CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

PAULO MEDINA CORRÊA

UM ESTUDO SOBRE A IMPLANTAÇÃO DA GOVERNANÇA DE TI COM BASE EM MODELOS DE MATURIDADE

SÃO PAULO

JUNHO, 2006

Paulo Medina Corrêa

UM ESTUDO SOBRE A IMPLANTAÇÃO DA GOVERNANÇA DE TI COM BASE EM MODELOS DE MATURIDADE

Dissertação apresentada como exigência parcial para obtenção do Título de Mestre em Tecnologia no Centro Estadual de Educação Tecnológica Paula Souza, no Programa de Mestrado em Tecnologia: Gestão Desenvolvimento e Formação, sob orientação do Prof. Dr. Napoleão Verardi Galegale.

São Paulo

Junho, 2006

C824u Corrêa, Paulo Medina
Um estudo sobre a implantação da governança de TI com base em modelos de maturidade / Paulo Medina Corrêa. -- São Paulo, 2006.
94 f.

Dissertação (Mestrado) – Centro Estadual de Educação Tecnológica Paula Souza, 2006.

1. Governança corporativa. 2. Nível de maturidade. I. Título.

CDU 681.3:007

Paulo Medina Corrêa

UM ESTUDO SOBRE A IMPLANTAÇÃO DA GOVERNANÇA DE TI COM BASE EM MODELOS DE MATURIDADE

_____

Prof. Dr.Napoleão Verardi Galegale

_____

Prof. Dr.Carlos Hideo Arima

_____

Prof. Dr. Aristides Novelli Filho

São Paulo, 30 de junho de 2006

DEDICATÓRIA

A minha esposa, idealizadora e cúmplice desse momento, leitora e revisora incansável, e meu filho, razões de todos meus objetivos.
Aos meus pais que me ensinaram a necessidade de procurar o caminho do conhecimento.

“O temor do Senhor é o princípio da ciência: os loucos desprezam a sabedoria e a instrução”.
Provérbios de Salomão (1:17)

AGRADECIMENTOS

Agradeço ao meu orientador por me incentivar durante a elaboração do trabalho.
Agradeço aos funcionários do Centro de Certificação Digital pela disposição e prontidão em participar desse estudo.
Enfim agradeço a todas as pessoas que de forma direta ou indireta tornaram possível a elaboração deste trabalho.

RESUMO

CORRÊA, P.M.. **Um Estudo sobre a Implantação da Governança de TI com base em Modelos de Maturidade**. 2006. 94 f. Dissertação (Mestrado em Tecnologia) - Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2006.

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. Por meio de 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, *Management Guidelines*.

ABSTRACT

CORRÊA, P.M.. **Um Estudo sobre a Implantação da Governança de TI com base em Modelos de Maturidade**. 2006. 94 f. Dissertação (Mestrado em Tecnologia) - Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2006.

This work contributed to the discussion of a process that emerges naturally at companies - IT governance. This process is embedded in a wider context, which is called "Corporate Governance". This study focuses on one of the CobiT 3rd edition tools - Management Guidelines - that, throughout the models, classifies the IT process maturity. Based on a case study in a technology company, more specifically at its Digital Certification Centre, we looked to understand how the maturity models can contribute to initiate the IT Governance implementation process. Using a gap analysis and classifying the current maturity level of the IT processes, it is possible to define the desired maturity level. Analysis were performed over the results of the IT processes that were evaluated as well as over the desired maturity levels defined by the people responsible for the management and for the operation of this business unit.

Keywords*:* IT Governance; Maturity Models, IT processes, CobiT, Management Guidelines.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AC – Autoridade Certificadora

BOVESPA – Bolsa de Valores de São Paulo

CCD – Centro de Certificação Digital

CEO – *Chief Executive Officer*

CIO – *Chief Information Officer*

CFO – *Chief Financial Officer*

CobiT – Control Objectives for Information and related Technology

CSF (Critical Sucess Factor) – Fatores críticos de sucesso

CVM – Comissão de Valores Mobiliários

DPC – Declaração de Política de Certificação

ITI – Instituto de Tecnologia da Informação

ITI – *IT Governance Institute*

ISACA – *Information Systems Audit and Control Association*

ECT – Empresa Brasileira de Correios e Telégrafos

KGI (Key Goal Indicator) – Indicadores de metas

KPI (Key Performance Indicator) – Indicadores de desempenho

LCR – Lista de certificados revogados

LSC – Learning and Skills Council

PC – Política de Certificação

SGCD – Sistema de Gerenciamento de Certificação Digital

SO – Sistema Operacional

TI – Tecnologia da Informação

SUMÁRIO

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.

Governança de TI vem inserida no contexto da governança corporativa que é um conceito que sustenta a transparência das operações para os investidores, clientes, empregados, fornecedores, credores e a própria comunidade.

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.

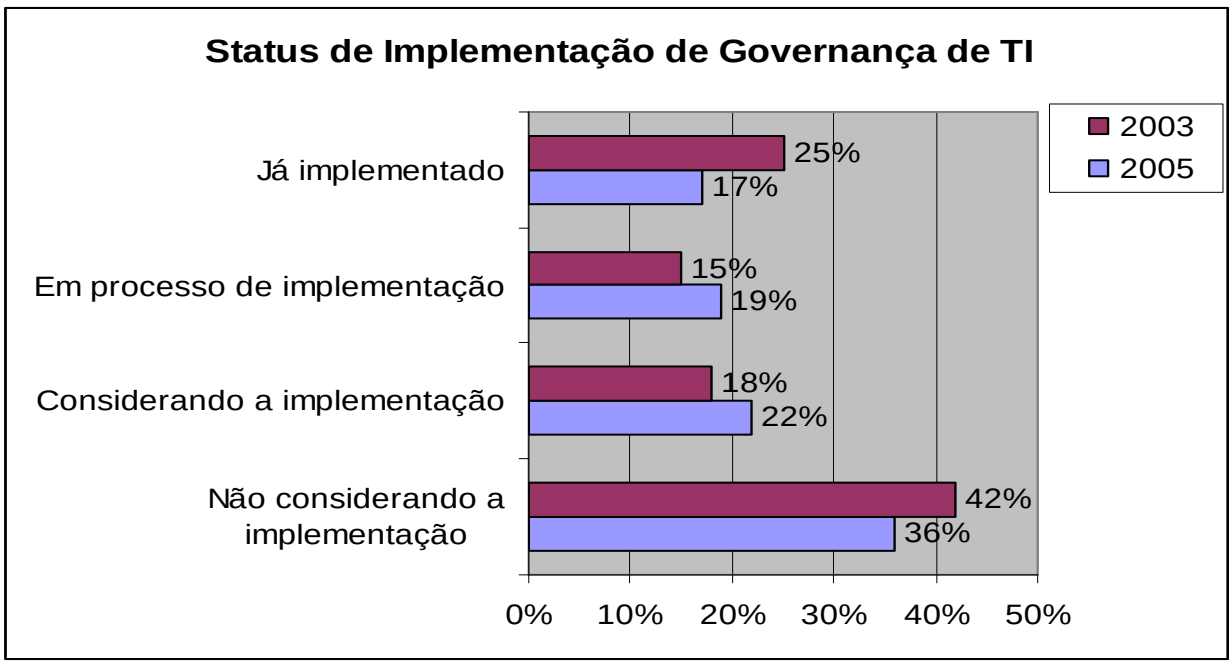

FIGURA 1 – Status da Implementação de Governança de TI
Fonte: IT Governance Institute, 2006

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.

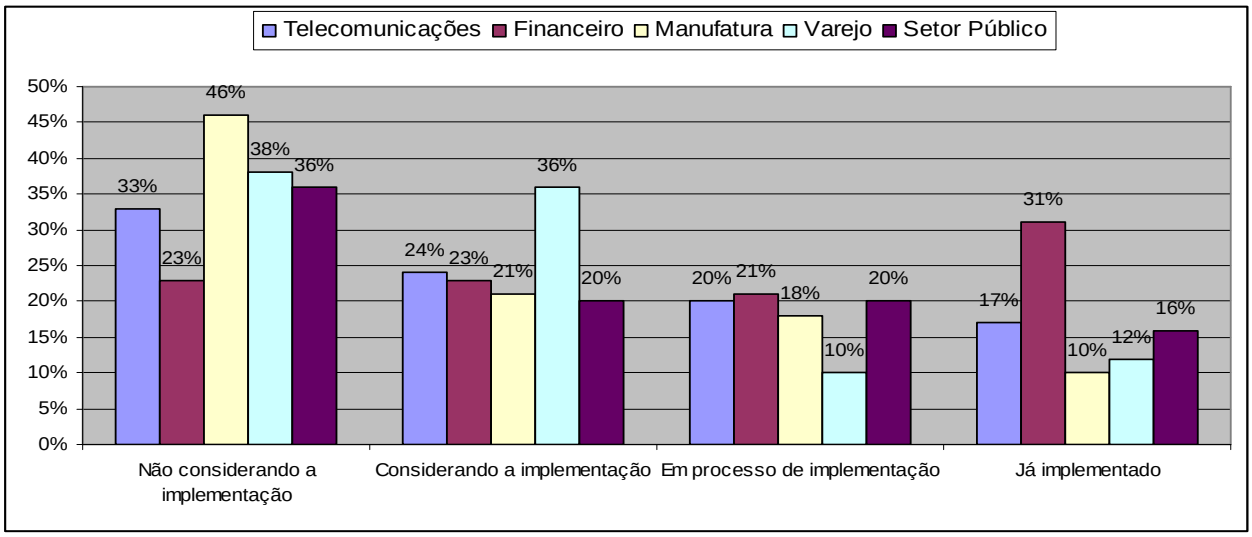

FIGURA 2 – Status da Implementação de Governança de TI – Por Setor da Indústria
Fonte: IT Governance Institute, 2006

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 não entendem que o CobiT não é um modelo fechado. A figura 3 mostra a dificuldade de implementação do CobiT.

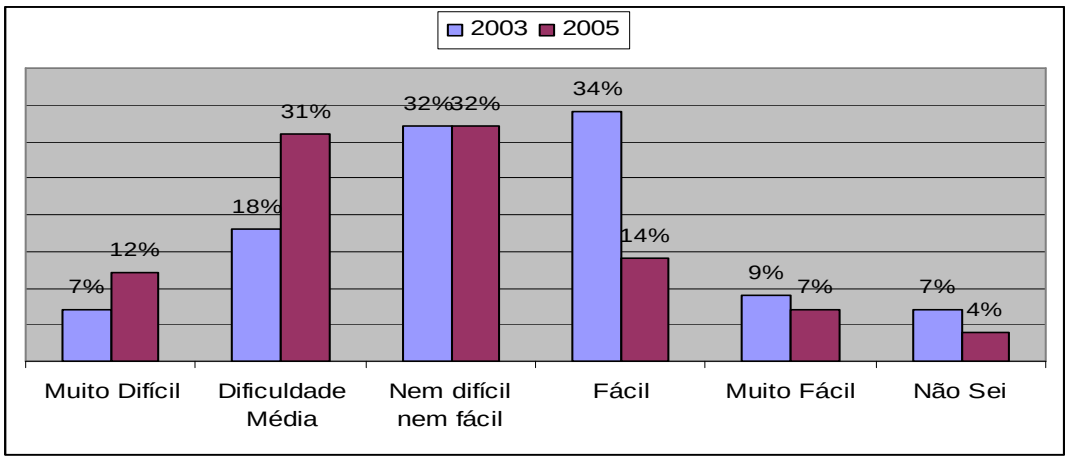

FIGURA 3 – Dificuldade na Implementação do CobiT
Fonte: IT Governance Institute, 2006

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.

