

Avaliação do Nível de Maturidade da Governança de Tecnologia da Informação em Empresas que Atuam em Mercados Globalizados: Estudo de Caso em Indústrias de Grande Porte

Haroldo Nunes Menezes

Universidade de Fortaleza (UNIFOR), Mestrado em Informática Aplicada (MIA)
Av. Washigton Soares, 1321- B. Edson Queiroz. CEP: 60.811.905, Fortaleza (CE), Brasil
haroldo.menezes@mdb.com.br

and

José Bezerra da Silva Filho

Universidade de Fortaleza (UNIFOR), Mestrado em Informática Aplicada (MIA)
Av. Washigton Soares, 1321- B. Edson Queiroz. CEP: 60.811.905, Fortaleza (CE), Brasil
bezerra@unifor.br

Abstract

This paper is about the level of adherence of large-sized enterprises in the branch of industrial activity to the processes involved in IT Governance contemplated by each one of the 34 processes described in CobiT® related to service management and infrastructure of IT. An evaluation was made of a sample of eighteen enterprises through a questionnaire structured into five sets, bringing together 39 questions. The results obtained suggest that the maturity levels of the processes involved in IT Governance are placed in the inexistent or Initial / Ad hoc categories. Within the sample, the indicators suggest a reactive behavior of managers in the IT area and ignorance of better practice guides and evaluation metrics.

Keywords: Corporate Governance, IT Governance, *Sarbanes-Oxley*, *ITIL*®, *CobiT*®.

Resumo

Este artigo apresenta uma avaliação em uma amostra de dezoito empresas de grande porte do ramo de atividade industrial que atuam em mercado globalizados, do nível de maturidade dos processos envolvidos na Governança de TI, contemplando cada um dos 34 processos descritos no *CobiT*® envolvendo o gerenciamento dos serviços e da infraestrutura de TI. Os resultados obtidos no experimento sugerem que os níveis de maturidade dos processos envolvidos na Governança de TI posicionam-se nas categorias *Inexistente* ou *Inicial/Ad hoc*. Indicadores sugerem um comportamento reativo por parte dos gerentes da área de TI, e desconhecimento das guias de melhores práticas de avaliação que influenciam na agregação de valor financeiro da empresa.

Palavras-chave: Governança corporativa, Governança de TI, *Sarbanes-Oxley*, *ITIL*®, *CobiT*®, Tecnologia da Informação.

1. INTRODUÇÃO

A evolução da TI e sua disseminação nos setores das organizações geraram uma dependência significativa do negócio em relação aos serviços prestados. Essa dependência cria novas exigências para serviços de TI tais como: disponibilidade, garantia de continuidade, segurança, eficiência, qualidade na entrega e no suporte, controles, conformidade, consistência e tempestividade. Diversos regulamentos surgiram no cenário internacional como decorrência da necessidade de mitigar riscos oriundos da indisponibilidade da tecnologia, bem como de proporcionar um grau de transparência compatível com as expectativas de investidores.

A conformidade com os regulamentos vigentes, as exigências decorrentes do aumento do grau de dependência do negócio em relação à área de TI e o gerenciamento financeiro dos projetos criaram as condições propícias para o surgimento de modelos de Governança de TI que sugerem a adoção de guias de melhores práticas para atingir a eficiência na gestão dos serviços de TI. Modelos de auditoria também foram propostos para identificar o nível de maturidade da organização, e técnicas foram adotadas para definir métricas que possibilitem avaliar sua evolução.

O principal objetivo deste estudo é avaliar o nível de maturidade da Governança de TI nas indústrias de grande porte, contemplando cada um dos 34 processos descritos no *CobiT® (Control Objectives for Information and related Technology)* com envolvimento do gerenciamento dos serviços e da infra-estrutura de TI.

Os objetivos complementares contemplam: identificar nas empresas pesquisadas o grau de conhecimento de métodos, técnicas e ferramentas que embasam os processos de TI, e a adoção das boas práticas de Governança de TI; verificar se as empresas estão certificando profissionais, com vistas à implementação futura de projetos na área de Governança de TI; e verificar a efetiva aplicação do conhecimento dos métodos, técnicas e ferramentas que apóiam a Governança de TI nas organizações pesquisadas.

Sobre o problema, formulam-se as seguintes hipóteses:

- **H₁** – As indústrias de grande porte encontram-se em níveis de maturidade de governança com *Processos definidos* ou, pelo menos, *Repetitivo mas intuitivo*, haja vista que atuam em mercados globalizados como exportadores, recebendo influências da Lei *Sarbanes-Oxley* (SARBANES -OXLEY ACT, 2002), e/ou são empresas de capital aberto, para as quais existe a cartilha *Recomendações da CVM sobre Governança Corporativa* (CVM, 2002).
- **H₂** – As empresas pesquisadas estão mobilizando os setores de TI, objetivando a adesão a normas e padrões (*compliance*) e a implantação de melhores práticas de gerenciamento de serviços e infra-estrutura de TI (*best practices*).
- **H₃** – Os executivos de TI das indústrias de grande porte pesquisadas detêm um conhecimento acerca de métodos e práticas que fundamentam a implantação da Governança de TI e estão treinando suas equipes técnicas para adequação dessas recomendações.

2. TECNOLOGIA DA INFORMAÇÃO E PRINCÍPIOS DA GOVERNANÇA

Segundo Toffler (1985) a informação tornou-se tão (ou mais) importante quanto a terra, o trabalho, o capital e a matéria-prima. Novos paradigmas tecnológicos apontam para um fator de riqueza determinante na era pós-industrial: a posse da informação (SIQUEIRA FILHO; SILVA FILHO, 2004).

