada pelas áreas de negócio, por meio de pesquisas sobre os aspectos relevantes dos serviços prestados pela área. O resultado da avaliação é usado na definição de melhorias nos serviços de TI
		19	Área de TI tem como controlar a quantidade de chamados abertos, bem como seu status e a documentação técnica dos desenvolvimentos de recursos elaborados internamente
5	Dependência de um ou mais profissionais técnicos na área de TI	18	Existe política formal de desenvolvimento de sistemas e é seguida pelos desenvolvedores da área de TI. Esta política contempla as melhores práticas no que tange aos controles e documentação técnica sobre os sistemas
6	Falta de cumprimento de obrigações por parte de fornecedor ocasiona prejuízos à empresa	12	Contratos de prestação de serviços são assinados de forma a a atingir dos objetivos de negócio, e há indicadores de desempenho que são monitorados pela área de TI
7	Falta de continuidade das operações da empresa em caso de desastres ou impossibilidade de acesso às dependências de TI	20	Há um plano de continuidade dos negócios contemplando as diretrizes para a manutenção das atividades de TI em caso de desastre ou impossibilidade de acesso às dependências da empresa
8	Informações incorretas são transferidas entre os sistemas	21	Interfaces entre os principais sistemas da empresa são monitoradas e os erros são prontamente resolvidos
9	Informações críticas não estão disponíveis quando necessário	16	Dados relevantes da empresa são gravados e mantidos em local apropriado, fora das dependências da empresa

Quadro continua na próxima página

Riscos		Controles	
N°	Descrição	N°	Descrição
10	Mudanças feitas em ambiente de produção podem impactar a integridade e confiabilidade dos aplicativos e possibilitar a ocorrência de fraudes	1	Ambientes de desenvolvimento e produção encontram-se segregados em servidores distintos, com acesso restrito
		6	Atualização do antivírus é realizada automaticamente no servidor e replicada a todas as máquinas da rede
		14	Mudanças somente são levadas ao ambiente de produção após testes e aprovação formal dos usuários das áreas de negócio
		15	Novos sistemas ou mudanças somente são levadas ao ambiente de produção após aprovação do gerente de TI
11	Perda de dados críticos ou paradas no funcionamento de recursos de TI	8	*Firewall* é utilizado com parâmetros adequados, e dispositivos e filtros impedem o acesso a *sites* com conteúdo duvidoso
12	Possibilidade de questionamentos trabalhistas quanto à equiparação de cargos e salários para profissionais de mesma área	13	Cargos da área de TI possuem requisitos básicos definidos formalmente, visando uma adequação às atividades realizadas pelo profissional.As atribuições de cada profissional são de conhecimento de todos os empregados das áreas de negócio
13	O processamento em lote não ocorre corretamente	22	Exceções no processamento em lote são identificadas e tratadas por profissional da área TI
14	Uso indevido ou mal intencionado dos recursos computacionais da empresa por parte dos empregados	2	Existe política formal de segurança da informação divulgada a todos os empregados da empresa. Esta política contempla as responsabilidades no uso dos recursos computacionais
15	Uso de recursos ilegais que pode acarretar autuações e danos nos equipamentos da empresa	17	Periodicamente é efetuado um inventário de *hardware* e *software* a fim de assegurar que as licenças instaladas nas máquinas estão de acordo com o registrado pela área de IT

Fonte: próprio autor.

A associação entre as organizações pesquisadas e os respectivos controles identificados pode ser vista na Tabela 1. A partir desse quadro pode-se identificar os controles mais comumente utilizados pelas organizações e os que são menos relevantes sob o ponto de vista de um sistema otimizado de controles internos. Verifica-se que os controles 4, 7 e 16 estão presentes em sete organizações pesquisadas, o controle 3 está presente em seis organizações, e os controles 1, 5, 9 e 11 estão presentes em cinco organizações. Somando-se a estes os controles 2, 6, 12 e 14, presentes em quatro organizações, tem-se os controles mais freqüentemente implementados no gerenciamento de riscos associados a TI. Todos esses controles estão presentes em pelo menos 50% das organizações pesquisadas.

