

Implementando governança de TI usando modelos de maturidade

Prof. Me. Paulo Medina Corrêa (CEETEPS) paulomedina@yahoo.com

Prof. Dr. Napoleão Galegale (CEETEPS) nvg@galegale.com.br

Resumo: *Esse trabalho contribui para a discussão sobre o processo que emerge como necessidade natural nas empresas - governança de TI - processo esse que se localiza dentro de um contexto mais amplo de governança corporativa. Esse estudo está focado em uma das ferramentas do CobiT 3ª Edição - Management Guidelines - que por meio de modelos classifica os níveis de maturidade dos processos de TI. Realizou-se um estudo de caso em uma empresa de tecnologia, mais especificamente em seu Centro de Certificação Digital, procurou-se entender como os níveis de maturidade podem contribuir para iniciar o processo de implantação de governança de TI. Ou seja, por meio de uma análise de gap, classificando o nível de maturidade atual dos processos de TI, é possível projetar em que nível de maturidade deseja-se chegar nesses processos, definindo assim o modelo de gestão e suas métricas. Na conclusão, analisou-se os resultados dos processos de TI avaliados e a projeção feita pelos responsáveis pela gestão e operação dessa unidade de negócio.*

Palavras-chave: Governança de TI; Nível de maturidade; Processos de TI; CobiT,

a) Introdução

Governança de TI é um tema que vem sendo amplamente discutido nos mais variados fóruns. Apesar de ser tratado de maneira informal há muito tempo, somente nos últimos anos vem ganhando destaque.

Dentro do contexto de governança corporativa, que é um conceito que sustenta a transparência das operações para os investidores, clientes, empregados, fornecedores, credores e a própria comunidade, vem inserida a governança de TI.

A origem da Governança Corporativa está diretamente relacionada à teoria da agência onde Jensen e Meckling (1976) definem o relacionamento de agência como um contrato onde uma ou mais pessoas, principal ou principais, contratam alguém (agente) para realizar algum serviço em seu nome, isso envolve delegar autoridade para o agente na tomada de decisões, o que pode causar conflito de interesses entre as partes relacionadas. [11]

Segundo Silveira (2002) o raciocínio da teoria da agência é baseado na relação entre agentes e principais, nas quais os agentes representam, em tese, os interesses dos principais. É o caso, por exemplo, do acionista (o principal, nesse caso) e do administrador (agente) de uma organização. O problema de agência ocorre quando o agente, que deveria agir sempre no melhor interesse do principal (razão pelo qual é contratado), age tendo em vista o seu melhor interesse, isto é, tendo em vista maximizar sua utilidade pessoal. Como não há conflitos de interesses

possíveis quando o mesmo indivíduo acumula as funções de acionista e administrador, o problema de agência surge na medida em que a propriedade e controle se separam.

Diante desse quadro, em 1998 foi criado o *IT Governance Institute*, organização sem fins lucrativos, que tem por missão desenvolver um entendimento avançado, promover boas práticas, influenciar positivamente a governança de TI da alta administração até os técnicos de TI.

Por definição do *IT Governance Institute*:

Governança de TI é responsabilidade do quadro de diretores e da gerência executiva. É parte integral da governança corporativa e consiste da direção, estrutura organizacional e processos que asseguram que Tecnologia da Informação sustenta e amplia os objetivos e estratégias organizacionais.(GULDENTOPS *et al*, 2000). [4]

A governança de TI não é uma disciplina ou atividade isolada e tem como propósito direcionar o desempenho e o alinhamento de tecnologia com os negócios. Hoje a tecnologia da informação faz parte da estratégia das empresas, bem como a implementação de governança de TI. Em 2005, o *IT Governance Institute* conduziu uma pesquisa sobre a conscientização, percepção e aplicação de governança de TI e *frameworks* associados. Trata-se de uma pesquisa global entre empresas do segmento financeiro, telecomunicações, manufatura, varejo e setor público onde os respondentes foram *Chief Executive Officers* (CEO), *Chief Financial Officer* (CFO) e *Chief Information Officer* (CIO), ou seja, membros da alta administração. JOHNSON *et al*(2006). Vide figura 1. [12]