Ao analisar diversas abordagens de alinhamento estratégico entre negócios e TI, Teixeira Júnior (2003) conclui que o alinhamento dos negócios e da TI é descrito não como um fenômeno unidimensional, mas como um grande conjunto de múltiplos e simultâneos componentes de alinhamento que resultam na adequação entre as prioridades e as atividades da área de TI e das unidades de negócio.

O alinhamento estratégico entre TI e negócios é o objetivo fundamental da Governança de TI. TI é responsável por universalizar a competência de negócios, criando produtos e serviços que adicionem valor, e transformando a organização (IT GOVERNANCE INSTITUTE, 2003). Para o *IT Governance*, o alinhamento compreende mais que apenas a integração de estratégias de TI e da organização; é uma jornada e não apenas um destino.

O atentado terrorista contra as Torres gêmeas (*World Trade Center*) em Nova Iorque, em 11 de setembro de 2001, produziu efeitos sob a ótica de TI. O episódio foi a comprovação factual de que a indisponibilidade de informações pode comprometer a sobrevivência da empresa, tanto quanto estratégias incorretas ou fatores ligados ao negócio.

O ano 2002 foi marcado pelos escândalos contábeis da Enron e da Worldcom. As fraudes contábeis produziam resultados fictícios, deixavam de declarar créditos em liquidação, apropriavam receitas antecipadas e pagavam bônus aos administradores por lucros irreais, tudo isso com a conivência de empresas de auditoria independente.

Após o “11 de setembro” e os escândalos contábeis, foi editada em 30 de Junho de 2002 nos Estados Unidos da América a Lei *Sarbanes-Oxley* com o objetivo de evitar a perda da confiança no mercado financeiro, dar maior

publicidade a informações e propiciar fiscalizações preventivas pela SEC (*Security and Exchange Commission*), a comissão de valores mobiliários dos Estados Unidos (SARBANES-OXLEY ACT, 2002).

A Lei exige a criação de mecanismos de auditoria e segurança, incluindo a instalação de comissões encarregadas de supervisionar as atividades e operações da empresa, de modo a inibir a ocorrência de fraudes. Dentre essas normas, passaram a ser exigidas características de confiabilidade e disponibilidade dos sistemas e aplicativos.

Em junho de 2002, a Comissão de Valores Mobiliários (CVM) publicou a cartilha “Recomendações da CVM sobre Governança Corporativa”, que contém orientações relativas a boas práticas de Governança Corporativa. Embora a cartilha não constitua norma cujo descumprimento implique sanções, a adoção das práticas ali recomendadas significa a utilização de padrões de conduta superiores aos exigidos pela lei e pela regulamentação da própria CVM (CVM, 2002).

Espera-se que a Governança Corporativa assegure a observância de critérios que garantam a proteção financeira dos acionistas, como equidade entre controladores e minoritários, transparência (*disclosure*), responsabilidade pelos resultados (*accountability*) e obediência às leis do país (*compliance*).

A expressão *IT Governance* é definida como uma estrutura de relações e processos que dirige e controla uma organização a fim de atingir seu objetivo de adicionar valor ao negócio por meio do gerenciamento balanceado do risco com o retorno do investimento. O objetivo principal da Governança de TI é alinhar a TI ao negócio, agregando valor e minimizando riscos (IT GOVERNANCE INSTITUTE, 2005). Broadbent (2005) ensina que a chave para a efetividade da Governança de TI é sua orientação para o negócio.

O propósito da Governança de TI é atingir os seguintes objetivos:

- alinhar a estratégia de TI com o negócio;
- usar a TI eficientemente, para explorar novas oportunidades e maximizar benefícios para a empresa, medindo o desempenho da TI e ajustando suas ações, quando necessário;
- usar recursos da TI de forma eficaz, garantindo uma boa relação custo/benefício; e
- assegurar adequado tratamento aos riscos originários da TI.

No segundo semestre de 2004 na pesquisa *CIO Metrics* (IDC, 2004) possibilitou constatar, com relação ao conhecimento profissional dos executivos de TI, que:

- a) mais de 50% não conhecem ou não têm planos para implementação de Governança de TI;
- b) mais de 85% não conhecem *CobiT*® (*Control Objectives for Information and related Technology*); e
- c) mais de 80% não conhecem *ITIL*® (*Information Technology Infrastructure Library*).

Em 2005, a pesquisa realizada pelo IDC no IT Fórum 2005 com os executivos de TI das maiores empresas brasileiras (IDC, 2005) levou à constatação de que, para 44% dos entrevistados, a maior prioridade da área de TI no ano de 2005 era “Alinhar TI ao negócio/Governança de TI”.

3. GOVERNANÇA DE TI: MELHORES PRÁTICAS, AUDITORIA E MÉTRICAS DE AVALIAÇÃO

3.1 *Information Technology Infrastructure Library – ITIL*®

ITIL®, Biblioteca de Infra-estrutura de TI, é uma estrutura de padrões e melhores práticas para gerenciar os serviços e a infra-estrutura de TI. É a abordagem mundialmente mais difundida e adotada para o Gerenciamento de serviços de TI (*Service Management*) (OFFICE OF GOVERNMENT COMMERCE, 2004).

O *ITIL*® é composto pelas seguintes publicações: *Best practice for Planning to Implement Service Management*; *Best practice for Service Support*; *Best practice for Service Delivery*; *Best practice for Security Management*; *Best practice for ICT Infrastructure Management*; *Best practice for Application Management*; *Best practice for Software Asset Management*; e *Best practice for The Business Perspective* (OFFICE OF GOVERNMENT COMMERCE, 2005).