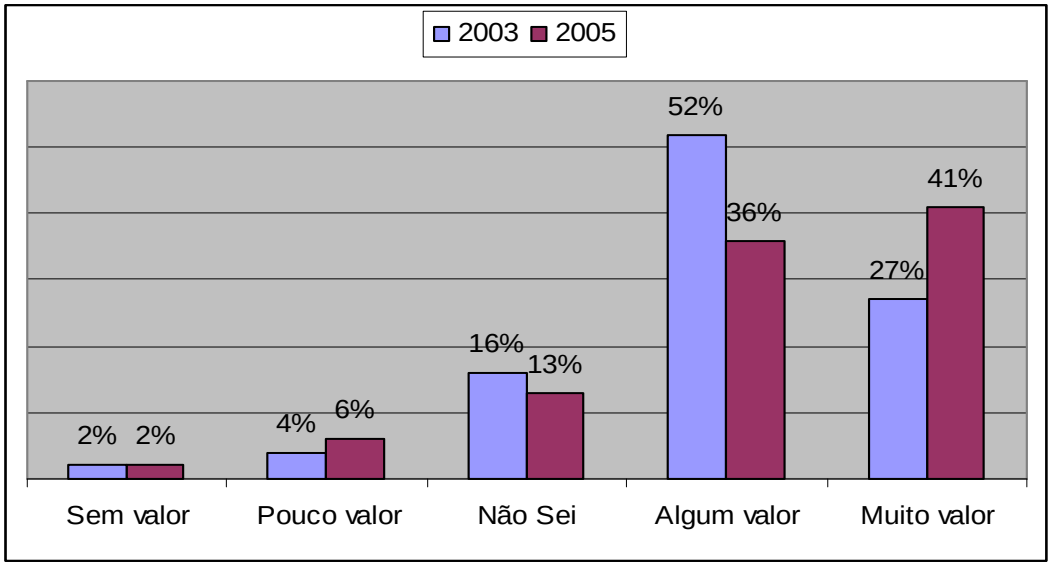

FIGURA 4 – Valor do CobiT nos esforços de Governança de TI
Fonte: IT Governance Institute, 2006

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 *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.

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.

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, aplicar um questionário com base 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.

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.

O protocolo desse estudo de caso foi desenvolvido da seguinte maneira:

a) 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 tem os seguintes objetivos:

- Proporcionar um primeiro contato dos respondentes com os modelos de maturidade;

- Fazer com que os respondentes reflitam em relação ao nível de maturidade atual dos principais processos de TI;

- Fazer com que os respondentes projetem o nível de maturidade desejado para os processos de TI em questão;

- Coletar dados para análise dos níveis de maturidade;

- Validar os modelos de maturidade como ferramenta de implementação de um processo de governança de TI.

b) Período de preparação – em agosto de 2005 foi desenvolvido um questionário com base nos modelos de maturidade descritos no *Management Guidelines* do Cobit. GULDENTOPS *et al* (2000).

c) Plano de coleta de dados - A unidade de análise definida para esse estudo é responsável pela emissão de certificados digitais de uma grande empresa de tecnologia (mais de 8.000 funcionários). A visita ocorreu nos meses de outubro e novembro de 2005 na cidade do Rio de Janeiro.

- O questionário, que se encontra no Apêndice A, sobre nível de maturidade foi encaminhado em novembro de 2005 para os funcionários responsáveis pela operação e pela gestão da unidade de certificação digital.

d) Avaliação dos resultados – após a realização de entrevistas e obtenção dos questionários devidamente respondidos, em janeiro de 2006 foi feita a consolidação das respostas e análise de *gap* que está descrita no Capítulo 5.

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.

No Capítulo 1 serão abordados os conceitos básicos de governança corporativa, governança de TI, CobiT, alinhamento entre governança corporativa e de TI e um plano de implementação de governança de TI.

As diretrizes de gerenciamento de processos serão abordadas no Capítulo 2, além de buscar a origem e a definição dos níveis de maturidade em desenvolvimento de sistemas e no CobiT.

No Capítulo 3 serão abordadas pesquisas da utilização da Internet, a necessidade da utilização da certificação digital e alguns exemplos e a estrutura das principais autoridades certificadoras no Brasil.

O estudo da utilização dos modelos de maturidade para implementar governança de TI na autoridade certificadora está situado no Capítulo 4.

1 GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

Nesse capítulo são tratados os conceitos básicos como a própria definição da palavra governança, a teoria da agência, o conceito de governança corporativa, o conceito de governança de TI, trazendo fundamentações para o entendimento do CobiT 3ª edição, seus domínios e processos, permitindo que todos esses conceitos se relacionem e se direcionem para um plano de implementação de governança de TI.

1.1 Governança Corporativa

No dicionário da língua portuguesa a palavra governança nos remete a governação, que é o ato de governar (-se); governo. Governar por sua vez apresenta os seguintes significados: 1. Regular o andamento de; conduzir. 2. Exercer o governo de; imperar em; dirigir; administrar. 3. Ter poder ou autoridade sobre; reger. 4. Reger; dirigir, administrar. (FERREIRA, 1995). Diante desse contexto, percebe-se a necessidade de uma estrutura mínima de controles que proporcione o ato de dirigir.

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.

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.

A Cartilha de Governança Corporativa da Comissão de Valores Mobiliários – CVM diz para os investidores a análise das práticas de governança e auxilia na

decisão de investimento, pois a governança determina o nível e as formas de atuação que estes podem ter na companhia, possibilitando-lhes exercer influência no desempenho da mesma. O objetivo é o aumento do valor da companhia, pois boas práticas de governança corporativa repercutem na redução de seu custo de capital, o que aumenta a viabilidade do mercado de capitais como alternativa de capitalização.

Quando investidores financiam companhias, eles sujeitam-se ao risco de apropriação indevida, por parte de acionistas controladores ou de administradores da companhia, de parcela do lucro do seu investimento. A adoção de boas práticas de governança corporativa constitui, também, um conjunto de mecanismos por onde os investidores, incluindo controladores, protegem-se contra desvios de ativos por indivíduos que têm poder de influenciar ou tomar decisões em nome da companhia.

A definição de Governança Corporativa contida na cartilha da CVM é:

> Governança corporativa é o conjunto de práticas que tem por finalidade otimizar o desempenho de uma companhia ao proteger todas as partes interessadas, tais como investidores, empregados e credores, facilitando o acesso ao capital. A análise das práticas de governança corporativa aplicada ao mercado de capitais envolve, principalmente: transparência, eqüidade de tratamento dos acionistas e prestação de conta. (RECOMENDAÇÕES [...] 2002)

A cartilha tem como objetivo recomendar boas práticas de governança corporativa e indica a adoção de padrões de conduta superiores ao exigido pela lei, ou pela própria regulamentação da CVM. Dessa forma, não se trata de uma norma cujo não cumprimento resultará em punição. O que é exigido são informações anuais das companhias abertas de indicação do nível de adesão das práticas ali recomendadas, na forma “pratique ou explique”, ou seja, caso a companhia não adote a recomendação, poderá explicar suas razões. Esse conceito de transparência também está sendo aplicado em empresas particulares, dada sua nítida aplicabilidade.

A Bolsa de Valores de São Paulo - Bovespa possui um segmento conhecido como Novo Mercado, que é destinado à negociação de ações emitidas por empresas que se comprometem voluntariamente a aderir a práticas de governança corporativa. A entrada de uma empresa nesse segmento amplia os direitos dos acionistas e melhora a qualidade das informações prestadas, além de solucionar eventuais conflitos societários por meio de uma Câmara de Arbitragem e oferecer segurança aos investidores.

O grau de comprometimento da empresa com “As Práticas Diferenciadas de Governança Corporativa”, é definido pela BOVESPA como: um conjunto de normas de conduta para as empresas, administradores e controles considerados importantes para uma boa valorização das ações e outros ativos emitidos pela empresa. A adesão a estas práticas é classificada como Nível 1 e Nível 2, o que dá destaque aos esforços da empresa na melhoria da relação com os investidores e eleva o potencial de valorização de seus ativos.

As companhias de Nível 1 comprometem-se, principalmente, com a melhoria da prestação das informações ao mercado, entre outras regras de negociação no mercado acionário. Já as companhias de Nível 2 precisam atender todas as práticas definidas para o Nível 1 e a aceitação de um conjunto mais amplo de práticas de Governança Corporativa e direitos adicionais para acionistas minoritários, além de atender também a normas internacionais.

Essas ações necessitam de uma estrutura básica de Governança Corporativa, onde tem como suporte os seguintes princípios:

a) Direcionamento e Condução – permite que os objetivos da organização sejam atingidos por meio de um administrador, pode ser uma pessoa ou um comitê.
b) Controle – exige controles na organização para permitir que a direção e objetivos sejam atingidos.
c) Abertura, transparência e prestação de contas – as atividades descritas acima devem ocorrer no espírito das companhias públicas e do governo para que os acionistas tenham confiança que as ações tomadas em seu interesse são legítimas e dentro do escopo da operação.

1.1.1 Direcionamento e Condução

Hoje em dia, governança corporativa é um sistema fundamental para as empresas, pois há várias partes interessadas na boa condução da empresa. Os americanos usam o termo *stakeholders* para definir as partes interessadas. Segundo Hamaker e Hutton (2003), o termo *stakeholders* abrange investidores, clientes, empregados, fornecedores, credores e a própria comunidade. Para uma empresa pública o principal *stakeholder* é a própria população.

1.1.2 Abertura, transparência e prestação de contas

A principal definição nesse caso é a transparência das operações que ocorrem dentro da companhia, de forma que as partes interessadas tenham

confiança na gestão. Um dos recursos utilizados é a definição de um código de conduta, onde os funcionários e gestores ficam sabendo da regra que deverá ser seguida, ou seja, todos sabem da necessidade da prestação de contas e da abertura necessária para gerir a empresa.

1.2 Governança de TI e o CobiT

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).

A estrutura, que apóia esse conceito e que viabiliza a implementação de um modelo de governança de TI é o Cobit (*Control Objetives for Information and related Technology*).

1.3 Evolução e Histórico do CobiT

A primeira edição foi liberada em 1996, com base nos objetivos de controle do *Information Systems Audit and Control Foundation* (ISACAF). Os objetivos de controle detalhados e de alto nível foram revisados para a 2ª edição publicada em 1998 acrescida de ferramentas de implementação. A 3ª edição foi marcada como a primeira publicação do *IT Governance Institute*, contando com uma ferramenta adicional *Management Guidelines*. (GULDENTOPS *et al*, 2000).

A informação necessária para satisfazer os objetivos de negócio deve atender a certos critérios. Dos modelos de referência conhecidos o CobiT usa os seguintes requerimentos:

a) Requerimentos de Qualidade: Qualidade, Custo e Entrega.
b) Requerimentos Fiduciários: Efetividade e eficiência das operações, confiabilidade das informações, cumprimento das leis e regulamentações.
c) Requerimentos de Segurança: Sigilo, integridade e disponibilidade.

Em termos de requerimento de qualidade, considera-se a ausência de falhas, confiabilidade e aspectos menos tangíveis como: estilo, atração, fazer além das expectativas, etc.

Para os requerimentos fiduciários, que são dependentes de confiança, usa-se como referência as definições do *COSO - COSO Report (Internal Control-Integrated Framework, Committee of Sponsoring Organisations of the Treadway Commission*, 1992) e estende-se a definição para todo tipo de informação e não somente informações financeiras.

Para os requerimentos de segurança são utilizados os conceitos considerados mundialmente como padrão em termos de segurança da informação.