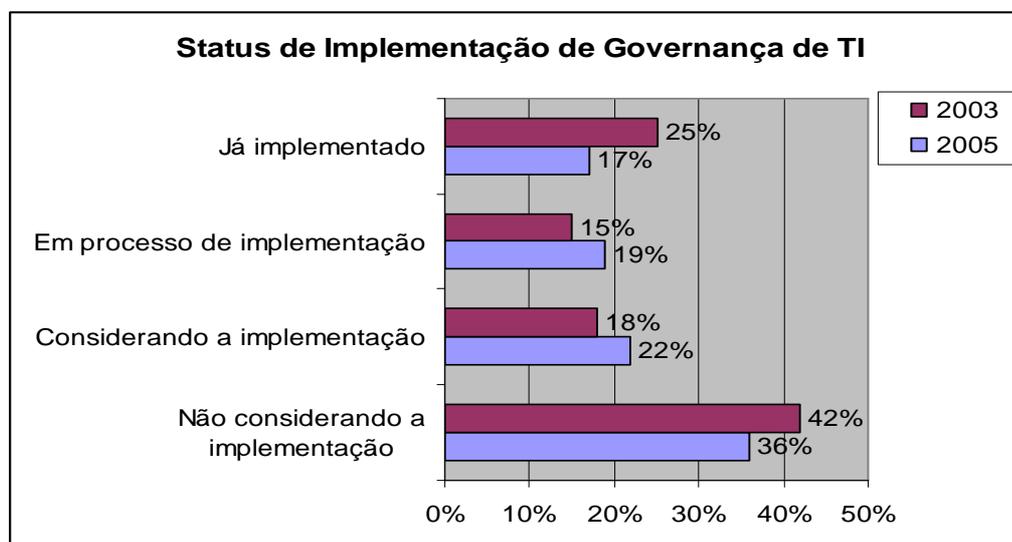


FIGURA 1 – Status da Implementação de Governança de TI nas empresas
Fonte: JOHNSON *et al* (2006) [12]

É possível observar na figura 1 que a porção de empresas que tem o processo de governança implementado diminui em 2005, por outro lado as empresas que não consideram a implementação diminuíram.

Na figura 2 observa-se o desdobramento da implementação de governança de TI por setor. A área de serviços financeiros é líder em termos de processo de governança de TI já implementado, no varejo é onde se concentra a maior tendência de implementação de governança de TI.

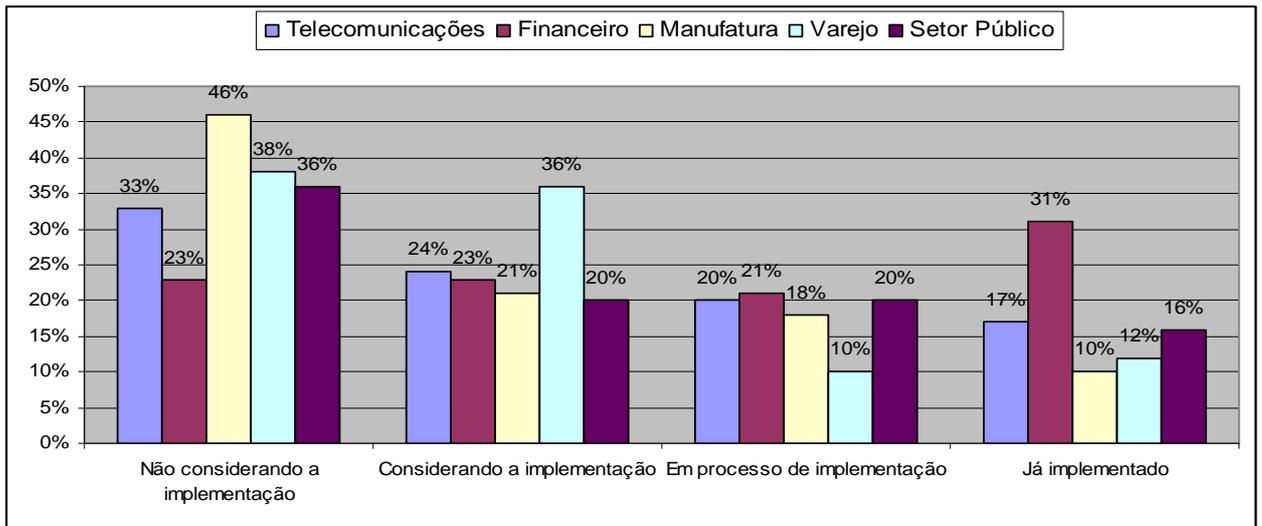


FIGURA 2 – Status da Implementação de Governança de TI – Por Setor da Indústria
 Fonte: JOHNSON *et al* (2006)