3.1.1 Gestão de serviços de TI

A gestão de serviços de TI (*Service Management*) visa à melhoria na qualidade dos serviços de TI e, conseqüentemente, no suporte aos processos de negócio. Para ser capaz de entregar o que o cliente deseja, a TI deve observar: a especificação, a conformidade, a consistência, o valor e a comunicação. A gestão dos serviços também é suportada pelas normas BS 15000-1:2002 e BS 15000-2:2003. A Gestão de Serviços de TI (*IT Service Management - ITSM*) é composto pelas disciplinas de *Service Support* e *Service Delivery*.

3.1.2 Suporte aos serviços

Composto pelos processos: Gestão de Incidentes, Gestão de Problemas, Gerência de Configuração, Gerência de Liberações e Gerência de Mudanças (OFFICE OF GOVERNMENT COMMERCE, 2004c).

Gestão de Incidentes (*Incident Management*) – Um incidente é um evento que não faz parte da operação normal, reduzindo a qualidade ou suspendendo a entrega do serviço. O objetivo da Gestão de Incidentes é restaurar a operação normal de um serviço no menor período de tempo possível, a fim de minimizar os aspectos negativos sobre a operação dos negócios e os melhores níveis de qualidade e disponibilidade. Trata do efeito, e não da causa.

Gestão de Problemas (*Problem Management*) – O objetivo da Gestão de Problemas é minimizar o impacto de incidentes sobre a capacidade de negócios de uma organização, causados por falhas na infra-estrutura, e prevenir a recorrência de incidentes. Dá-se através da investigação, diagnóstico e solução de cada problema. Busca a causa-raiz dos incidentes.

Gestão de Configuração (*Configuration Management*) – Tem por objetivo assegurar que somente componentes autorizados, ou seja, itens de configuração, como *software*, *hardware*, documentos, processos e procedimentos sejam utilizados no ambiente de TI, e que todas as mudanças nesses componentes sejam gravadas e rastreadas durante todo o ciclo de vida de cada um. Objetiva ainda garantir a comunicação entre todas as disciplinas da Gestão de Serviços, por meio do Banco de Dados de Gerência de Configurações (*CMDB*).

Gerência de Liberações (*Release Management*) – Tem os seguintes principais objetivos: coordenar e gerenciar implantação de *releases* no ambiente em operação; desenhar procedimentos eficientes para distribuição e implantação de mudanças no ambiente de TI. Mantém o banco de dados de configurações atualizado. Implanta *releases* de forma controlada e segura, garantindo segurança e rastreabilidade.

Gestão de Mudanças – O objetivo da Gestão de Mudanças é garantir a aplicação de métodos e procedimentos padronizados, para lidar eficientemente com todas as mudanças no ambiente computacional, minimizando impactos na qualidade dos serviços ocasionados por incidentes relacionados a esses eventos. Todas as partes afetadas por uma mudança devem ter a oportunidade de acompanhá-la e entender seus impactos.

3.1.3 Entrega de serviços

Os processos relacionados com a Entrega de Serviços (*Service Delivery*) compreendem: Gerência de Nível de Serviço, Gerência de Capacidade, Gerência de Disponibilidade, Gerência Financeira e Gerência de Continuidade (OFFICE OF GOVERNMENT COMMERCE, 2005a).

Gerência de Nível de Serviço (*Service Level Management*) – Tem por objetivo definir, monitorar e controlar os Acordos de Nível de Serviço (*Service Level Agreements*). *SLA* é um acordo formal, realizado entre a área de TI e seus clientes, no qual são definidas as metas objetivas de desempenho e as responsabilidades das partes.

Gerência de Capacidade (*Capacity Management*) – Planeja, justifica e gerencia níveis apropriados de recursos necessários para soluções específicas de TI, evitando a falta ou o excesso de recursos. Responde por atividades de ajuste para otimizar o uso dos recursos disponíveis. Atua no gerenciamento da capacidade de negócios, serviços e recursos.

Gerência de Disponibilidade (*Availability Management*) – Este processo é responsável pela racionalização da capacidade da infra-estrutura e da organização do suporte, para que possa entregar os serviços de TI a um custo

compatível com os níveis de disponibilidade necessários para a satisfação dos requisitos do negócio, dentro das especificações dos Acordos de Níveis de Serviços.

Gerência Financeira (*Financial Management*) – Realiza a gestão dos recursos financeiros da área de TI. A Gerência Financeira deve otimizar os recursos financeiros, contabilizar as despesas de forma a apropriar os custos de TI de acordo com os serviços prestados, e apoiar decisões de investimentos em TI. Cobre orçamento (previsão das despesas e investimentos), contabilidade (registro) e cobrança (apropriação por centros de custos).

Gerência de Continuidade (*IT Service Continuity Management – ITSCM*) – Garante que qualquer serviço de TI é capaz de prover valor para seus clientes e usuários, mesmo em situações em que falharem as soluções normais de disponibilidade. Suporta o planejamento de continuidade dos negócios, garantindo que todos os recursos e serviços de TI possam ser recuperados no tempo combinado. Avalia impactos, riscos e ameaças.

3.1.4 Gestão da Infra-estrutura da TI e da Comunicação

O crescente grau de dependência do negócio em relação à tecnologia, a crescente complexidade do ambiente, as necessidades de flexibilidade e satisfação do cliente, as restrições de investimentos e os reduzidos ciclos de vida de produtos compõem os desafios do gerenciamento (OFFICE OF GOVERNMENT COMMERCE, 2004a).

O escopo do gerenciamento da infra-estrutura de ICT engloba o desenho, o planejamento, a implantação, a operação e o suporte técnico. Essa disciplina se relaciona com as disciplinas entrega dos serviços e suporte ao serviço.