Dos requerimentos acima, são extraídos sete conceitos distintos que muitas vezes se sobrepõem:

a) Efetividade: Lida com a informação relevante e pertinente ao processo de negócio, entregue no prazo, de forma correta, consistente e utilizável;
b) Eficiência: Fornecimento da informação por meio do uso mais produtivo e econômico dos recursos;
c) Sigilo: Proteção da informação de revelação não-autorizada;
d) Integridade: Relativo à informação completa e precisa, válida de acordo com expectativas e valores de negócio;
e) Disponibilidade: relativos à informação disponível quando requerida pelo processo de negócio no momento e no futuro. Considera também a salva-guarda dos recursos necessários;
f) Conformidade: Lida com o cumprimento das leis, regulamentações e contratos aos quais os processos de negócio estão sujeitos, ou seja, critérios externamente impostos;
g) Confiabilidade da Informação: Relativo à provisão de informação apropriada para a gerência operar a entidade e para o exercício de responsabilidades de reportar as responsabilidades financeiras e de cumprimento das leis e das regulamentações;

Já os recursos de TI são definidos como:

a) Dados: São objetos no senso mais amplo, estruturados e não-estruturados, gráficos, som, etc;
b) Aplicações: A soma de procedimentos manuais e programados;

c) Tecnologia: Máquinas computacionais, sistemas operacionais, sistemas de gerenciamento de base de dados, rede, multimídia, etc;
d) Instalações: São todos os recursos das instalações, sistemas de suporte de informação;
e) Pessoas: Inclui as habilidades das pessoas envolvidas, conscientização e plano de produtividade. Organizar, adquirir, entregar, dar suporte e monitorar sistemas da informação e serviços;

1.4 Estrutura Conceitual do CobiT

O esquema do CobiT em sua 3ª Edição é composto por objetivos de controle de alto nível e toda uma estrutura para a classificação, ou seja, três níveis a serem considerados no gerenciamento de recursos de TI. Começando pelas atividades e tarefas necessárias para atingir resultados mensuráveis. Os processos estão situados em um nível acima e são formados pelo conjunto de atividades e tarefas e seus controles associados. No nível mais alto situam-se os domínios que agrupam os processos. Esse agrupamento é organizado conforme as responsabilidades e o gerenciamento. A estrutura conceitual pode ser demonstrada de acordo com o cubo do CobiT, conforme figura 5.

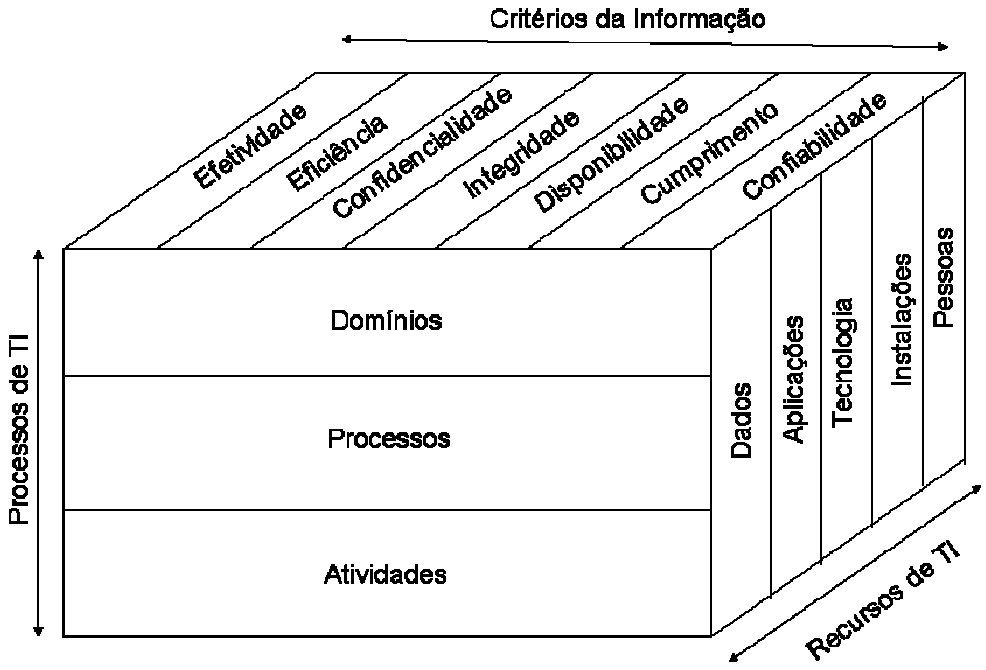

FIGURA 5 – Cubo CobiT
Fonte: Guldentops *et al*, 2000

1.4.1 Domínios do CobiT

Os domínios são classificados usando termos que identificam as atividades do dia-a-dia. Daí surgem quatro domínios: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte e por fim Monitoramento. Definindo cada domínio:

a) Planejamento e Organização - Uma organização apropriada e uma infra-estrutura tecnológica devem ser montadas. A realização da visão estratégica precisa ser planejada, comunicada e gerenciada em diferentes perspectivas (a estratégia e a tática). Identifica o caminho de TI que melhor contribui para se atingir os objetivos de negócio.
b) Aquisição e Implementação – Para realizar a estratégia de TI é necessário identificar, desenvolver e integrar soluções de TI com os processos de negócio. Adicionalmente, mudanças e manutenções dos sistemas são cobertas por esse domínio para assegurar que o ciclo de vida desses sistemas é regularmente mantido.
c) Entrega e Suporte – Esse domínio trata a entrega atual dos serviços requeridos, que inclui as operações tradicionais sobre os aspectos de segurança, continuidade até treinamento. É necessário montar processos de suporte para entregar os serviços. Esse domínio inclui o processamento atual de dados pelos aplicativos, normalmente classificado sob controles de aplicativos.
d) Monitoramento – Todos os processos de TI precisam ser avaliados regularmente considerando a qualidade, o cumprimento e os requerimentos de controle. Esse domínio prevê também um processo de auditoria independente interna ou externa.

Dentro dos domínios existem os processos de TI que compõem os domínios do CobiT, são eles:

Planejamento e Organização

PO1 - Definição do Plano Estratégico de TI;

PO2 - Definição da Arquitetura da Informação;

PO3 - Determinação da Direção Tecnológica;

PO4 - Definição da Organização de IT e Relacionamentos;

PO5 -Gerenciamento do Investimento de TI;

PO6 - Divulgação dos Objetivos de Gestão e Diretrizes;

PO7 - Gerenciamento de Recursos Humanos;

PO8 - Garantia de Aderência aos Requerimentos Externos;

PO9 - Gerenciamento de Riscos;

PO10 - Gerenciamento de Projetos;

PO11 - Gerenciamento de Qualidade.

Aquisição e Implementação

AI1 - Identificação das Soluções Automatizadas;

AI2 - Aquisição e Manutenção de Software de Aplicação;

AI3 - Aquisição e Manutenção de Infra-estrutura Tecnológica;

AI4 - Desenvolvimento e Manutenção de procedimentos;

AI5 - Instalação e Certificação de Sistemas;

AI6 - Gerenciamento de Mudanças.

Entrega e Suporte

DS1 - Definição e Gerenciamento de Níveis de Serviço;

DS2 - Gerenciamento de Serviços de Terceiros;

DS3 - Gerenciamento de Desempenho e Capacidade;

DS4 - Garantia de Serviço Contínuo;

DS5 - Garantia de Segurança para Sistemas;

DS6 - Identificação e Alocação de Custos;

DS7 - Educação e Treinamento de Usuários;

DS8 - Ajuda e Aconselhamento a Usuários;

DS9 - Gerenciamento de Configuração;

DS10 - Gerenciamento de Problemas e Incidentes;

DS11 - Gerenciamento de Dados;

DS12 - Gerenciamento de Instalações;

DS13 - Gerenciamento de Operações.

Monitoramento

M1 - Monitoramento dos Processos;

M2 - Avaliação da Adequação dos Controles Internos;

M3 - Obtenção de Garantia Independente;

M4 - Auditoria Independente.

Em resumo, para prover a informação necessária a fim de atingir os objetivos de negócio, a governança de TI deve ser exercitada dentro da organização de forma a garantir que os processos de TI sejam gerenciados de forma

naturalmente agrupada. A figura 6 ilustra o conceito relacionando os requisitos de negócio, os recursos de TI e os domínios discutidos até aqui.

FIGURA 6 - Governança de TI e Domínios
Fonte: Guldentops *et al*, 2000

Detalhando, deve ser considerado que dentro de cada processo de TI existe um conjunto de objetivos de controle que são descritos de maneira genérica atendendo a qualquer tipo de plataforma, porém de forma extremamente detalhada.

Em termos de estrutura o CobiT versão 3 é composto por 4 domínios, 34 processos de TI e 318 objetivos de controle.

1.5 Domínios da Governança de TI e o alinhamento entre Governança Corporativa, Governança de TI e o CobiT

A governança de TI não ocorre no vácuo, depende de uma série de fatores ambientais que irão influenciar diretamente na implementação. Esses fatores variam desde as regulamentações, cultura, missão e visão da empresa até as intenções contidas nos planos estratégicos e de negócios. Dentro desses fatores TI tem uma influência bastante significativa. Todos os direcionadores captados no ambiente devem ser utilizados como motivadores de mudanças. GULDENTOPS *et al*(2003b)

Segundo Guldentops *et al* (2003b) divide-se em 5 diferentes domínios.

1.5.1 Alinhamento Estratégico de TI

O ambiente provê as informações necessárias para definir a missão, visão e estratégia de TI, assegurando que os serviços de TI estão alinhados com todos os elementos da organização. Esse alinhamento inclui: o planejamento estratégico de negócios e de TI, planejamento operacional de TI e análise de riscos, desempenho e serviços.

1.5.2 Valor de Entrega de TI

Os princípios básicos são: entregas de produtos de TI no prazo e dentro do orçamento com os benefícios previamente identificados. Os processos de TI devem ser desenhados, distribuídos e operados de maneira eficiente e efetiva. As expectativas e objetivos são determinados pelos direcionadores de negócio que também são influenciados pelo ambiente. Esse valor deve estar alinhado diretamente com os valores em que o negócio está focado e deve ser medido de maneira transparente, mostrando o impacto e a contribuição dos investimentos de TI e na criação de valor. O nível de eficiência e efetividade dos processos de TI depende do nível de maturidade.

1.5.3 Gerenciamento de Risco

Cobre o processo de preservação do valor, além do tradicional gerenciamento de riscos financeiros, hoje existe a preocupação com os riscos operacionais e sistêmicos. A integração dos diferentes modos de gerenciar riscos

gera a transparência necessária para todos os envolvidos. Deve ser um processo contínuo, iniciado com a identificação dos riscos (impacto nos ativos, ameaças e vulnerabilidades). Uma vez identificado, o risco deve ser mitigado por contramedidas (controles). Mas também é necessária atenção aos riscos residuais e sua aceitação formal, além de gerenciar, medir e monitorar.

1.5.4 Gerenciamento de Recursos de TI

Estabelece e distribui as capacidades corretas de TI para as necessidades de negócio. O foco inicial deve ser sobre o conhecimento e a infra-estrutura. Essa preocupação lida com a origem dos processos, considerando os modelos desenvolvidos em casa e os modelos de *outsourcing*, usando critérios de avaliação que vêm das intenções estratégicas da empresa e fatores críticos de sucesso. A finalidade é assegurar que seja fornecida uma infra-estrutura de TI integrada e econômica, onde novas tecnologias possam ser introduzidas e que os sistemas obsoletos sejam substituídos. Reconhecer a importância das pessoas em conjunto com hardware e o software, focando na manutenção e na disponibilidade. É necessário o desenvolvimento de habilidades, treinamento, promoção, de forma a proporcionar competências às pessoas chave de TI, bem como a sua retenção. Isso inclui também gerenciar o *outsourcing* e fornecedores.

1.5.5 Mensuração de Desempenho

Sem estabelecer e sem monitorar desempenho é improvável que as fases anteriores atinjam os resultados desejados. Isso inclui auditoria e avaliação de atividades e monitoração contínua de desempenho. Existe uma ligação com a fase de alinhamento por meio de evidências de que a direção está sendo seguida ou não. Proporciona a oportunidade de criar medidas corretivas, se necessário. *IT Balanced Score Cards* traduzem a estratégia de TI alinhada com a estratégia de negócios. Dessa forma, TI necessita de seus próprios *balanced score cards*, definindo metas claras e medidas adequadas que reflitam o impacto de TI nos negócios.

1.6 Relacionamento entre os Princípios de Governança Corporativa e de TI

Dados os domínios de Governança de TI é possível citar a dissertação desenvolvida para o *Chartered Management Institute* de Londres intitulado como: *Is*

there a relationship between IT governance and corporate governance? What improvements (if any) would IT governance bring to the LSC? GRAY(2004), onde a autora desenvolve um estudo sobre a implementação de Governança de TI em um orgão governamental inglês, *Learning and Skills Council* – LSC, que é responsável por financiar, planejar educação e treinamento para maiores de 16 anos na Inglaterra. Nesse trabalho a autora apresenta um relacionamento entre os princípios de Governança Corporativa, Governança de TI e o CobiT. Esse relacionamento está representado graficamente na figura 7.