O CobiT vem sendo adotado como *framework* para governança de TI por ser reconhecido internacionalmente e por auxiliar no entendimento e gerenciamento dos riscos envolvidos em tecnologia. Apesar dessas características a sua aplicação não é elementar e muitos entendem que o CobiT não é um modelo fechado. A figura 3 mostra a dificuldade de implementação do CobiT.

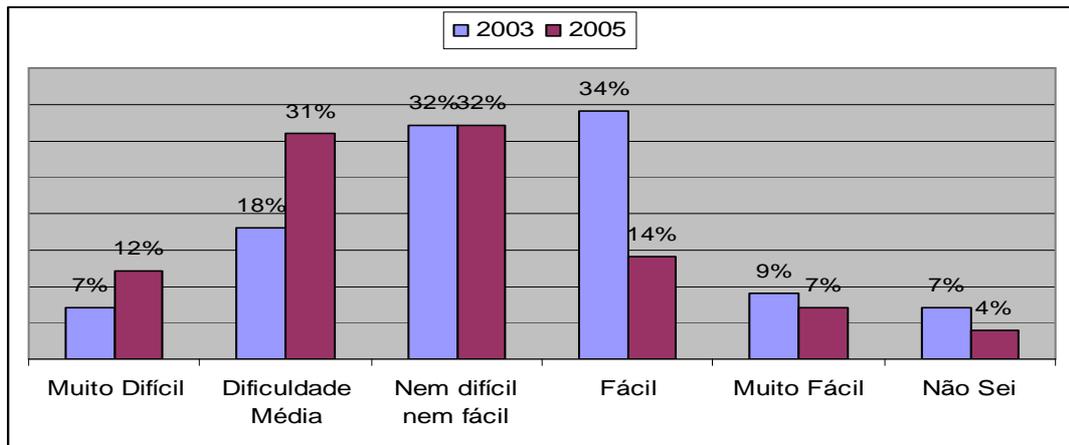


FIGURA 3 – Dificuldade na Implementação do CobiT
 Fonte: JOHNSON *et al* (2006)

Por outro lado considera-se que o CobiT agrega valor nos esforços de governança de TI, conforme mostra a figura 4, todavia não há necessidade de implementá-lo por completo. O CobiT pode ser implementado parcialmente e adaptado de acordo com a situação. O CobiT não é uma receita pronta e sim uma estrutura para gestão de TI que pode e deve ser complementada por outros *frameworks*, metodologias, normas e boas práticas de mercado.