3.1.5 Gestão da segurança

A Gestão da Segurança (*Security Management*) tem como propósito garantir a segurança do negócio, e limitar os danos através da prevenção, minimizando o impacto dos incidentes de segurança da informação. A Gestão de Segurança adota a BS 7799-1:1999 como referência de melhores práticas a serem adotadas. Referências podem ser obtidas também na norma ISO/IEC 17799:2000 e em sua equivalente nacional, a ABNT NBR ISO/IEC 17799.

A segurança preserva o valor da informação sobre os seguintes aspectos: confidencialidade, integridade e disponibilidade. A confidencialidade protege informações importantes de uso ou interceptação não autorizados, garantindo que estarão acessíveis somente a pessoas autorizadas. A integridade salvaguarda a exatidão e a completude da informação e do *software*. A disponibilidade assegura que a informação e os serviços de TI estejam disponíveis quando necessário (OFFICE OF GOVERNMENT COMMERCE, 2004b).

Existem três fontes principais de requisitos de segurança:

- aquela derivada da avaliação de risco dos ativos da organização, identificando-se as ameaças aos ativos, as vulnerabilidades, a probabilidade de ocorrência e o impacto potencial;
- a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço devem atender; e
- o conjunto particular de princípios, objetivos e requisitos para o processamento da informação que uma organização precisa desenvolver para apoiar suas operações.

A ISO/IEC 17799:2000 e sua equivalente nacional, a NBR ISO/IEC 17799, são compostas pelos seguintes módulos: Política de segurança; Segurança organizacional; Classificação e controle dos ativos de informação; Segurança em pessoas; Segurança física e do ambiente; Gerenciamento das operações e comunicações; Controle de acesso; Desenvolvimento e manutenção de sistemas; Gestão da continuidade do negócio; e Conformidade.

3.2 Control Objectives for Information and related Technology – COBIT®

CobiT®, Objetivos de Controle para Informação e Tecnologia Relacionada, é um *framework* para a gestão de TI recomendado pelo ISACF (*Information Systems Audit and Control Foundation*) (ISACA, 1999). O *CobiT*® fornece um detalhado conjunto de procedimentos e diretrizes que devem ser aplicados na auditoria dos processos de TI, bem como uma avaliação dos riscos e probabilidades de sua ocorrência (ISACA, 2005).

As práticas de gestão do *CobiT*® auxiliam a otimizar os investimentos em TI, e fornecem métricas para avaliação dos resultados, por meio de um conjunto de recursos, compreendendo um sumário executivo, um *framework*, controle de objetivos, mapas de auditoria, um conjunto de ferramentas de implantação e um guia com técnicas de gerenciamento (IT GOVERNANCE INSTITUTE, 2005).

O *CobiT*® está distribuído em quatro domínios:

- Planejamento e organização – Cobre o uso da tecnologia e o modo como pode ser melhor utilizado na organização para que os objetivos e metas sejam atingidos. Também destaca a organização e a forma como a infra-estrutura de TI está preparada para otimizar resultados e gerar maiores benefícios do uso de TI;
- Aquisição e implementação – Endereça a estratégia da empresa na identificação de requerimentos de TI, aquisição de tecnologia e implementação dentro dos processos de negócio;
- Entrega e suporte – Foca nos aspectos da entrega da TI. Cobre áreas como execução de aplicações de sistemas de TI e seus resultados, bem como os processos de suporte que habilitam a execução desses sistemas com efetividade e eficiência. Os processos de suporte incluem objetivos de segurança e treinamento; e
- Monitoramento – Alinha com a estratégia da empresa, avaliando se as necessidades do negócio são atingidas com os sistemas de TI e se os necessários objetivos de controle cobrem os requerimentos regulatórios. Cobre também os objetivos de efetividade e disponibilidade, a auditoria e os objetivos de controles internos e externos.

Os domínios estão subdivididos em processos, que garantem a completude da gestão de TI, conforme descritos a seguir.

Domínio planejamento e organização (PO – *Planning and Organization*):

- PO1 – Define a estratégia de TI;
- PO2 – Define a arquitetura da informação;
- PO3 – Determina a direção tecnológica;
- PO4 – Define a organização de TI e seus relacionamentos;
- PO5 – Gerencia os investimentos de TI;
- PO6 – Gerencia a comunicação das diretrizes de TI;
- PO7 – Gerencia os recursos humanos;
- PO8 – Assegura alinhamento de TI com os requerimentos externos;
- PO9 – Avalia os riscos;
- PO10 – Gerencia os projetos; e
- PO11 – Gerencia a qualidade.

Domínio aquisição e implementação (AI – *Acquisition and Implementation*):

- AI1 – Identifica as soluções de automação;
- AI2 – Adquire os *softwares* e provê sua manutenção;
- AI3 – Adquire a infra-estrutura tecnológica e provê sua manutenção;
- AI4 – Desenvolve os procedimentos e provê sua manutenção;
- AI5 – Instala e certifica *softwares*; e
- AI6 – Gerencia mudanças.

Domínio entrega e suporte (DS – *Delivery and Support*):

- DS1 – Define os acordos de níveis de serviço (SLA) e provê sua manutenção;
- DS2 – Gerencia os serviços de terceiros;
- DS3 – Gerencia a *performance* e a capacidade do ambiente;
- DS4 – Assegura a continuidade de serviços;
- DS5 – Assegura a segurança dos serviços;
- DS6 – Identifica e aloca custos;
- DS7 – Treina os usuários;
- DS8 – Assiste e aconselha os clientes;
- DS9 – Gerencia a configuração;
- DS10 – Gerencia problemas e incidentes;
- DS11 – Gerencia os dados;

- *DS12* – Gerencia a infra-estrutura; e
- *DS13* – Gerencia as operações.