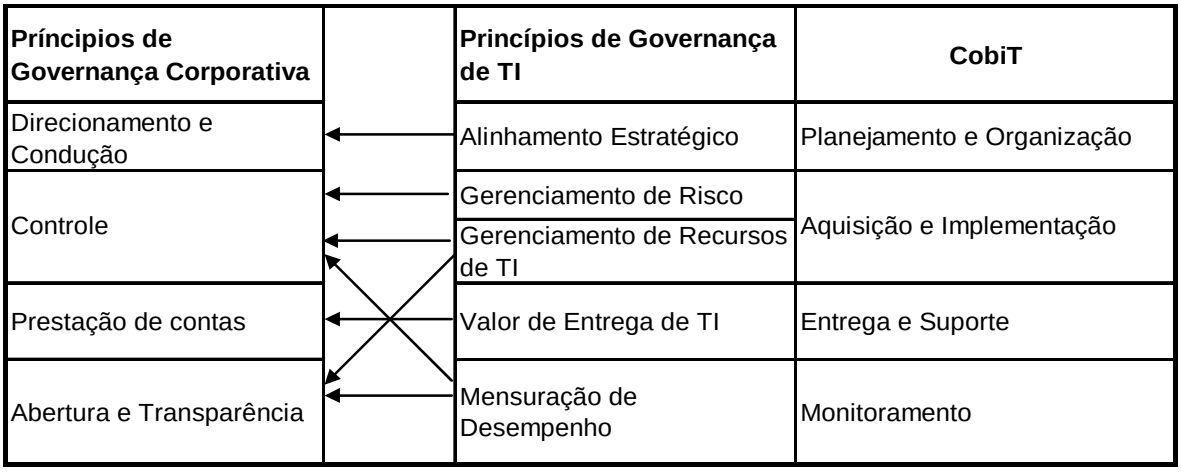

FIGURA 7 - Relacionamento entre governança corporativa, governança de TI e CobiT
Fonte: GRAY,H: 2004

Os domínios de governança de TI provêem uma estrutura que está contemplada na nova versão do Cobit 4.0, segundo Casciano *et al* (2005) essa estrutura assegura que:

a) TI esteja alinhada com os negócios;
b) TI proporcione negócios e maximize os benefícios;
c) Os recursos de TI sejam usados de maneira responsável;
d) Os riscos de TI sejam gerenciados adequadamente.

1.7 Plano de Implementação de Governança de TI e o papel de cada membro envolvido no processo

Para iniciar um projeto de implementação de governança de TI a necessidade pelo tema precisa ser reconhecida pela empresa, para chegar a esse ponto é importante que sejam reiterada e comunicada tal necessidade por meio dos seguintes passos, segundo Guldentops *et al* (2003b).

a) Entender a iniciativa de governança de TI e definir objetivos de negócio para TI mensuráveis;
b) Entender os objetivos de negócio e como eles podem ser traduzidos em objetivos de TI;
c) Entender os riscos e como podem afetar as metas de TI;
d) Decidir com base no que foi levantado nos itens anteriores, o escopo do projeto de melhoria;
e) Identificar os processos de TI a serem implementados ou melhorados.

Após a realização desses passos é possível partir para um plano de ação para implementar governança de TI, conforme figura 8:

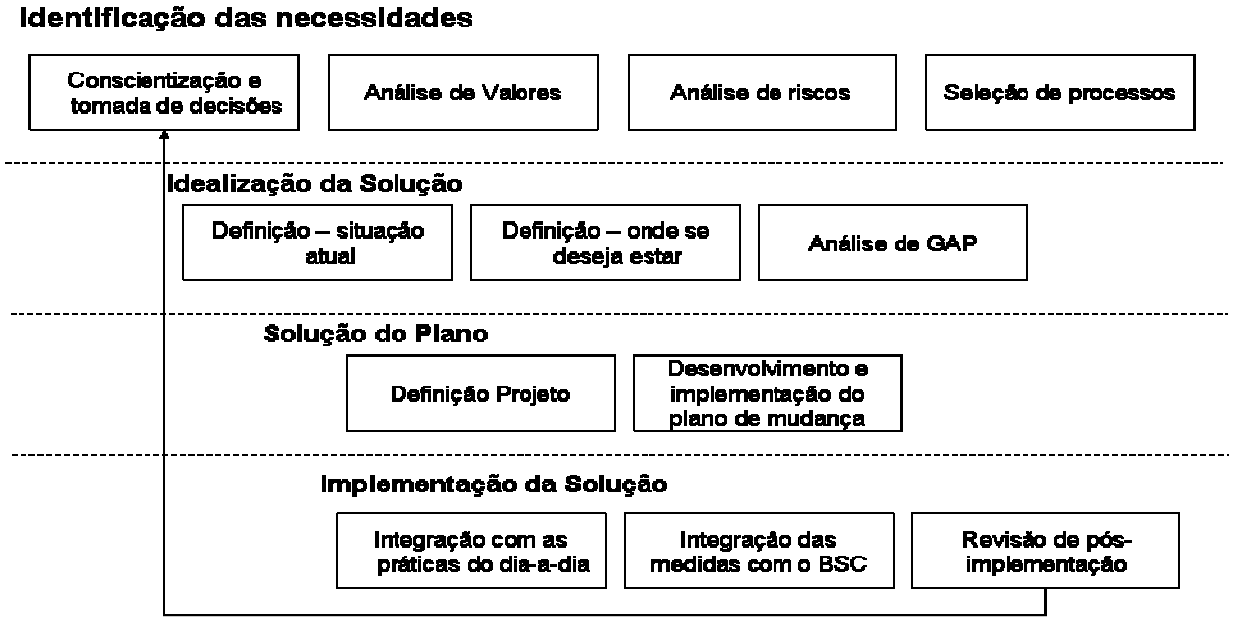

FIGURA 8 - Fases e passos de implementação de governança de TI
Fonte: IT Governance Implementation Guide, 2003b

Existem vários membros envolvidos nesse tipo de projeto, onde há tarefas específicas para cada um. Essas tarefas correspondem ao papel atribuído para cada membro em cada etapa. Os papéis definidos são: Comitê e Executivos, Gerente de Negócios, Gerente de TI, Auditor de TI e Gerente de Riscos e Conformidade.

Doze passos compõem um plano de implementação de governança de TI.

A fase de identificação das necessidades é dividida em quatro passos:

1. Conscientização e tomada de decisões, onde os seguintes objetivos são:

- Entender e definir objetivos;
- Definir organização, responsabilidades e recursos requeridos;

- Selecionar esquema de controles de TI e procedimentos gerenciais;
- Comunicar metas e objetivos.

2. Análise de valores

- Entender metas de negócio e contribuição de TI;
- Definir o valor de TI em função dos negócios.

3. Análise de Riscos

- Entender apetite de risco e histórico de riscos;
- Avaliar riscos operacionais de TI;
- Avaliar riscos de projeto;
- Definir riscos com base nas metas de TI.

4. Seleção de Processos

- Selecionar processos de TI e metas.

Dentro dessa fase os responsáveis e os respectivos papéis, conforme quadro 1:

Quadro 1 - Papéis e responsabilidades na fase de identificação das necessidades

Responsável	Papel
Comitê e Executivos	Define a direção, aprova a abordagem, define os projetos principais, dá visibilidade, suporte e comprometimento. Considera as prioridades de negócio e riscos. Patrocina, comunica e promove o plano.
Gerente de Negócios	Define os requerimentos de negócio para TI e proporciona entendimentos para os riscos e prioridades. Estabelece escopo com TI. Provê recursos e comprometimento para suportar a iniciativa.
Gerente de TI	Obtém requerimentos e objetivos de todos os envolvidos. Dá conselhos e guias considerando as preocupações de TI e assegura que todos entendem as preocupações apresentadas.
Auditor de TI	Dá conselhos e desafia as atividades e as ações, assegura decisões balanceadas e objetivas. Aconselhar considerando controles e gerenciamento de riscos.
Gerente de Riscos e Conformidade	Dá conselhos e orienta, considerando as preocupações de conformidade e assegura que a abordagem sugerida irá atender os requerimentos de conformidade e riscos.

Fonte: IT Governance IMPLEMENTATION GUIDE, 2003b

A fase de idealização da solução é composta dos passos 5, 6 e 7:

5. Avaliar a maturidade atual;

6. Determinar a maturidade desejada;
7. Analisar o intervalo (*gap*) e identificar oportunidades de melhorias

Dentro dessa fase os responsáveis e os respectivos papéis, conforme descrito no quadro 2:

Quadro 2 - Papéis e responsabilidades na fase de idealização das soluções

Responsável	Papel
Comitê e Executivos	Interpreta os resultados/conclusões das avaliações. Define prioridades, escala de tempo e expectativas, considerando a capacidade futura requerida de TI.
Gerente de Negócios	Assegura que as metas de negócio foram entendidas por TI, revisa as prioridades e verifica se as metas de TI são razoáveis. Auxilia TI na definição de metas.
Gerente de TI	Aplica julgamento profissional na formulação dos planos de melhorias e iniciativas. Obtém consenso na meta requerida.
Auditor de TI	Dá conselhos e auxilia nas avaliações, define situação atual e prioridades. Se necessário, de forma independente verifica o resultado.
Gerente de Riscos e Conformidade	Revisa as avaliações para assegurar que os riscos e que a conformidade estão senda atendidas de forma adequada.

Fonte: IT GOVERNANCE IMPLEMENTATION GUIDE, 2003b

A contribuição desse trabalho está situada dentro dessa etapa de implementação de governança de TI.

A fase da solução do plano é composta dos passos 8 e 9:

8. Priorizar melhorias em projetos justificáveis;
9. Desenvolver programas de melhorias.

Dentro dessa fase os responsáveis e os respectivos papéis, quadro 3:

Quadro 3 - Papéis e responsabilidades na fase solução do plano

Responsável	Papel
Comitê e Executivos	Considera e desafia as propostas, dá suporte para ações justificadas, provê orçamento e define prioridades.
Gerente de Negócios	Assegura que os requerimentos de negócio estão definidos de forma precisa e que ações propostas de melhoria estão alinhadas com as prioridades de negócio.
Gerente de TI	Assegura viabilidade e propostas razoáveis. Assegura que os planos são viáveis de serem atingidos e que os recursos estão disponíveis para

	executar a estratégia proposta.
Auditor de TI	Garante, de maneira independente, que os pontos identificados são válidos e que o caso de negócio está precisamente definido e que os planos podem ser atingidos. Dá conselhos quando apropriado.
Gerente de Riscos e Conformidade	Assegura que qualquer risco ou conformidade estão sendo atendidos e que as propostas estão em conformidade com as políticas relevantes e regulamentações.

Fonte: IT GOVERNANCE IMPLEMENTATION GUIDE,2003b

A fase de implementação é composta de três passos:

10. Implementar melhorias;
11. Integrar métricas em *Balanced Score Cards*;
12. Conduzir revisão de pós implementação.

Dentro dessa fase os responsáveis e os respectivos papéis, conforme quadro 4:

Quadro 4 - Papéis e responsabilidades na fase de implementação

Responsável	Papel
Comitê e Executivos	Avalia desempenho no encontro dos principais objetivos. Considera a necessidade de redirecionar atividades futuras.
Gerente de Negócios	Dá retorno e considera a efetividade da contribuição ao negócio e a iniciativa. Usa resultados positivos para melhorar as atividades de negócio relacionadas às atividades de governança de TI. Usa as lições aprendidas para adaptar e melhorar as abordagens de negócios em futuras iniciativas de governança de TI.
Gerente de TI	Dá retorno e considera a efetividade da contribuição de TI e a iniciativa. Usa os resultados positivos para melhorar as atividades de TI relacionadas às atividades de governança de TI. Usa as lições aprendidas para adaptar e melhorar as abordagens de TI em futuras iniciativas de governança de TI
Auditor de TI	Provê avaliação independente de toda efetividade e eficiência da iniciativa. Dá retorno e considera a efetividade da contribuição da auditoria para a iniciativa. Usa resultados positivos para melhorar as atividades de auditoria relacionadas às atividades de governança de TI. Usa as lições aprendidas para adaptar e melhorar as abordagens da auditoria em futuras iniciativas de governança de TI
Gerente de Riscos e	Avalia se a iniciativa melhorou a habilidade da organização em identificar

Conformidade	e gerenciar riscos e requerimentos legais, regulatórios e contratuais. Dá retorno e faz recomendações necessárias de melhorias.