Não se pode simplesmente descartar os demais controles que estão presentes em apenas três ou menos organizações. As organizações pesquisadas possuem portes diferentes e atuam em setores e segmentos diferentes. Em razão disso, pode-se inferir que alguns controles são aplicáveis somente a determinados setor ou ramos de atuação, e também são influenciados pelo porte das organizações. Por outro lado, é plausível considerar que os controles mais freqüentemente utilizados devem ser levados em conta durante a implementação de uma estrutura de controles internos na área de TI, ou conforme definição do COBIT®, eles podem ser classificados como parte dos Controles Gerais de Tecnologia de Informação (ITGC) principais das organizações privadas.

Tabela 1 – Controles mais freqüentes utilizados pelas organizações pesquisadas.

Tipo de controle	Organizações pesquisadas								Total
	1	2	3	4	5	6	7	8	
4	●	●		●	●	●	●	●	7
7	●	●		●	●	●	●	●	7
16	●	●		●	●	●	●	●	7
3	●	●	●	●		●	●		6
1	●	●		●	●		●		5
5	●	●		●	●			●	5
9		●	●	●	●		●		5
11	●		●	●	●		●		5
2		●		●	●			●	4
6		●		●	●	●			4
12			●	●	●		●		4
14	●		●	●	●				4
8		●		●	●				3
13				●				●	2
15	●			●					2
18					●			●	2
21	●							●	2
22	●	●							2
10		●							1
17				●					1
19							●		1
20								●	1
Total	11	12	5	16	13	5	9	8	

Fonte: próprio autor.

A partir dos principais controles identificados nesta pesquisa, foi efetuada uma associação destes controles com os objetivos de controle recomendados pelo *framework* COBIT®. Essa associação esta ilustrada no Quadro 3. Analisando os resultados dessa associação é possível constatar que todos os quatro domínios do COBIT® (Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte e Monitoramento e Controle) são considerados nos 12 principais controles implementados pelas organizações pesquisadas.

Quadro 3 – Controles relacionados com os objetivos de controle do COBIT®.

Controle	*Framework* COBIT®	
	Dimensão	Objetivo de controle
1	Planejamento e Organização	PO 4.11 – Segregação de funções AI 7.4 – Ambiente de testes
2	Planejamento e Organização	PO 6.1 – Políticas e procedimentos de TI PO 6.3 – Gerenciamento das políticas de TI
3	Planejamento e Organização	PO 4.11 – Segregação de Funções PO 7.8 – Desligamento de empregados
4	Planejamento e Organização	PO 4.11 – Segregação de funções

Quadro continua na próxima página

Controle	*Framework* COBIT®	
	Dimensão	Objetivo de controle
5	Planejamento e Organização Entrega e Suporte	PO 4.11 – Segregação de funções DS 5.4 – Gerenciamento das contas de usuários
6	Entrega e Suporte	DS 5.10 – Segurança da rede
7	Planejamento e Organização Entrega e Suporte	PO 4.11 – Segregação de funções DS 12.2 – Segurança Física DS 12.3 – Acesso Físico
9	Planejamento e Organização Monitoramento e Controle	PO 4.2 – Comitê Estratégico de TI PO 4.3 – Gerenciamento do Comitê Estratégico de TI ME 4.2 – Alinhamento Estratégico
11	Planejamento e Organização Entrega e Suporte	PO 4.11 – Segregação de Funções DS 5.4 – Gerenciamento das contas de usuários
12	Entrega e Suporte	DS 1.1 – Modelo de gerenciamento do nível de serviço DS 1.3 – Gerenciamento do nível de serviço
14	Aquisição e Implementação I	AI 7.2 – Planos de testes AI 7.3 – Plano de implementação AI 7.7 – Aceite final do usuário
16	Entrega e Suporte	DS 4.9 – Backup e manutenção DS 11.5 – Backup e recuperação

Fonte: próprio autor.

5 CONCLUSÃO

O objetivo deste trabalho é analisar casos de implementação de controles para garantir a integridade da TI. Este objetivo foi atingido por uma pesquisa exploratória, envolvendo um estudo de múltiplos casos com oito organizações brasileiras de médio e grande porte, onde foram entrevistados os gestores dos projetos de implementação de controles internos na área de TI.

Observou-se que o principal item a ser considerado no início de qualquer implementação de controles internos é a identificação dos riscos de negócio da empresa, que devem ser convertidos em riscos inerentes ao ambiente de TI. Em seguida, deve-se analisar quais seriam os controles que podem mitigar tais riscos, utilizando como modelo para esta análise o *framework* COBIT®.