Domínio Monitoramento (M – *Monitoring*):

- *M1* – Monitora os processos;
- *M2* – Analisa a adequação dos controles internos;
- *M3* – Provê auditorias independentes; e
- *M4* – Provê segurança independente.

O *CobiT*® é eficiente em controles e métricas de TI para auditoria; descreve, para cada processo, os objetivos de controle, fatores críticos de sucesso, indicadores-chave de metas e desempenho, além de um modelo de maturidade; mas não descreve a forma de implementar os processos (FERNANDES, 2004; COEN; RUBINATO FILHO, 2005).

3.3 IT Governance Maturity Model

O *IT Governance Maturity Model* apóia-se nos conceitos do modelo *CMM SW (Capability Maturity Model for Software)* proposto pelo *SEI (Software Engineering Institute)*, com foco no nível de serviço (IT GOVERNANCE INSTITUTE, 2003).

O modelo descreve os processos e atividades, requeridos em cada um dos seis níveis de maturidade, a saber:

0-Inexistente

Não há gerenciamento de atividades relacionadas a TI para medir o que os objetivos de TI adicionam de valor para a organização, nem para medir se os riscos relacionados com TI são apropriadamente gerenciados.

1-Inicial / Ad hoc

O conceito de Governança de TI não existe formalmente, e a supervisão se baseia principalmente em considerações gerenciais de objetivos relacionados de TI caso a caso. A Governança de TI depende da iniciativa e da experiência de um time de gerenciamento, que limita a entrada dos demais integrantes da organização. A alta gerência somente é envolvida quando surgem problemas mais graves. O gerenciamento de desempenho é tipicamente limitado a medidas técnicas.

2-Repetitivo mas intuitivo

A realização supera a formalização. Requer supervisão de TI, sendo necessário compartilhar responsabilidades com a gerência sênior. Práticas regulares de Governança são metas. A criação de relatórios regulares de desempenho e investigação de problemas tomou lugar recentemente nas iniciativas do time de TI. Usuários-chave ou *stakeholders* são participantes voluntários ou cooptados.

3-Processos definidos

Um *framework* organizacional e de processos está definido para a supervisão e gerenciamento de atividades de TI e está sendo introduzido na organização como base para Governança de TI. O corpo gerencial tem objetivos de direção, que têm sido desenvolvidos segundo procedimentos específicos de gerenciamento, compatíveis com atividades de Governança..

4-Processos gerenciáveis e medidos

Ajustes de objetivos foram desenvolvidos para um estágio sofisticado, com relacionamentos entre objetivos externos em termos de negócios. Processos de TI provêm métricas bem compreendidas. O time da gerência corporativa agora trabalha junto com os objetivos de maximizar o valor da entrega de serviços de TI e gerenciar os riscos relacionados a TI. Existe um *assessment* regular das capacidades de TI, e os projetos têm sido entregues com os requisitos reais de desempenho. Relacionamentos são agora baseados em funções definidas e acordos de níveis de serviço.

5-Processos otimizados

Práticas de Governança de TI são desenvolvidas segundo uma sofisticada abordagem. Existe controle das estratégias de TI. Atividades são priorizadas de acordo com a real prioridade do negócio, o valor entregue para a corporação pode ser medido, e passos adotados tempestivamente corrigem desvios significativos ou problemas. O esforço despendido no gerenciamento de risco é minimizado por meio da adoção de padrões e automação de processos. A prática de melhoria

contínua da capacidade de TI está embebida na cultura. Auditorias independentes provêm garantias de gerenciamento. O custo de TI é efetivamente monitorado.

4. METODOLOGIA DA PESQUISA

A pesquisa realizada foi de natureza teórico-empírica, na medida em que buscou na literatura própria a fundamentação teórica, testando-se, na prática, o uso de métodos, técnicas e ferramentas; aplicada, pois se caracteriza pelo interesse prático, isto é, com resultados que sejam aplicados ou utilizados, imediatamente, na solução de problemas reais (MCDANIEL; GATES, 2003).

A pesquisa tem cunho descritivo, na medida em que delinea o que é o funcionamento no presente, e é focalizada em acontecimentos contemporâneos, caracterizando-se como estudo de caso com corte transversal (*cross-sectional study*).

O Sebrae (SEBRAE, 2003) classifica como empresa de grande porte quando na indústria, se emprega mais de 499 pessoas; e no comércio e serviços, se emprega mais de 99 pessoas. Pesquisa do Sebrae (SEBRAE, 2003) aponta a existência de 1.378 indústrias de grande porte no Brasil em 2003. Essa categoria de empresa compreende a população objeto da nossa pesquisa.

Uma amostra representativa tem as mesmas características da população de onde foi extraída (LAPPONI, 2005). Uma amostra pequena pode refletir com precisão as características da população de onde foi extraída (MCDANIEL; GATES, 2003). A amostra não-probabilística é um subconjunto de uma população no qual pouca ou nenhuma tentativa é feita para assegurar uma seção cruzada representativa (MCDANIEL; GATES, 2003). Nossa amostra de 19 empresas corresponde a 1,38% da população das indústrias de grande porte do Brasil.

As variáveis da pesquisa são qualitativas, ou seja, observações não numéricas, ordinais, pois observam uma ordem, uma hierarquia, dando nome a um objeto, categoria ou classe. Os números são utilizados para diferenciar em ordem de superioridade, seguindo algum critério hierárquico (LAPPONI, 2005).

A preparação do questionário envolveu um estudo detalhado do *CobiT*®, principal *framework* para auditoria dos níveis de Governança de TI, bem como uma análise das aplicações dos modelos de maturidade, para identificação do nível de maturidade de cada um dos processos e seus domínios (IT GOVERNANCE INSTITUTE, 2003).