Fonte: IT GOVERNANCE IMPLEMENTATION GUIDE, 2003b

Guldentops; De Haes (2002) realizaram uma pesquisa entre os compradores do CobiT 3ª edição onde constatou-se que o CobiT é efetivamente utilizado por 75% das empresas que o adquiriram.

As empresas estão espalhadas por vários continentes (Américas, Europa e Ásia) e há uma concentração em empresas de grande porte (entre 1000 e mais de 10.000 funcionários). Dentre os principais motivos apontados para a utilização dessa metodologia podemos destacar a melhoria dos programas de auditoria e os guias de governança de TI.

A adoção da governança de TI é hoje eminente em todas as empresas e não somente àquelas que adotam o conceito por necessidades legais ou regulatórias, pois os modelos de mercado mostram uma nova forma de gestão que requer transparência e entendimento do que acontece na área de tecnologia por todos dentro da organização.

2 NÍVEL DE MATURIDADE

Nesse capítulo aborda-se o *Management Guidelines*, sua função no CobiT e seus componentes com foco nos modelos de maturidade. O surgimento do modelo de maturidade no desenvolvimento de sistemas e um exemplo de nível de maturidade 5. E finalmente um quadro comparativo entre os níveis de maturidade do CMM e do CobiT. Os itens estudados contribuíram para o aprofundamento dos modelos de maturidade.

2.1 Management Guidelines

O *Management Guidelines* foi introduzido na 3ª versão do CobiT (GULDENTOPS et al, 2000) e é composto de:

a) Modelos de Maturidade
b) Fatores Críticos de Sucesso (CSF)
c) Indicadores de Metas (KGI)
d) Indicadores de Desempenho (KPI)

É um esquema que proporciona uma série de métricas necessárias para o controle e gerenciamento dos 34 processos do CobiT.

Existem várias mudanças em TI e na rede que mostram a necessidade de um melhor gerenciamento dos riscos de TI. A dependência de informações eletrônicas e sistemas de TI são essenciais para suportar os processos críticos de TI. Negócios de sucesso precisam gerenciar melhor a tecnologia complexa que permeia toda a organização de forma a responder rapidamente e de forma segura aos requerimentos de negócio, sem deixar de lado as necessidades regulatórias.

Com o aumento da interconexão e da dependência de TI na economia global, o gerenciamento de risco é dependente de práticas específicas. Em ambientes complexos, o gerenciamento está continuamente procurando por informações consolidadas e no prazo de forma a tornar decisões de risco e de controle rápidas e acertadas. As questões tradicionais de gerenciamento das informações são:

a) Como manter o “navio” em curso?
b) Como atingir resultados satisfatórios para os *stackholders* ?
c) Como adaptar a organização às tendências e desenvolvimento no ambiente empresarial?

As respostas seriam respectivamente: painéis de controle, *scorecards* e *benchmarking*. Porém, os painéis de controle necessitam de indicadores, os *scorecards* de medidas e *benckmarking* de escalas para comparação.

Benchmarking é um processo contínuo e sistemático que permite a comparação de desempenho das organizações e respectivas funções ou processos face ao que é considerado o melhor nível. (O QUE [...], 1996)

O principal objetivo do *Management Guidelines* é prover informações gerenciais para atender necessidades básicas para cada organização, e entender seu próprio sistema e decidir que segurança e qual controle deve ser implementado. Não é fácil obter essa informação de maneira óbvia. O que deve ser medido e como medir? Os controles implementados justificam os custos envolvidos? É nesses pontos que o CobiT pode ajudar, pois é genérico e orientado à ação com o propósito de atender os seguintes pontos:

a) Medição de desempenho – Quais são os indicadores de bom desempenho?
b) Controle de TI – O que é importante? Quais são os fatores críticos de sucesso para controle?
c) Conscientização – Quais são os riscos se não atingirmos nossos objetivos?
d) *Benchmarking* – O que os outros fazem? Como medimos e comparamos?

As respostas para os itens acima são:

a) *Benchmarking* dos controles de TI - Modelos de Maturidade
b) Indicadores de desempenho dos processos de TI - resultados e desempenho
c) Fatores críticos de sucesso para ter os processos sob controle.

O *Management Guidelines* é consistente e desenvolvido com base na estrutura do COBIT, nos objetivos de controle e guia para auditoria. Tem foco no gerenciamento de desempenho com base nos princípios de *Balanced ScoreCard*. Auxilia na definição de indicadores de metas, na identificação e medição de resultados dos processos e indicadores de desempenho para avaliar quão bem os processos estão por meio da medição da tecnologia que é o viabilizador do processo. O relacionamento entre essas entidades é representado graficamente na figura 9:

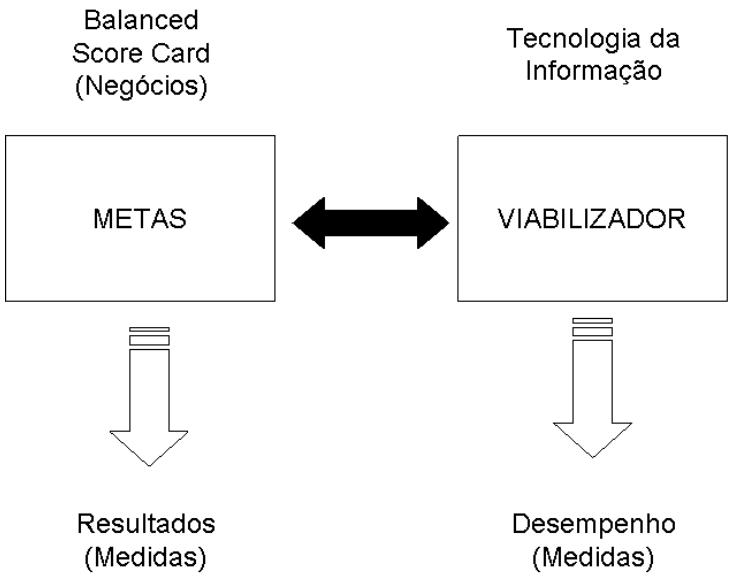

FIGURA 9 - Relacionamento entre KGI x KPI
Fonte: Guldentops *et al*, 2000

Essas medidas irão auxiliar na monitoração da organização de TI da sua organização, respondendo as seguintes questões:

1. Qual a preocupação da gerência?

Ter certeza que as necessidades da empresa estão totalmente preenchidas?

2. Onde estão as medições?

No *balanced scorecard* como KGI (indicador de meta) representando um resultado do processo de negócio.

3. Qual é a preocupação de TI?

Que o processo de TI seja entregue no prazo e a informação correta para a empresa, viabilizando o processo de negócio a ser atendido. Isso é um fator crítico de sucesso para a empresa (CSF)

4. Onde está a medição?

No *balanced scorecard* de TI como KGI que representa o resultado de TI, onde a informação é entregue com o critério correto (efetividade, eficiência, sigilo, integridade, disponibilidade, conformidade e confiabilidade).

5. O que mais necessita ser mensurado?

Indicadores de meta (KPI) que irão demonstrar quão bem TI está indo.

Modelo de maturidade para controles de processos de TI consiste do desenvolvimento de um método de graduação, onde uma organização pode se auto-avaliar por meio de uma escala que varia de não-existente até otimizado (0 a 5).

Essa abordagem é derivada do modelo de maturidade que o *Software Engineering Institute* definiu para o desenvolvimento de software.

Os fatores críticos de sucesso (CSF) definem as mais importantes questões ou ações de gerenciamento para atingir os controles de TI. Devem ser guias de orientação e devem identificar as coisas mais importantes a fazer (estratégias, técnicas, organizações e procedimentos).

Os indicadores de metas (KGI) definem medidas que digam o que fazer – antes do fato – se o processo de TI atingiu seus requerimentos de negócios, normalmente expressos em termos de critérios da informação, por exemplo:

a) Disponibilidade da informação necessária para suportar as necessidades de negócio;
b) Ausência de riscos, de integridade e de sigilo;
c) Eficiência dos custos dos processos e operações;
d) Confirmação da confiabilidade, efetividade e conformidade.

Os indicadores de desempenho (KPI) definem medidas para determinar quão bem os processos de TI estão na viabilização da meta a ser atingida, são indicadores guias que dizem se a meta será ou não atingida, sendo bons indicadores de capacidade, práticas e habilidades.

Em suma, os indicadores acima possuem as seguintes características: orientados a ações, genéricos, mantêm controle sobre a informação, relacionados a processos e tecnologia.

a) Modelos de Maturidade – escolha estratégica e comparação (benckmarking)
b) CSF - manter os processos sobre controle
c) KGI - monitorar o atingimento das metas dos processos de TI
d) KPI – monitorar desempenho dentro de cada processo de TI

No momento em que os negócios eletrônicos aumentam e cresce a dependência por tecnologia é necessário que as empresas demonstrem que seus níveis de segurança e de controle aumentam. Utilizando-se de métricas e *benchmarking* é uma maneira assertiva de atingir um nível competitivo de segurança em TI e controles.

Existem perguntas clássicas que, quando se trata de gestão de tecnologia, surgem e devem ser respondidas, são elas:

- Para atender aos meus objetivos de negócio, qual é o nível de controle correto que devo empregar em TI?

- Os controles empregados hoje estão longe do ideal? O custo justifica o benefício?

Para responder a essas perguntas, existem outras perguntas diretamente relacionadas:

a) Existem padrões internacionalmente reconhecidos e como estão relacionados?
b) O que os outros estão fazendo e como estamos em relação aos demais?
c) Como estamos em relação às melhores práticas da indústria?
d) Com base nas comparações externas, podemos dizer que tomamos precauções razoáveis para salvaguardar nossas informações e ativos?

Não é fácil responder as perguntas acima. Normalmente se procura por ferramentas de auto-avaliação que façam comparações de mercado.

2.2 Nível de Maturidade

O nível de maturidade do CobiT foi desenvolvido com base no *Capability Maturity Model for Software*, que surgiu e foi desenvolvido pela Carnegie Mellon University e relatado no livro *The Capability Maturity Model*.

Em novembro de 1986, o *Software Engineering Institute* (SEI) com a assistência da MITRE *Corporation* iniciou um esquema de maturidade que ajudaria as organizações a melhorar seu processo de desenvolvimento de software. Esse esforço foi iniciado em resposta a uma requisição do governo federal americano que solicitava um método para avaliação da capacidade dos fornecedores contratados. Em 1987, foi emitida uma breve descrição do esquema de processo de maturidade de software, que foi expandido posteriormente. Dois métodos, uma avaliação do processo de *software* e avaliação de capacidade de *software*, acompanhados de um questionário de maturidade foram desenvolvidos para avaliar a maturidade do processo. PAULK *et al*, 1995).

Após anos de experiência com o esquema de maturidade e o questionário fez com que o SEI evoluisse para o esquema *Capability Maturity Model for Software* (CMM) que:

a) Baseia–se nas práticas atuais;
b) Reflete o melhor da prática;
c) Reflete as necessidades dos indivíduos que realizam as melhorias no processo de software e avaliações dos processos de software;
d) Está documentado;
e) Está disponível ao público.

O CMM está baseado no conhecimento adquirido nas avaliações de processos de software e extenso retorno da indústria e governo. A versão inicial do CMM foi revista e usada pela comunidade de software durante 1991 e 1992. Conhecimento adicional nesse processo foi obtido por meio de:

a) Estudos em organizações não ligadas a software;
b) Realização e observação da avaliação de processos de software e capacidade;
c) Solicitações e análises de modelos de requisição de mudanças;
d) Participações de reuniões e workshops com indústria e governo;
e) Solicitações de pontos de vistas dos revisores da indústria e governo.

O CMM é um documento em evolução contínua e os fatores que irão influenciar incluem atividades padronizadas internacionais e a reação dos usuários.