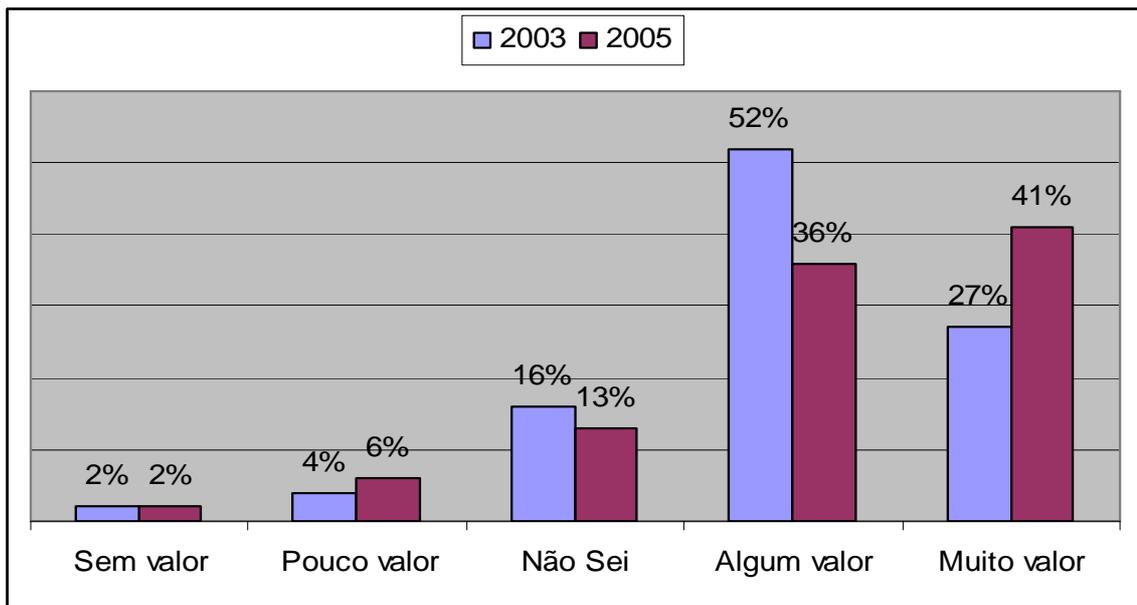


FIGURA 4 – Valor do CobiT nos esforços de Governança de TI
 Fonte: JOHNSON *et al* (2006)

De maneira geral, as empresas tentam implementar um processo consistente de governança de TI, mas esbarram no método de implementação, muitas vezes desistindo do projeto no meio do caminho ou contratando consultorias especializadas para tal finalidade. A necessidade é clara, as empresas precisam gerir e medir de forma mais eficiente a Tecnologia da Informação.

Considerando a implementação de um processo de governança de TI, a dúvida que surge é por onde começar.

Os modelos de maturidade, que se encontram no CobiT na parte do *Management Guidelines*, podem ser o primeiro passo para a implementação de um processo de governança de TI. O processo de implementação de governança de TI que é proposto pelo *IT Governance Implementation Guide* (GULDENTOPS *et al*, 2003b) sugere 4 etapas. [6]

- a) Identificação das necessidades;
- b) Idealização da Solução;
- c) Solução do Plano;
- d) Implementação da Solução.

Atualmente, a maior preocupação das empresas é com a operação e controle do ambiente de tecnologia da informação, sendo desconsiderada uma gestão eficaz com foco em riscos, essa postura causa muita confusão na concepção exata de governança de TI.

b) Metodologia

O objetivo desse estudo está situado na segunda etapa do *IT Governance Implementation Guide* (GULDENTOPS *et al*, 2003b), chamada de idealização da solução, ou seja, por meio da aplicação de um questionário com embasamento nos modelos de maturidade do CobiT versão 3, avaliar o resultado do nível atual dos processos de TI selecionados e do nível a ser atingido, bem como efetuar uma análise de *gap* que poderá direcionar a implementação de um processo de governança de TI. Vide figura 5. [6]

Identificação das necessidades

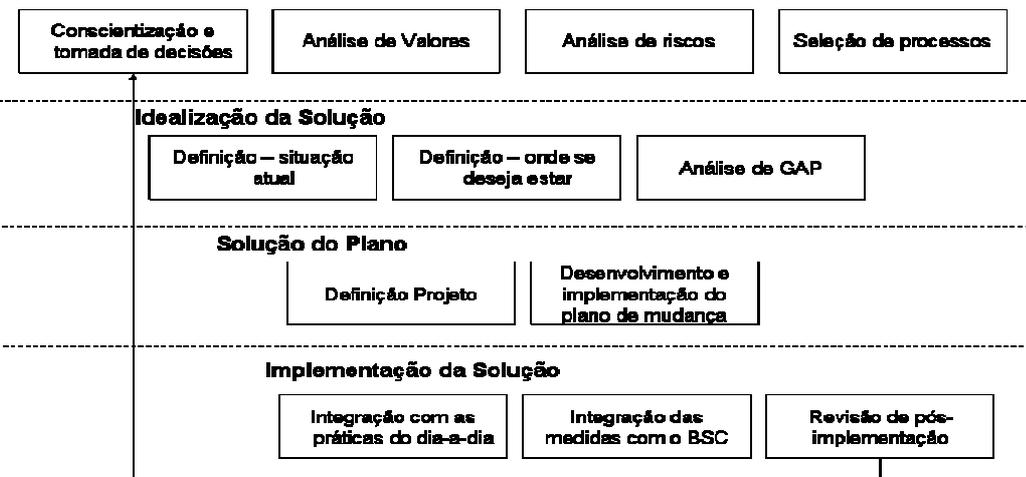


FIGURA 5 - Fases e passos de implementação de governança de TI

Fonte: GULDENTOPS *et al*, 2003b [6]