Foram enviados 79 questionários sendo 19 restituídos, correspondendo a 24,05% do total. O questionário foi estruturado em cinco blocos, reunindo ao todo 39 questões. Descreve-se a seguir o conteúdo dos cinco blocos e a qualificação das respostas.

Os quatro blocos iniciais do questionário avaliam os quatro domínios do *CobiT*®: *Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte e Monitoramento*. As 34 questões correspondem aos processos do *CobiT*®. Todas as respostas dos quatro blocos iniciais foram qualificadas e hierarquizadas numa escala de 0 a 5, representando os níveis de maturidade (seção 2.3).

O quinto bloco avaliou, em cinco questões, o grau de conhecimento e aplicação de guias de melhores práticas, *framework* de auditoria, métodos e técnicas relacionados à Governança de TI. As respostas do quinto bloco foram qualificadas e hierarquizadas numa escala de 0 a 5, representando os graus conhecimento e aplicação da teoria.

Para facilitar a tabulação dos dados e a análise dos resultados da pesquisa, para cada questão foi preparada uma tabela de frequência, para registro do número de respondentes de cada opção de resposta, dos percentuais de cada nível de maturidade e dos índices acumuladosⁱ. Foi construído o gráfico de barras e calculadas as medidas de tendência central e de dispersão. O desvio-padrãoⁱⁱ significa o grau ao qual dados tendem a dispersar-se em torno de um valor médio. As medidas de dispersão são importantes para identificar iniciativas isoladas em processos específicos de Governança de TI.

A tabulação dos dados, a geração dos resultados estatísticos, a apresentação em tabelas e a representação gráfica foram desenvolvidas utilizando-se o Microsoft® Office Excel 2003. Laponi (2005) descreve detalhadamente a construção de resultados estatísticos utilizando o MS-Excel®.

5. RESULTADOS DE MEDIDAS EXPERIMENTAIS

A Tabela 5.1 apresenta os resultados da análise dos dados pesquisados propiciando um entendimento dos níveis de maturidade de Governança de TI de cada um dos 34 processos do *CobIT*® e do grau de conhecimento de métodos, técnicas e boas práticas que suportam o modelo.

Tabela 5.1 – Medidas de tendência central e de dispersão

Processo / Conhecimento da tecnologia	Tendência central			Dispersão	
	Média	Mediana	Moda	Desvio padrão	Variância
PO1 Define a estratégia de TI	1	1	1	0,647	0,418
PO2 Define a arquitetura da informação	2	2	2	0,767	0,588
PO3 Determina a direção tecnológica	2	2	2	0,786	0,618
PO4 Define a organização de TI e seus relacionamentos	1	1	0	1,629	2,654
PO5 Gerencia os investimentos de TI	2	2	1	1,259	1,585
PO6 Gerencia as comunicações das diretrizes de TI	0	0	0	0,705	0,497
PO7 Gerencia os recursos humanos	1	1	1	1,179	1,389
PO8 Assegura alinhamento de TI com requerimentos externos	1	1	0	0,857	0,735
PO9 Avalia os riscos	2	2	2	0,832	0,693
PO10 Gerencia os projetos	1	0	0	0,786	0,618
PO11 Gerencia a qualidade	0	0	0	0,686	0,471
AI1 Identifica as soluções de automação	1	1	1	0,583	0,340
AI2 Adquire os <i>softwares</i> e provê sua manutenção	1	0	0	1,364	1,859
AI3 Adquire a infra-estrutura tecnológica e provê sua manutenção	2	3	3	1,211	1,467
AI4 Desenvolve os procedimentos e provê sua manutenção	2	2	2	0,958	0,918
AI5 Instala e certifica os <i>softwares</i>	3	3	3	0,778	0,605
AI6 Gerencia mudanças	0	0	0	0,669	0,448
DS1 Define os acordos de nível de serviço e provê sua manutenção	1	0	0	0,924	0,853
DS2 Gerencia os serviços de terceiros	1	0	0	0,943	0,889
DS3 Gerencia a <i>performance</i> e a capacidade do ambiente	1	0	0	1,618	2,618
DS4 Assegura a continuidade de serviços	2	2	1	0,698	0,487
DS5 Provê a segurança dos serviços	2	2	2	0,323	0,105
DS6 Identifica e aloca custos	2	3	0	1,896	3,595
DS7 Treina os usuários	1	0	0	0,943	0,889
DS8 Assiste e aconselha os usuários	1	1	1	0,857	0,735
DS9 Gerencia a configuração	1	1	1	0,840	0,706
DS10 Gerencia problemas e incidentes	2	1	0	1,782	3,176
DS11 Gerencia os dados	1	0	0	0,970	0,941
DS12 Gerencia a infra-estrutura	2	2	2	1,043	1,088
DS13 Gerencia as operações	2	2	2	0,784	0,614
M1 Monitora os processos	1	1	1	0,979	0,958
M2 Analisa a adequação dos controles internos	2	3	3	1,328	1,765
M3 Provê auditorias independentes	1	0	0	1,215	1,477
M4 Provê segurança independente	1	0	0	1,138	1,294

ITIL	1	1	1	0,840	0,706
CobiT	1	1	0	0,616	0,379
IT Governance Maturity Model	1	1	1	0,539	0,291
PMBOK	1	1	1	0,647	0,418
CMM SW	1	1	1	0,000	0,000

6. CONSIDERAÇÕES FINAIS

O problema levantado enfatiza a necessidade de focar as ações no gerenciamento dos serviços de TI, observando-se todos os processos envolvidos: planejamento e organização, aquisição e implementação, entrega e suporte aos serviços e monitoramento. O trabalho avaliou os níveis de maturidade da Governança de TI em indústrias de grande porte.