Antes de entender o conceito de maturidade de processo de software, existem alguns conceitos fundamentais que são usados para descrever organizações maduras. O CMM foca na capacidade de software para produzir produtos de alta-qualidade.

Segundo Pauk *et al* (1995), processo é a seqüência de passos realizados para um dado propósito. De forma mais simples, é o que cada um faz. O processo integra pessoas, ferramentas e procedimentos. Processo é o que as pessoas fazem usando procedimentos, métodos, ferramentas e equipamentos para transformar matéria prima (entrada) em produtos (saída) que é o valor para os clientes.

Considerando desenvolvimento de software como um processo imaturo, onde geralmente é improvisado pelos desenvolvedores e pelos gerentes durante o projeto, mesmo que haja especificação não é rigorosamente seguida ou reiterada. Os gerentes são reativos e estão focados na resolução de problemas imediatos conhecidos como “incêndios”. Isso normalmente faz com que o orçamento e os prazos não sejam cumpridos.

Por outro lado, um processo maduro possui um processo de manutenção e desenvolvimento de software preciso, onde todos os envolvidos conhecem suas atividades que ocorrem de acordo com o planejado. Existe documentação e são atualizadas quando necessário. Os gerentes monitoram a qualidade do software e dos processos. Existe uma base como referência para análise e julgamento do produto. Prazos e orçamentos são feitos com base em desempenhos históricos e realistas. Em geral, uma organização madura segue um processo disciplinado e

consistente, pois todos os participantes entendem o valor do que fazem e existe uma infra-estrutura para suporte ao processo.

2.3 Nível de Maturidade no CobiT

Por meio da utilização de um modelo aceito e testado internacionalmente como o CMM derivou-se um modelo de maturidade que pode mapear cada um dos 34 processos de TI do CobiT, mostrando:

a) A situação atual da organização – onde a organização está hoje
b) A situação atual da indústria (melhor da classe) – comparação
c) A situação atual das práticas internacionais – comparação adicional
d) A estratégia de melhoria da organização – onde a organização quer estar.

A figura 10 ilustra o modelo de maturidade.

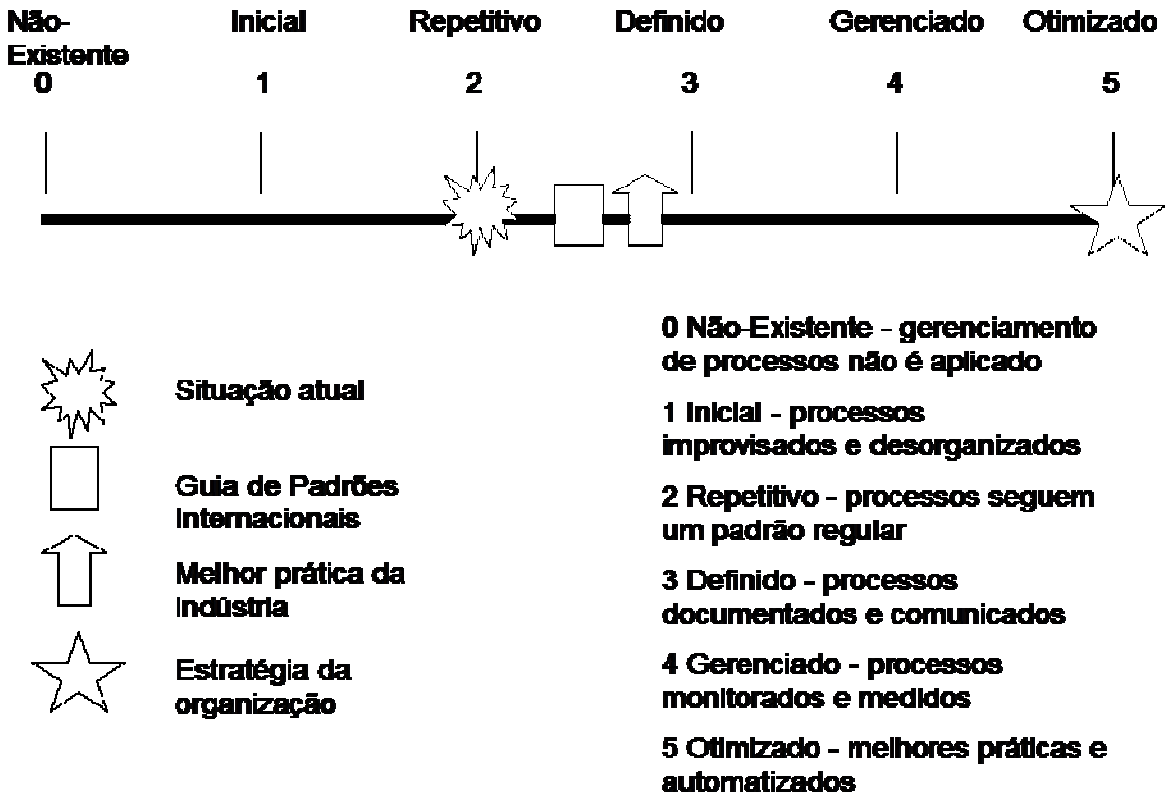

FIGURA 10 - Modelo de Maturidade
Fonte: Guldentops *et al*, 2000

Para cada um dos processos de TI , relacionados no CobiT, existe uma escala incremental associada a um modelo qualitativo e genérico, conforme descrito:

0 – Não Existente – Completa ausência de reconhecimento de processos. A organização nem reconhece que existem pontos a serem endereçados.
1 – Inicial – Existem evidências que a organização reconhece que existem pontos a serem endereçados. Entretanto, não existem processos padronizados, porém há abordagens improvisadas e tendem a serem aplicadas de forma individual de acordo com a situação. O gerenciamento de todo processo é desorganizado.
2 – Repetitivo – Os processos são desenvolvidos num estágio onde procedimentos similares são seguidos por pessoas diferentes que podem estar realizando as mesmas tarefas. Não existe comunicação nem treinamento formal dos procedimentos padrões. Existe uma alto grau de confiança no conhecimento dos indivíduos e é provável que aconteçam erros.
3 – Definido – Os procedimentos são padronizados, documentados e comunicados por meio de treinamentos. Entretanto, permite-se que cada um siga ou não esses procedimentos. É improvável que desvios sejam detectados. Os procedimentos não são sofisticados, mas há formalização das práticas existentes.
4 – Gerenciado – É possível monitorar e medir a conformidade dos procedimentos e tomar ações onde o processo parece não estar funcionando efetivamente. Os processos estão sob constante melhoria e provêm boas práticas. A automação e ferramentas são utilizadas de forma limitada e de forma fragmentada.
5 – Otimizado – Os processos estão refinados em nível de melhores práticas com base nos resultados de melhoria contínua e de modelos de maturidade com outras organizações. TI é usada como forma integrada de fluxo de trabalho, provendo ferramentas para melhorar qualidade e efetividade.

2.4 Exemplo de Maturidade Nível 5 em desenvolvimento de sistemas

Em termos de desenvolvimento de software, um exemplo de necessidade de atingir um alto nível de maturidade é o software de bordo de naves espaciais do projeto IBM-Houston. Antes de cada lançamento os gerentes assinam um certificado (*Certificate of Flight Readiness*), que atesta que não há falhas no software de bordo. Por mais de uma década, a equipe de projeto luta para assegurar a ausência de falhas no chamado *Space Shuttle Orbiter Primary Avionics Software System*, que é o software de vôo, quando novas versões são entregues a NASA.

Para satisfazer os requerimentos de alto padrão de confiabilidade, a equipe possui um processo de software que produz um resultado previsível de

qualidade. Acreditam que dado um processo definido que produz um produto em um conhecido nível de qualidade, a melhor maneira de assegurar que o próximo produto irá exibir a mesma qualidade é executar o processo fielmente ao processo padrão. Após duas décadas de trabalho, o software é exibido por um processo de manufatura sob controle de qualidade estatístico. Como resultado o software produzido por esse processo fica próximo da isenção de erros, o que dá confiança aos gerentes para assinar o certificado.

A última falha de software relativa à segurança ocorreu durante um vôo, foi identificada em outubro de 1986, mas era uma falha benigna que apontava uma mensagem, indicando uma falha que poderia ocorrer em 1989.

O software da espaçonave (*Primary Avionics Software System*) é responsável pela direção, navegação e funções de controle de vôo durante todas as fases. Adicionalmente, o software dá suporte a todas as funções de interface entre a espaçonave e as operações em terra. Monitora e gerencia todas as funções do sistema de bordo, realiza detecção de falha e anúncios, realizando procedimentos de checagem de segurança.

Esse software possui aproximadamente 420.000 linhas de código, onde o sistema operacional é escrito na linguagem *Assembler* e o restante em uma linguagem chamada HAL/S. Essa linguagem é específica para aplicações de bordo e foi desenvolvida pela Intermetrics especialmente para a NASA. (THE DEVELOPMENT […], 199-?)

Durante as fases críticas (subida e reentrada) o software de vôo roda de forma redundante em 4 dos 5 computadores de bordo, criando requerimentos de sincronização em tempo real.

O projeto *Onboard Shuttle* também desenvolve e mantém 1,7 milhões de linhas de código de ferramentas que suportam gerenciamento de configuração, desenvolvimento de software, testes, simulação, verificação automática e reconfiguração de software, que rodam num computador equivalente ao IBM S/370.

Os resultados da avaliação de capacidade de software, realizada em 1989, determinaram que o projeto tivesse nível 5. O projeto *On Board Shutlle* foi nomeado como IBM *Best Software Lab* e é o único fornecedor que recebeu da NASA o prêmio *Excellence Award* por duas vezes.

Para que o projeto tivesse nível de maturidade 5, no *Capability Maturity Model*, foi necessário que os todos os requisitos de desenvolvimento de software

fossem atendidos. Vide quadro 5, item de desenvolvimento de *software*. Lembrando que para atingir um nível de maturidade acima todos os itens do nível de maturidade anterior devem estar totalmente atendidos.

Certamente, muitas organizações têm atingido alguns desses critérios em alguns projetos. Entretanto, atingir nível 5 requer uma aderência universal para todos os projetos em todos os grupos de desenvolvimento de projetos. O processo de software CMM pode ser aplicado. Por meio de todo ciclo de vida de desenvolvimento de software, desde os requerimentos até o teste final.

2.5 Comparação entre os níveis de maturidade em desenvolvimento de software e em processos de TI

Uma dúvida comum que sempre surge nas discussões relacionadas à utilização do modelo de maturidade do CobiT é sua relação e semelhanças com o modelo de maturidade do CMM.

Observando os critérios dos níveis de maturidade de desenvolvimento ou mesmo sua adaptação para o CobiT, percebe-se a sua aplicabilidade e abrangência, ou seja, é possível adaptar e aplicar o conceito de nível de maturidade em diversos segmentos independente do sistema ou mercado em que atua. Principalmente em um segmento que necessita de processos de TI consistentes que garantam fé pública que é o caso da certificação digital.

Para apresentar a derivação e a conseqüente adaptação dos modelos de maturidade desenvolveu-se o quadro 5 descrevendo os itens de maturidade do CMM e do CobiT.