O estudo delimitou-se a pesquisar os principais processos de Tecnologia da Informação de uma empresa de tecnologia. Dessa forma, identificou-se como objeto de estudo uma autoridade certificadora que não possuía um processo formal de governança de TI. A pesquisa foi realizada junto à unidade operacional dessa linha de negócio.

Adotou-se como modalidade de pesquisa o estudo de caso, pois trata de questões do tipo como e por que. Segundo Yin (2005) tais questões lidam com ligações operacionais que necessitam ser traçadas ao longo do tempo, em vez de serem encaradas como meras repetições e incidências. [15]

Propósito do estudo de caso - A pergunta como pode ser formulada da seguinte maneira: Como iniciar um processo de governança de TI? E teria como resposta: Utilizando modelos de maturidade. Para a pergunta por que a formulação seria a seguinte: Por que modelos de maturidade? Resposta: Usando esses modelos é possível situar o nível de maturidade dos processos de TI e projetar o nível a que se deseja chegar. Dessa forma, o questionário aplicado teve os seguintes objetivos:

- a) Proporcionar um primeiro contato dos respondentes com os modelos de maturidade;
- b) Fazer com que os respondentes reflitam em relação ao nível de maturidade atual dos principais processos de TI;
- c) Fazer com que os respondentes projetem o nível de maturidade desejado para os processos de TI em questão;
- d) Coletar dados para análise dos níveis de maturidade;
- e) Validar os modelos de maturidade como ferramenta de implementação de um processo de governança de TI.

Segundo Yin, 2005 uma das mais importantes fontes de informações para o estudo de caso são as entrevistas. É comum que as entrevistas para o estudo de caso sejam conduzidas de forma espontânea. Dessa forma, pode-se indagar dos respondentes-chave tanto os fatos relacionados a um assunto quanto pedir a opinião deles sobre determinados eventos. [15]

c) Resultados

Partindo-se dessa definição e seguindo a metodologia proposta por Guldentops *et al* (2003b) no *IT Governance Implementation Guide*, antes de se definir a situação atual, é necessário que previamente seja realizado um entendimento dos valores e direcionadores de negócio para assegurar que os processos críticos de TI sejam selecionados. Nesse trabalho assumiu-se que 7 processos que estão relacionados a planejamento estratégico, gerenciamento de riscos, gerenciamento de projetos, gerenciamento de mudanças, segurança, gerenciamento de dados e monitoramento dos processos são os críticos.

Para a definição da situação atual foi elaborado um questionário de múltipla escolha tendo como base o nível de maturidade do *Management Guidelines* do CobiT, relacionado aos processos selecionados, onde cada um dos participantes, em sua opinião, indicou o nível de maturidade atual de cada processo.

Para se definir a situação a ser atingida foi incluída uma questão de múltipla escolha, que foi elaborada com base no modelo genérico de maturidade, onde cada um dos participantes, em sua opinião, indicou o nível de maturidade a ser atingido.

Os participantes foram selecionados de acordo com a relação das atividades executadas e diretamente relacionadas à gestão e operação da Autoridade Certificadora.

O perfil dos dos participantes apresentam as seguintes características: média de idade dos participantes é de 43,6 anos, onde 60% possui formação de nível superior.

Na figura 6, a representação gráfica da análise de *gap* efetuada demonstra uma visão geral sobre o nível de maturidade de cada processo avaliado e o nível de maturidade a ser atingido, nível 4.