Os resultados do experimento não validaram a hipótese **H₁**. As organizações pesquisadas, pertencentes ao ramo de atividade indústria e ao segmento de grande porte, possuem iniciativas de implementação de modelos de Governança de TI incipientes ou não as possuem. Ao observar a medida estatística que determina a maior frequência, a moda (Apêndice A), dos 34 processos do CobiT®, verifica-se que 16 processos encontram-se no estágio *Inexistente* (PO4, PO6, PO8, PO10, PO11, AI2, AI6, DS1, DS2, DS3, DS6, DS7, DS10, DS11, M3 e M4) e 8 se situam no *Inicial / Ad hoc* (PO1, PO5, PO7, AI1, DS4, DS8, DS9 e M1). Como podemos observar no Gráfico 1, os mais baixos níveis de maturidade foram encontrados nos processos PO6 *Gerencia as comunicações das diretrizes de TI*, PO11 *Gerencia a qualidade* e AI6 *Gerencia mudanças*.

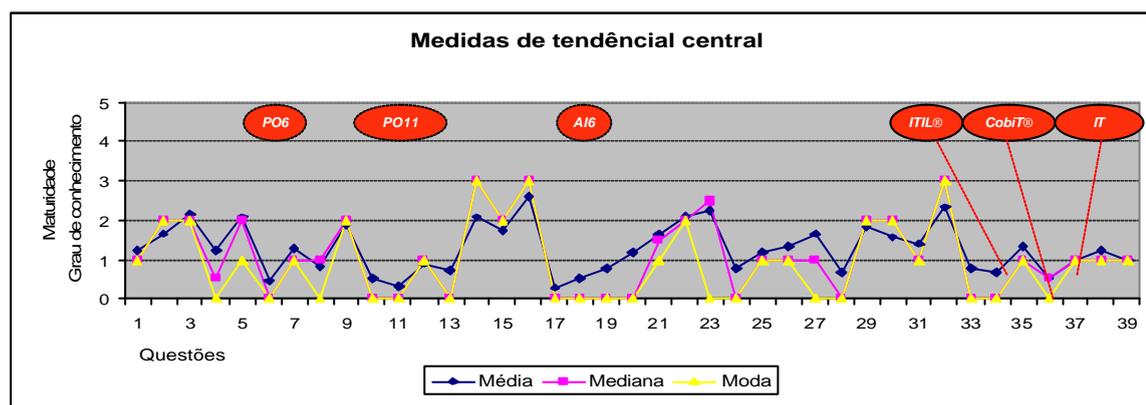


Gráfico 1 – Medidas de tendência central

A tabulação das respostas obtidas não validou a hipótese **H₂**. Para os pesquisadores, o comportamento da área de TI pode ser caracterizado como reativo, levando-se em conta que os processos com maior nível de maturidade (*Processos definidos*), em que foram encontrados modelos formais, decorrem de exigências de outras áreas, tais como: Financeiro, Controladoria e Auditoria. Esses processos dizem respeito à aquisição de infra-estrutura (AI3), em que o Financeiro exige análise de viabilidade econômica para aprovação do investimento; a Controladoria exige alocação de custos (DS6); e a Auditoria determina a adequação de controles internos (M2).

Os resultados da pesquisa evidenciaram um desconhecimento da teoria que suporta a aplicação de melhores práticas, metodologias, ferramentas e critérios de avaliação, visando à elevação dos níveis de maturidade dos processos que compõem a Governança de TI. Nenhuma das organizações pesquisadas possuía técnicos sendo treinados ou em fase de certificação no ITIL® ou no CobiT®, com o objetivo de aplicar em projetos na organização. Tais resultados invalidaram a hipótese **H₃**. Estes resultados corroboram a pesquisa *CIO Metrics* (IDC, 2004) relatados na seção 1.

De modo geral, os dados obtidos no estudo indicam que as organizações pesquisadas ainda não estão se preparando para adequação aos regulamentos e recomendações na área de TI e, como consequência, pode haver impactos na agregação de valor da empresa decorrentes da Lei *Sarbanes-Oxley* e da Cartilha de recomendações de boas práticas de

governança corporativa da CVM. As medidas de dispersão demonstram uma homogeneidade em quase todos os itens pesquisados (Gráfico 2).

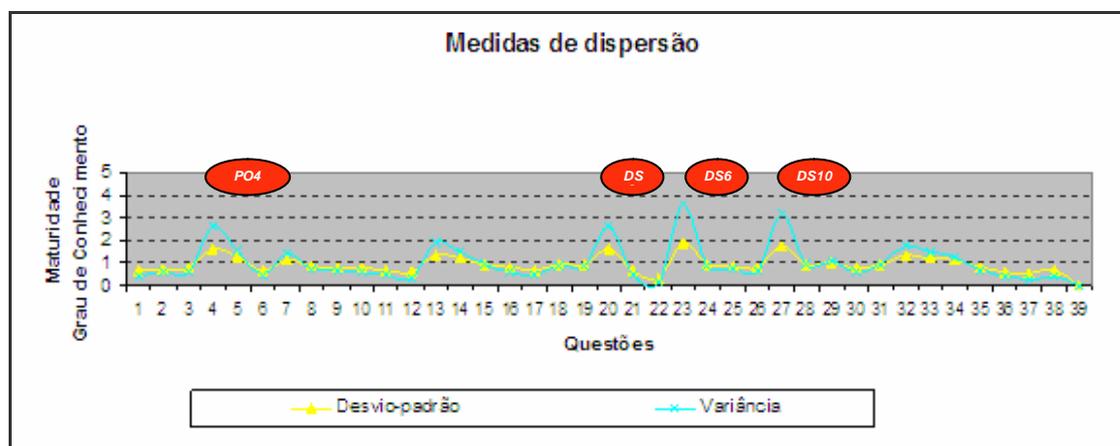


Gráfico 2 – Medidas de dispersão

Baseada no estudo das referências bibliográficas que fundamentaram este trabalho e na experiência dos pesquisadores, a implantação de guias de melhores práticas em organizações de grande porte pode demandar em média dois anos. Os resultados obtidos no estudo de caso ficaram aquém das expectativas dos pesquisadores reportadas nas três hipóteses definidas na introdução. Esperava-se um maior grau de conscientização da importância do problema, e também uma mobilização mais significativa.