Quadro 5 – Quadro comparativo dos níveis de maturidade de desenvolvimento e de processos de TI

Desenvolvimento de Software	**Processos de TI**
0 Não Existente - Não Aplicável	0 Não Existente - Completa ausência de reconhecimento de processos. A organização nem reconhece que existem pontos a serem endereçados
1 Inicial - Nesse nível, o desenvolvimento de software é improvisado, não existe um processo bem definido a ser seguido. O foco está sobre os desenvolvedores chaves ou "heróis" que passam o dia consertando os problemas de software. Organizações nesse nível de maturidade não têm probabilidade de entregar nenhum projeto grande com sucesso, somente projetos muito simples.	1 Inicial - Existem evidências que a organização reconhece que existem pontos a serem endereçados. Entretanto não existem processos padronizados, porém há abordagens improvisadas e tendem a serem aplicadas de forma individual em caso-a-caso. O gerenciamento de todo processo é desorganizado.
2 Repetitivo -Nesse nível, existe foco em gerenciamento de projetos de forma a repetir o processo de desenvolvimento de software. Os processos chave são: a) Gerenciamento de requerimentos: os requerimentos de software são desenvolvidos antes do desenho e da codificação. A cada passo no processo de desenho do software os requerimentos são mapeados para as funções de software de forma a assegurar que todos os requerimentos serão atendidos. b) Planejamento de Projeto de Software: o orçamento e os agendamentos dos projetos de software são feitos de forma precisa. Os engenheiros de software têm a habilidade e experiência correta para cada projeto. c) Controle de projeto de software: os projetos são acompanhados de acordo com o planejado. Gerenciamento de riscos é executado de forma a identificar os riscos de projeto. d) Gerenciamento de Aquisição de Software: Qualquer software adquirido para uso é avaliado em relação ao treinamento, desempenho, usabilidade ou outras limitações que possam impor ao projeto. e) Garantia de Qualidade de Software: cada desenvolvedor é responsável pela qualidade de software. Métricas de qualidade são estabelecidas e a qualidade é acompanhada por	2 Repetitivo - Os processos são desenvolvidos num estágio onde procedimentos similares são seguidos por pessoas diferentes realizando as mesmas tarefas. Não existe comunicação nem treinamento formal dos procedimentos padrões. Existe um alto grau de confiança no conhecimento dos indivíduos e erros são prováveis de ocorrer.

meio das métricas. f) Gerenciamento de Configuração: todos desenvolvedores usam um sistema de controle de revisão para toda codificação do projeto. As bases de software são apropriadamente estabelecidas e acompanhadas.	
3 Definido - As organizações movem-se de um simples gerenciamento de desenvolvimento de software para um foco de processos em engenharia de software. Processos chave: a) Foco do Processo: O foco do processo está firmemente estabelecido na cultura de desenvolvimento da organização. b) Definição de processos da organização: A organização traduz o foco em uma clara definição dos processos em todos os aspectos do processo de desenvolvimento de software que vai das definições de requerimentos iniciais até a aceitação em nível de produção c) Programa de Organização de Treinamento: A organização treina os engenheiros de software nas tecnologias a serem usadas, bem como em todos os processos. d) Gerenciamento Integrado de Software: implementação da categorização, indexação, pesquisa e recuperação dos componentes de software para fomentar a reutilização do software quando possível. e) Engenharia de Produto Software: Softwares individuais não são desenvolvidos de forma isolada, mas como parte de um processo que define a arquitetura de negócios. f) Coordenação de Interação entre projetos: Projetos de software individuais não são definidos de forma isolada. g) Revisões: Acontecem em vários estágios durante o ciclo de vida do software após o desenho, durante a codificação e antes de iniciar o teste unitário.	3 Definido - Os procedimentos são padronizados, documentados e comunicados Por meio de treinamentos. Entretanto, deixa-se que cada um siga esses procedimentos e é improvável que desvios sejam detectados. Os procedimentos não são sofisticados, mas há formalização das práticas existentes.
4 Gerenciado - Nesse nível todo o processo de desenvolvimento de software está definido, mas é gerenciado de maneira pró-ativa. Os processos chave a serem planejados pelas	4 Gerenciado - É possível monitorar e medir a conformidade dos procedimentos e tomar ações onde o processo parece não estar

organizações nesse nível são: a) Compartilhamento de software: a reutilização é feita no processo de desenho seguindo desenhos comuns e padronizados, interfaces, guias de programação e outros padrões. b) Processo de Desempenho: A organização estabelece métricas para avaliar o desempenho dos processos de software. c) Gerenciamento estatístico de processos: Métodos estatísticos são usados e gerenciados no desenvolvimento, implementação e rastreamento do uso do processo e efetividade.	funcionando efetivamente. Os processos estão sob constante melhoria e provêm boas práticas. Automação e ferramentas são utilizadas de forma limitada e de forma fragmentada.
5 Otimizado - É o estado da arte em desenvolvimento de software. Poucas organizações atingiram essa graduação nas avaliações da SEI. Deve demonstrar um processo contínuo de melhoria em desenvolvimento de software. Os processos chave são: a) Prevenção de defeitos: Tem foco em garantia de qualidade, isto é, procura e corrige defeitos, mas em prevenção de defeitos. b) Processo e Inovação em Tecnologia: A organização inova continuamente em novos processos e tecnologias aplicadas no processo de desenvolvimento de software. c) Melhoria no desenvolvimento: Processo contínuo na melhoria do desenvolvimento de software, planejamento, execução, rastreamento e acompanhamento por um cronograma.	5 Otimizado - Os processos estão refinados em nível de melhores práticas com base nos resultados de melhoria contínua e de modelos de maturidade com outras organizações. TI é usado como forma integrada de fluxo de trabalho, provendo ferramentas para melhorar qualidade e efetividade

Fonte: O Autor

3 CERTIFICAÇÃO DIGITAL

Nesse capítulo apresenta-se resumidamente o mercado em que o estudo foi desenvolvido. Inicia-se mostrando pesquisas sobre a utilização da Internet, os perfis de usuários, a necessidade da utilização de certificados digitais e alguns exemplos e conceitos básicos de criptografia.

Em termos de autoridade certificadora, mostra-se a estrutura de certificação digital, alguns requisitos necessários para operação e finalmente as autoridades certificadoras credenciadas no Brasil.

3.1 A utilização da Internet

Com o advento da Internet as pessoas têm direcionado várias de suas atividades para o mundo digital, haja vista a quantidade de recursos disponíveis. A seguir serão mostradas algumas pesquisas realizadas pelo Ibope.

Segundo os dados do Web Brasil, estudo trimestral do IBOPE/NetRatings realizado no penúltimo trimestre de 2005, os *sites* de e-mail, comunidades, busca, jogos on-line e os portais são os principais destaques no uso residencial da Internet entre brasileiros, americanos e espanhóis. (IBOPE, 2005a)

Um dos segmentos da economia que mais se beneficia com o desenvolvimento da Internet é o varejo. A venda eletrônica permite a oferta de uma maior seleção de produtos, para consumidores dispersos geograficamente, com custos operacionais , estoques, locação de lojas, atendimento, reduzidos.

A seguir analisa-se uma pesquisa realizada no Brasil pelo IBOPE/NetRatings publicada em outubro de 2005. Mais de 3,9 milhões de usuários residenciais visitaram *sites* de varejistas on-line em agosto de 2004. Este número representou um aumento de 17,5% superior ao Natal de 2003.(IBOPE, 2005b)

Do total de usuários residenciais no Brasil (11,6 milhões), cerca de 48% visitam *sites* de comércio eletrônico e 35% acessam *sites* varejistas online. Os números são bastante similares aos verificados nos EUA, onde os *sites* de comércio são visitados por 51% e os de varejo, por 37%.

É importante observar os perfis de acesso entre os brasileiros, americanos e espanhóis. Os brasileiros acessam na Internet principalmente as comunidades como Orkut, Gazzag, seguido pelo e-mail, portais e instituições

financeiras. Os americanos usam a Internet para acesso a e-mail, jogos *online* como Counter Strike e Portais de interesse geral.

Os espanhóis têm a mesma preferência que os americanos em relação ao e-mail e em seguida acessam os portais dos fabricantes de software. Esses perfis de acesso estão representados no quadro 6.

Quadro 6 – Cinco principais subcategorias por % sobre o tempo total de exposição - 1o trimestre de 2005 - acesso domiciliar

.**Subcategoria Brasil**		**Subcategoria EUA**		**Subcategoria Espanha**	
Comunidades	20,5%	E-mail	7,7%	E-mail	10,9%
E-mail	11,3%	Jogos On-Line	7,2%	Fabricantes de Software	8,5%
Portais de Interesse Geral	10,5%	Portais de Interesse Geral	6,6%	Ferramentas de Busca	8,4%
Instituições Financeiras	6,2%	Classificados e Leilões	5,0%	Portais de Interesse Geral	6,9%
Ferramentas de Busca	4,7%	Ferramentas de Busca	3,9%	Comunidades	5,1%

Fonte: Web Brasil – 1º Trimestre 2005 – IBOPE /NetRatings

A Internet no Brasil é concentrada na classe A e B e tem características próprias, pois o acesso é feito na escola, na biblioteca, na lanchonete e nos telecentros, diferente dos países de primeiro mundo, onde no mínimo 90% das pessoas que têm acesso à Internet, podem fazê-lo em suas casas. (MAGALHÃES, 2005).

Dos 32 milhões de brasileiros que declararam ter acesso à Internet, 58% acessam a partir de seu domicílio, um número bem inferior aos países desenvolvidos. A figura 11 demonstra como está distribuída a forma de acesso à Internet pelos brasileiros.

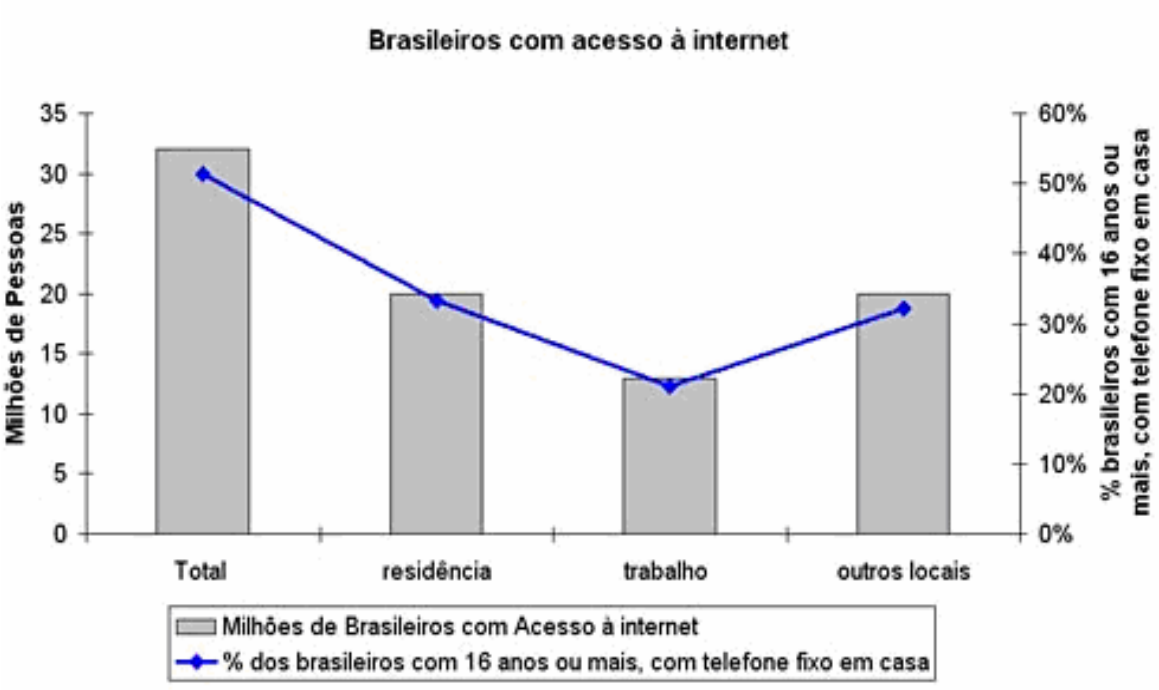

FIGURA 11 – Distribuição dos canais de acesso à Internet
Fonte: Nielsen//NetRatings, 2005

3.2 A identificação na Internet

A maioria dos recursos disponíveis na Internet pode ser utilizada de maneira anônima pelos usuários. Existe uma charge bastante conhecida (Steiner, 1993) que ilustra bem essa situação. Publicada na revista *The New Yorker* em 05 de julho de 1993, a charge mostra um cachorro sentando ao lado de um computador conversando com outro dizendo que na Internet ninguém sabe que é um cachorro que está ali navegando. Realmente é difícil termos certeza de com quem falamos, efetuamos operações ou trocamos correspondências na Internet.

Usando como referência as cartilhas disponíveis no *site* do ITI Brasil, pode-se extrair uma série de conceitos, definições e exemplos.