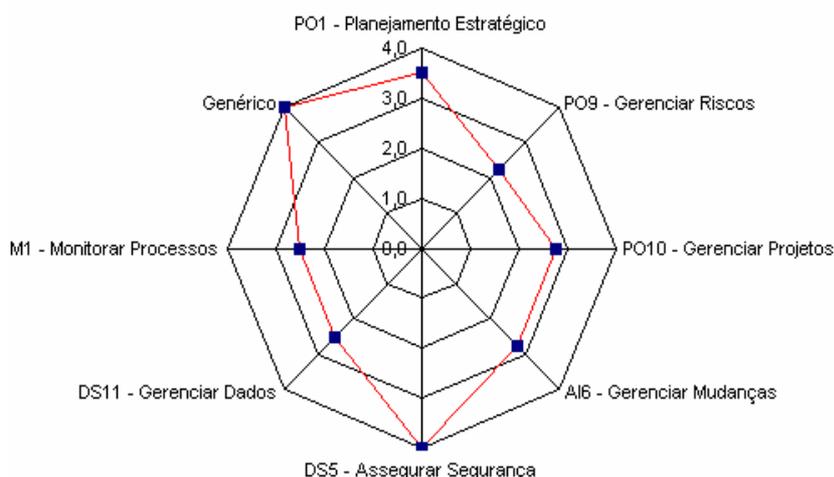


FIGURA 6 - Estudo do nível de maturidade dos processos de TI em uma Autoridade Certificadora
Fonte: o Autor [2]

Com o resultado obtido analisa-se separadamente cada processo em relação ao nível de maturidade atual e a maturidade requerida.

No processo referente ao planejamento estratégico (PO1) as respostas mantiveram uma proximidade e os participantes atribuíram nível de maturidade entre três e quatro, totalizando uma média de 3,5; onde o nível três define que existe uma política que regulamenta a realização desse processo e que segue uma abordagem

estruturada com embasamento e assegura que um plano está sendo realizado de maneira apropriada.

O nível quatro diz que deve haver uma prática padrão, mas exceções podem ser notadas. Uma função sênior é responsável pelo processo que pode ser monitorado e as informações relativas a decisões são feitas com base em medições de eficácia.

Em relação ao processo gerenciamento de risco (PO9) as respostas foram divergentes e calculou-se uma média 2,3. Considerando que o nível de maturidade dois define que existe um emergente entendimento que o gerenciamento dos riscos de TI é importante e deve ser considerado. Existe uma abordagem ainda imatura, pois é realizada sem muita profundidade e somente em projetos maiores.

O gerenciamento de projeto (PO10) foi avaliado com média 2,8, ou seja, necessita de pequenos ajustes para atingir o nível três, que define o processo e a metodologia, com base em objetivos técnicos e de negócios apropriados e devidamente comunicados a empresa.

O processo de gerenciamento de mudanças (AI6) tem a mesma média apontada no processo anterior 2,8. Após alguns ajustes o processo estará definido incluindo: categorização, priorização, procedimentos de emergência, autorização de mudanças e gerenciamento de versões, mas não haverá total aderência e erros ainda poderão ocorrer.

O processo relacionado à segurança dos sistemas (DS5) foi o item que recebeu a maior classificação na escala de maturidade, atingindo média 4. O principal motivo são os inúmeros itens de segurança física exigidos pelo ITI Brasil, órgão responsável pelo credenciamento de autoridades certificadoras. No nível de maturidade quatro as responsabilidades estão claramente definidas, gerenciadas e reiteradas. Os riscos de TI e análise de impacto são consistentemente realizados. Políticas e práticas de segurança são complementadas por bases específicas.

O gerenciamento de dados (DS11) atingiu média 2,5. Ou seja, atende a todos requisitos de nível dois que são: a conscientização da necessidade da precisão dos dados e manutenção da integridade que prevalecem por toda organização. As regras e requerimentos estão documentados para indivíduos-chaves e não estão consistentes pela organização e plataformas. Alguns itens do nível três também são atendidos.

A monitoração dos processos (M1) obteve também uma média 2,5. E atualmente, atende aos seguintes itens: existem medidas básicas de monitoração, definição de técnicas e métodos de avaliação e coleta, mas esse processo ainda não foi adotado por toda a organização.

De maneira geral todos os participantes entendem que devem evoluir para um nível de maturidade quatro nos processos avaliados. O modelo genérico de maturidade nível quatro sugere que deve ser possível monitorar os processos, medir sua aderência com os procedimentos e tomar ações corretivas onde pareçam não funcionar de maneira efetiva. Os processos devem estar em constante melhoria e provendo boas práticas. Nesse nível a automação e ferramentas devem ser usadas de maneira limitada.