Referências bibliográficas

BRITISH STANDARD. **BS 7799-1:1999. Information security management – Part 1: code of practice for information security management.** BSI/DISC Committee BDD/2. London: 1999.

BRITISH STANDARD. **BS 15000-1:2002. IT service management – part 1: specification for service management.** Technical Committee BDD/3 – Information services management. London: 2002.

BRITISH STANDARD. **BS 15000-2:2003. IT service management – part 2: code of practice for service management.** Technical Committee BDD/3 – Information services management. London: 2003.

BROADBENT, M. Tailor IT governance to your Enterprise. **Gartner.** Disponível em <http://www.itsmf.it/download/PAGINE_BIANCHE/Gartner.ppt>. Acesso em 05 dez. 2005.

COEN, G; RUBINATO FILHO, S. **itSMF no Brasil.** In: IT Service Management Forum. Disponível em <<http://www.itsmf.com.br>>. Acesso em 07 jun. 2005.

COMISSÃO DE VALORES MOBILIÁRIOS. **Recomendações da CVM sobre Governança Corporativa.** São Paulo: 2002.

FERNANDES, J. H. C. **Para onde seguem os modelos de qualidade de TI e software: relação entre os modelos CMMI, CobiT®, ITIL® e SPICE.** Simpósio Brasileiro de Engenharia de Software, 2004.

IDC. **Pesquisa CIO metrics - 2004.** Disponível em <<http://idc.com>>. Acesso em 30 jun. 2005.

IDC. **Pesquisa IT fórum - 2005.** Disponível em <<http://idc.com>>. Acesso em 30 jun. 2005.

INFORMATION SYSTEM AUDIT & CONTROL ASSOCIATION. **CobiT®: control objectives for enterprise governance.** Illinois: IT Governance Institute, 1999.

INFORMATION SYSTEM AUDIT & CONTROL ASSOCIATION. **IS standards, guidelines and procedures for auditing and control professionals**. Illinois: ISACA, 2005.

INTERNATIONAL STANDARDS ORGANISATION. **ISO/IEC 17799:2000: code of practice for information security management**. Switzerland: ISO, 2000.

IT GOVERNANCE INSTITUTE. Disponível em <<http://www.itgovernance.org>>. Acesso 21 abr. 2005.

IT GOVERNANCE INSTITUTE. **Board briefing on IT governance**. Illinois: IT Governance Institute, 2003.

IT GOVERNANCE INSTITUTE. **CobiT® framework**. Illinois: IT Governance Institute, 2000.

LAPPONI, J. C. **Estatística usando o Excell**. Rio de Janeiro: Elsevier, 2005.

MCDANIEL, C. D.; GATES, R. **Pesquisa de marketing**. São Paulo: Pioneira Thomson Learning, 2003.

OFFICE OF GOVERNMENT COMMERCE. **An introduction to ITIL®**. London: TSO, 2004.

OFFICE OF GOVERNMENT COMMERCE. **Best practice for ICT infrastructure management**. ITIL®. London: TSO, 2004a.

OFFICE OF GOVERNMENT COMMERCE **Best practice for planning to implement service management**. ITIL®. London: TSO, 2005.

OFFICE OF GOVERNMENT COMMERCE **Best practice for service delivery**. ITIL®. London: TSO, 2005a.

OFFICE OF GOVERNMENT COMMERCE **Best practice for security management**. ITIL®. London: TSO, 2004b.

OFFICE OF GOVERNMENT COMMERCE **Best practice for service support**. ITIL®. London: TSO, 2004c.

SARBANES-OXLEY ACT. **Congress of the United States of America**. Washington: 2002.

SEBRAE. **Boletim Estatístico de micro e pequenas empresas**. Observatório Sebrae, 2003. Disponível em <http://www.sebrae.com.br/br/mpe_numeros/>. Acesso em 02 nov. 2005.

SIQUEIRA FILHO, J. B.; SILVA FILHO, J.B. **Tecnologia da informação para administradores**. Fortaleza: Universidade de Fortaleza, 2004.

SPIEGEL, M. R. **Estatística: resumo da teoria, 875 problemas resolvidos, 619 problemas propostos**. Coleção Schaum. São Paulo: McGraw-Hill do Brasil, 1976.

TEIXEIRA JÚNIOR, F. **Alinhamento estratégico entre os negócios e a tecnologia da informação (TI): Estudo de Caso em uma Instituição Financeira**. Dissertação (Mestrado em Administração de Empresas) – Universidade de Fortaleza, Fortaleza, 2003.

TOFFLER, A. **A empresa flexível**. Rio de Janeiro: Record, 1985.

ⁱ O somatório de todos os valores inferiores ao limite superior de um dado intervalo de classe é denominado frequência acumulada até e inclusive aquele intervalo (SPIEGEL, 1976).

ⁱⁱ Mede a dispersão de uma distribuição da frequência, correspondendo à raiz quadrada da média das diferenças individuais em relação à média aritmética (MCDANIEL; GATES, 2003).