A área de TI é dinâmica e está em constante evolução, o que dificulta a identificação de riscos e seus respectivos controles. Essa realidade acrescentou limitações à realização desta pesquisa, entre as quais se destacam: as entrevistas foram feitas pelo próprio pesquisador o que ajudou na obtenção de respostas mais confiáveis, mas certamente acrescentou o viés do pesquisador; e o estudo de múltiplos casos, utilizado como estratégia de pesquisa, impede a generalização dos resultados.

Os resultados obtidos estão apresentados em dois tópicos, de acordo com as perguntas de pesquisa formuladas na seção 3.

- **Principais controles utilizados pelas organizações brasileiras**. Nas oito empresas analisadas na pesquisa foram identificados 22 controles relacionados à área de TI. Destes, 12 podem ser considerados como os principais, pois estão presentes em pelo menos 50% das empresas pesquisadas.
- **Associação entre os controles utilizados nas organizações e os objetivos de controle do COBIT®**. Os 12 principais controles abrangem os quatro domínios do *framework* COBIT®, e endereçam 19 objetivos de controle. Isso mostra a relevância desse conjunto de controles em fase a todos os objetivos de controle previstos pelo

COBIT®. Esse conjunto resumido de controles permite às organizações priorizar os esforços de gerenciamento de riscos associados a TI, iniciando o gerenciamento com um conjunto reduzido de controles e, portanto, de menor custo para organizações. Mais ainda, permite uma maior flexibilidade aos processos organizacionais por focar em um conjunto menor de controles.

REFERÊNCIA

ALBERTIN, A. L. Valor Estratégico dos Projetos de Tecnologia de Informação. **Revista de Administração de Empresas**, São Paulo, p. 42-50, jul./set. 2001.

ALBERTIN, A. L. **Administração de Informática**. 4ª ed. São Paulo: Atlas, 2002.

BATEMAN, T. SNELL, S. **Administração: construindo vantagem competitiva**. São Paulo: Ed. Atlas, 2002.

CONSIGLIO, E. P. G. **Avaliação de Tecnologia de Informação nas Organizações – Indicadores de Performance**. São Paulo: MBA in Company – FGV/EAESP PriceWaterHouse Coopers, 2003.

CORRÊA, P. M. **Um estudo sobre a implantação da governança de TI com base em modelos de maturidade**. Tese (Mestrado em Tecnologia) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2006.

FERNANDES, A. A.; ABREU, V. F. **Implantando a Governança de TI**. Rio de Janeiro: Brasport, 2006.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4ª ed. São Paulo: Ed. Atlas, 2002.

ISACA. http://www.isaca.org.br/novoportal. Brasil, 2009 acessado em 01/05/2009.

ITGI, The IT Governace Institute. **CobiT 4.1: Control Objectives for Information and related Technology**. Printed in United States of America, 2007.

MENEZES, H. N. **Avaliação do nível de maturidade da governança de tecnologia da informação: Estudo de caso em indústrias de grande porte**. Tese (Mestrado em Ciência da Computação) – Universidade de Fortaleza, 2005.

PCAOB, Public Accounting Oversight Board. http://www.pcaobus.org acessado em 14/05/2009.

PMI, O Project Management Institute. www.pmi.org. EUA, 2009 acessado em 14/05/2009

PROJECT MANAGMENT INSTITUTE. **A guide to the project managment body of knowledge – PMBOK Guide**. Newton Square: PMI, 2004.

PORTER, M. E.; MILLAR, V. E. **How information gives you competitive advantage**. Harvard Business Review, Jul./Ago.1985.

RICHARDSON, R. J.; PERES, J. A. S.; WARDELEY, J. C. V.; CORREIA, L. M.; PERES, M. H. M. **Pesquisa Social - Métodos e Técnicas**. São Paulo: Atlas, 1999.

ROBBINS, S. **Administração: mudanças e perspectivas**. São Paulo: Ed. Saraiva, 2000.

SEI, Software Engineering Institute. **CMMI 1.2** Carnegie Mellon University, 2007

SILVA, E. M. **Direcionamento Estratégico da Gestão da Tecnologia da Informação**. São Paulo: POLI – USP, 2007

TSAI, L. W. K. **Modelo de gestão estratégica das informações: Um estudo comparativo de casos de pequenas empresas**. Tese (Mestrado em Engenharia Naval e Oceânica) – Universidade de São Paulo, Escola Politécnica. São Paulo, 2006.

YIN, R. K. **Estudo de caso planejamento e métodos**. 3. ed. Porto Alegre: Bookman, 2005.