Em suma, pode-se concluir que o objetivo do trabalho foi atingido, ou seja, a aplicação do questionário sobre nível de maturidade, obtenção do posicionamento do nível atual dos processos de TI e projeção do nível ideal para a indústria de certificação digital, bem como conhecer a percepção dos entrevistados em relação ao modo de aplicação do questionário.

É importante ressaltar que quanto maior o nível de maturidade almejado, maior o tempo de implementação e maior investimento é necessário, pois isso implica na implementação ou adequação de procedimentos e controles para atender a todos os requisitos de um nível para atingir o próximo nível. [2]

d) Discussão e conclusões

Para que esse estudo fosse possível foi necessário encontrar um grupo de pessoas disposto a colaborar com a pesquisa, haja vista que anteriormente uma série de organizações, associações e empresas foram procuradas e não se mostraram receptivas para tal contribuição. Por outro lado, os funcionários da empresa que foi objeto desse estudo foram extremamente cooperativos, abertos e disponíveis para essa realização.

Por meio dessa valiosa contribuição foi possível atingir plenamente os objetivos propostos inicialmente que eram de avaliar a aplicabilidade e a aceitação do nível de maturidade proposto pelo CobiT, como forma de direcionar a implementação de um processo de Governança de TI, através da aplicação de um questionário sobre nível de maturidade dos processos de TI, de acordo com os seguintes itens:

- a) Avaliação dos processos do CobiT versão 3:
 1. PO1 - Definição do Plano Estratégico de TI;
 2. PO9 - Gerenciamento de riscos;
 3. PO10 - Gerenciamento de Projetos;
 4. AI6 - Gerenciamento de Mudanças;
 5. DS5 - Garantia de Segurança para Sistemas;
 6. DS11 - Gerenciamento de Dados;
 7. M1 - Monitoramento dos Processos.
- b) Consideração dos níveis de maturidade do *Management Guidelines*, nas dimensões Entendimento & Conscientização e Processos & Práticas.
- c) Aplicação do questionário na unidade de certificação digital de uma grande empresa de tecnologia.

Partindo dessa análise é possível comprovar a adaptabilidade do CobiT o que dispensa a aplicação total do *framework*.

Observou-se nesse estudo que o nível de maturidade encontrado no módulo *Management Guidelines* do CobiT é um método que pode ser utilizado como início de um processo de governança de TI, pois permite discussões entre os diversos setores da empresa. Proporciona a medição e referência do nível de maturidade dos processos de TI. A partir daí pode-se definir para que nível de maturidade os processos devem caminhar, bem como definir os planos de ação necessários.

Os resultados obtidos no estudo permitiram identificar que é possível classificar o nível de maturidade por meio das características descritas. Proporcionando ao participante do estudo uma visão mais ampla do processo de TI avaliado.

Em uma autoridade certificadora, os processos de TI são fundamentais para a o objetivo final que é a emissão de certificados digitais com credibilidade tanto nos processos administrativos como nos processos de TI.

Em relação às respostas obtidas houve algumas divergências. Alguns dos participantes não se sentiram confortáveis ao responder algumas das questões

propostas, pois não participam direta ou indiretamente de alguns processos, dessa forma a resposta indicada foi apenas uma inferência.

A forma proposta pelos participantes para sanar as divergências, de maneira unânime, seria por meio de uma reunião no formato *workshop* com a presença dos responsáveis de negócio, para a discussão e alinhamento da classificação dos níveis de maturidade dos processos selecionados.

Essa proposta vai ao encontro do que propõe o IT Governance Institute na 2ª Edição do Board Briefing on IT Governance:

Para uma efetiva Governança de TI ser implementada a empresa deve avaliar como está seu desempenho atual e identificar onde e quais melhorias podem ser feitas. Isso se aplica aos próprios processos de governança e todos os processos que precisam ser gerenciados dentro de TI. O uso dos modelos de maturidade simplifica essa tarefa e fornece uma abordagem pragmática e estruturada para medir quão bem os processos estão desenvolvidos numa escala de fácil entendimento. GULDENTOPS *et al* (2003a). [3]

Vale ressaltar, que na ocasião, o processo de governança de TI não foi implementado, mas motivou uma série de discussões com relação aos níveis de maturidade podendo ser utilizado futuramente como modelo para melhoria dos processos.

Não existe a pretensão de esgotar esse assunto e sim contribuir para o enriquecimento dos estudos, como por exemplo, sugerir uma outra forma de iniciar o processo de governança de TI.

Esse estudo pode ser ampliado e detalhado, incluindo:

- a) As demais dimensões do nível de maturidade (Treinamento & Comunicação, Técnicas & Automação, Conformidade e Competência),
- b) Os demais 27 processos de TI descritos pelo CobiT;
- c) A nova versão do CobiT (CobiT 4).
- d) A participação de auditorias externas para validar o processo da aplicação do modelo de maturidade.

Se forem realizados novos estudos como propostos nos itens acima, certamente haverá um aprofundamento e novas contribuições nos estudos em Governança de TI.

e) Referências

[1] CASCIANO, D. *et al.* **COBIT 4.0**. 4 ed. Rolling Meadows, Illinois – USA.:Information Systems Control Association, 2005

[2] CORRÊA, P. M. **Um Estudo sobre a Implementação da Governança de TI com Base em Modelos de Maturidade**. 2006. 94f. Tese (Mestrado) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2006

[3] GULDENTOPS, E.*et al.* **Board Briefing on IT Governance**, 2 ed. Rolling Meadows, Illinois – USA.. Information Systems Control Association, 2003a.

[4] _____.**COBIT - Control Objectives for Information and related Technology**, 3 ed. Rolling Meadows, Illinois – USA. Information Systems Control Association, 2000

- [5] _____. **IT Control Maturity Survey**. In: IG_Surveys. CD Supplemental Tools and Materials. (Transparência). IT Governance Implementation Guide. IT Governance Institute, 2003.
- [6] _____. **IT Governance Implementation Guide**, Rolling Meadows, Illinois – USA. IT Governance Institute, 2003b.
- [7] GULDENTOPS, E. **Maturity Measurement – First the Purpose Then the Method**,.In: Information Systems Control Journal. Rolling Meadows, Illinois-USA. Volume 4.p.15 -16. jul.2003.
- [8] GULDENTOPS, E., GREMBERGEN, W.V. e HAES, S. DE. **Control and Governance Maturity Survey: Establishing a Reference Benchmark and Self Assessment Tool**. In: Information Systems Control Journal. Rolling Meadows, Illinois – USA,.Volume 6. p.32 -35.nov.2002
- [9] GULDENTOPS, E. e HAES S.DE. **CobIT 3rd Edition Usage Survey: Growing Acceptance of Cobit**. In:Information Systems Control Journal.Rolling Meadows. Illinois – USA., Volume 6. p.25-26. nov.2002
- [10] HAMAKER, S. e HUTTON, A. **Principles of IT Governance**. In:Information Systems Control Journal. Rolling Meadows, Illinois – USA., Vol 3, p.44 -49. mai.2003
- [11] JENSEN, M. C. e MECKLING, W.H, **Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure**, Harvard University Press, 2000, disponível em <<http://hupress.harvard.edu/catalog/JENTHF.html>>, acesso em 15/01/2006
- [12] JOHNSON, E. *at al.* **IT Governance Global Status Report - 2006**, Rolling Meadows. Illinois – USA. 2006
- [13] PEDERIVA, A. **The CobIT Maturity Model in a Vendor Evaluation Case**. In:Information. Systems Control Journal. Rolling Meadows, Illinois – USA.. Vol. 3. p.26 -29. jun.2003
- [14] SILVEIRA, A. DI M. **Governança Corporativa Desempenho e Valor da Empresa no Brasil**. 2002. 165f. Tese (Mestrado) - Universidade de São Paulo, São Paulo, 2002
- [15] YIN, R. K. **Estudo de Caso: Planejamento e Métodos**. 3 ed. Porto Alegre: Bookman, 2005

f) Contato

Paulo Medina Corrêa
R. dos Bandeirantes, 169 - Bom Retiro - São Paulo/ SP
Cep 01124-010
Tel: (11) 8175-1189
paulomedina@yahoo.com