No mundo físico para se ter certeza da identidade de uma pessoa recorre-se aos cartórios. Para o mundo virtual utiliza-se uma infra-estrutura de chave pública, que funciona de maneira análoga, ou seja, é uma terceira parte que tem fé-pública, tendo como função validar sua identidade digital. Isso tudo é possível por meio de técnicas de certificação digital, que é capaz de prover mecanismos de segurança para garantir a autenticidade, sigilo e integridade às informações eletrônicas.

3.3 A Certificação Digital

Define-se Certificação Digital como um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos. (CARTILHA[..], 200?b)

Em linhas gerais, utilizando-se da Certificação Digital, é possível, por exemplo, evitar que pessoas mal-intencionadas interceptem ou adulterem as comunicações realizadas via Internet. Também é possível saber, com certeza, quem foi o autor de uma transação ou de uma mensagem, ou, ainda, manter dados confidenciais protegidos contra a leitura por pessoas não autorizadas. Embora baseada em conceitos matemáticos altamente sofisticados, a utilização de certificação digital é extremamente simples.

O Sistema de Pagamento Brasileiro (SPB) movimenta milhões de reais a cada dia, utilizando a Certificação Digital para oferecer segurança na transmissão dos arquivos entre os bancos.

A Certificação Digital baseia-se na existência de certificados digitais, que são emitidos por uma Autoridade Certificadora, que é uma entidade considerada confiável pelas partes envolvidas numa comunicação e/ou negociação. Esses certificados podem ser emitidos para pessoas físicas ou jurídicas (incluindo Municípios), equipamentos ou aplicações.

O uso da Certificação Digital emprega técnicas de criptografia. A palavra criptografia tem origem grega e significa a arte de escrever em códigos de forma a esconder a informação na forma de um texto incompreensível. A informação codificada é chamada de texto cifrado. O processo de codificação ou ocultação é chamado de cifragem, e o processo inverso, ou seja, obter a informação original a partir do texto cifrado, chama-se decifragem.

3.4 Conceitos Básicos de Criptografia e Assinatura Digital

A cifragem e a decifragem são realizadas por programas de computador chamados de cifradores e decifradores. Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave que é utilizado para definir como o programa irá se comportar. Os cifradores e decifradores se comportam de maneira diferente para cada valor da chave. Sem o conhecimento

da chave correta não é possível decifrar um dado texto cifrado. Assim, para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave.

A criptografia utilizada no processo de certificação digital é assimétrica ou de chave pública.

Os algoritmos de chave pública operam com duas chaves distintas: chave privada e chave pública. Essas chaves são geradas simultaneamente e são relacionadas entre si, o que possibilita que a operação executada por uma seja revertida pela outra. A chave privada deve ser mantida em sigilo e protegida por quem gerou as chaves. A chave pública é acessível e disponibilizada a qualquer indivíduo que deseja se comunicar com o proprietário da chave privada correspondente.

Para que a mensagem seja enviada em sigilo é necessário que o emissor utilize a chave pública do destinatário, que deve estar disponível em um diretório público acessível na Internet. Por meio do processo de cifragem com a chave pública garante-se o sigilo, pois somente o destinatário poderá decifrar o conteúdo da mensagem utilizando sua chave privada, garantindo assim o sigilo.

Para autenticar a mensagem as chaves são aplicadas no sentido inverso do sigilo, ou seja, o autor do documento utiliza sua chave privada para o processo de cifragem para garantir a autoria do documento ou identificação em uma transação. O destinatário, por sua vez, poderá decifrar essa informação da chave pública do autor.

A assinatura digital utiliza o mesmo método de criptografia de chave pública, operando com uma função resumo também conhecida por uma função de *hash*. O resumo criptográfico é o resultado retornado por uma função de *hash*. Este pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, altera o resumo criptográfico.

A vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, pois os algoritmos de criptografia assimétrica são muito lentos. A submissão de resumos criptográficos ao processo de cifragem com a chave privada reduz o tempo de operação para gerar uma assinatura por serem os resumos, em geral, muito menores que o documento em si. Assim, consomem um tempo uniforme e baixo, independente do tamanho do documento a ser assinado.

Na assinatura digital, o documento não sofre qualquer alteração e o *hash* cifrado com a chave privada é anexado ao documento.

Para comprovar uma assinatura digital é necessário inicialmente realizar duas operações:

a) Calcular o resumo criptográfico do documento;
b) Decifrar a assinatura com a chave pública do signatário.

Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro. Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações no documento ou na assinatura pública.

O certificado digital é um documento eletrônico assinado digitalmente e cumpre a função de associar uma pessoa ou entidade a uma chave pública. As informações públicas, contidas num certificado digita, são o que possibilita colocá-lo em repositórios públicos.

Um Certificado Digital normalmente apresenta as seguintes informações:

a) Nome da pessoa ou entidade a ser associada à chave pública;
b) Período de validade do certificado;
c) Chave pública;
d) Nome e assinatura da entidade que assinou o certificado;
e) Número de série.

3.5 Exemplos da utilização de certificação digital

Um exemplo comum do uso de certificados digitais é o serviço bancário provido via Internet. Os bancos possuem certificado para autenticar-se perante o cliente, assegurando que o acesso está realmente ocorrendo com o servidor do banco. E o cliente, ao solicitar um serviço, como por exemplo, acesso ao saldo da conta corrente, pode utilizar o seu certificado para autenticar-se perante o banco.

Serviços governamentais também têm sido implantados para suportar transações eletrônicas utilizando certificação digital, visando proporcionar aos cidadãos benefícios como agilidade nas transações, redução da burocracia, redução de custos, satisfação do usuário, entre outros.

Outro exemplo que pode ser citado é a utilização da assinatura eletrônica pelo Presidente da República, em seus despachos (decretos de nomeação dos ministros, secretários-executivos e consultores jurídicos dos Ministérios). Essa

prática vem sendo adotada desde o governo anterior com o Presidente Fernando Henrique Cardoso (FAIXA[..], 2002)

Desde o final de dezembro de 2004, o Governador de São Paulo Geraldo Alckmin também realiza seus despachos por assinatura digital. TRAIN (2005)

Entre os campos obrigatórios do certificado digital encontra-se a identificação e a assinatura da entidade que o emitiu, os quais permitem verificar a autenticidade e a integridade do certificado. A entidade emissora é chamada de Autoridade Certificadora ou simplesmente AC. A AC é o principal componente de uma Infra-Estrutura de Chaves Públicas e é responsável pela emissão dos certificados digitais. O usuário de um certificado digital precisa confiar na AC. A escolha de confiar em uma AC é similar ao que ocorre em transações convencionais, que não se utilizam do meio eletrônico.

Por exemplo, uma empresa que vende parcelado aceita determinados documentos para identificar o comprador antes de efetuar a transação. Estes documentos normalmente são emitidos pela Secretaria de Segurança Pública e pela Secretaria da Receita Federal, como o RG e o CPF. Existe, aí, uma relação de confiança já estabelecida com esses órgãos. Da mesma forma, os usuários podem escolher uma AC à qual desejam confiar a emissão de seus certificados digitais.

Para a emissão dos certificados, as ACs possuem deveres e obrigações que são descritos em um documento chamado de Declaração de Práticas de Certificação – DPC. A DPC dever ser pública, para permitir que as pessoas possam saber como foi emitido o certificado digital. Entre as atividades de uma AC, a mais importante é verificar a identidade da pessoa ou da entidade antes da emissão do certificado digital.

O certificado digital emitido deve conter informações confiáveis que permitam a verificação da identidade do seu titular. Por estes motivos, quanto melhor definidos e mais abrangentes os procedimentos adotados por uma AC maior sua confiabilidade.

3.6 As Autoridades Certificadoras

No Brasil o órgão responsável pela regulamentação do uso de certificados digitais é o Instituto Nacional de Tecnologia da Informação – ITI que é uma autarquia federal vinculada à Casa Civil da Presidência da República. Como tal é a primeira

autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

A cadeia de Autoridades Certificadoras é composta pela Autoridade Certificadora Raiz (AC Raiz), pelas Autoridades Certificadoras (AC) e pelas Autoridades de registro, conforme figura 12.

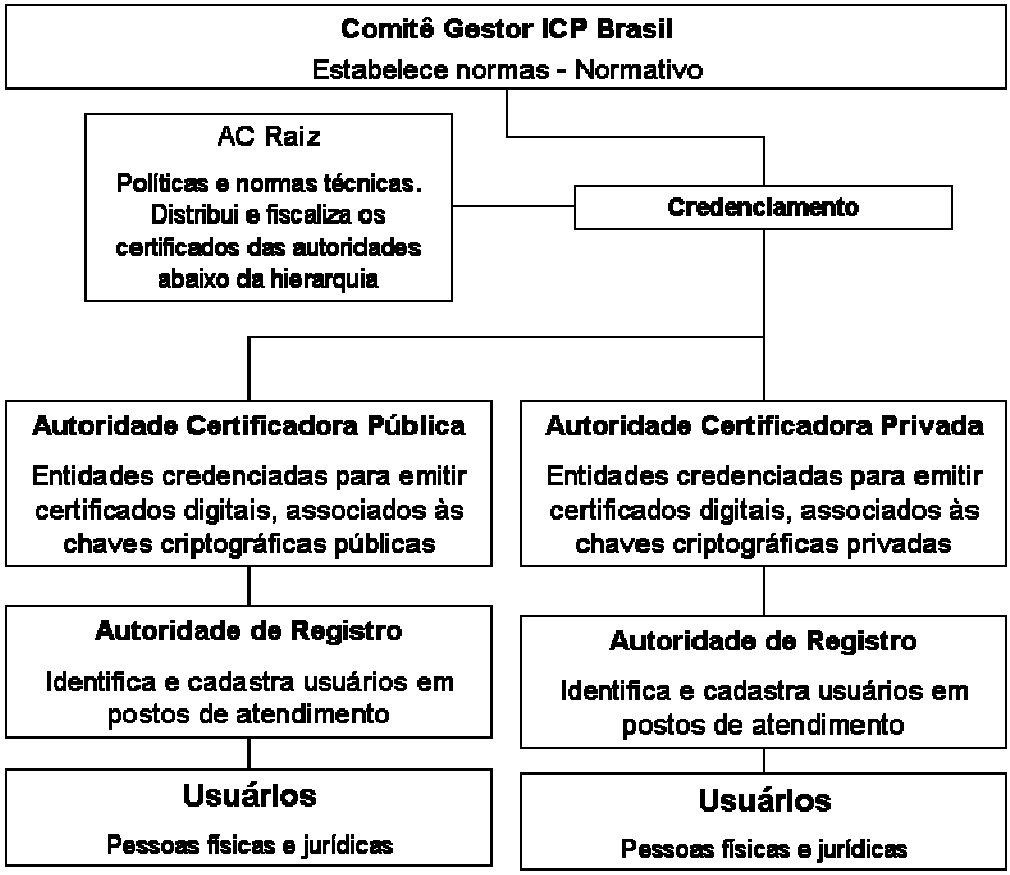

FIGURA 12 – Estrutura ICP Brasil
Fonte: Train, 2005

3.7 Procedimentos e exigências para uma Autoridade Certificadora

No *site* do ITI-Brasil estão disponíveis as resoluções referentes ao assunto Certificação Digital, onde descreve-se os principais itens exigidos para uma Autoridade Certificadora.

No Brasil, o Comitê Gestor da ICP-Brasil é o órgão governamental que especifica os procedimentos que devem ser adotados pelas ACs. Uma AC que se submete às resoluções do Comitê Gestor, pode ser credenciada e com isso fazer parte da ICP-Brasil. O cumprimento dos procedimentos é auditado e fiscalizado, envolvendo, por exemplo, exame de documentos, de instalações técnicas e dos sistemas envolvidos no serviço de certificação, bem como seu próprio pessoal. A

não concordância com as regras acarreta em aplicações de penalidades, que podem ser inclusive o descredenciamento.

As ACs credenciadas são incorporadas à estrutura hierárquica da ICP-Brasil e representam a garantia de atendimento dos critérios estabelecidos em prol da segurança de suas chaves privadas.

O certificado digital, diferentemente dos documentos utilizados usualmente para identificação pessoal como CPF e RG, possui um período de validade. Só é possível assinar digitalmente um documento enquanto o certificado é válido. É possível, no entanto, conferir as assinaturas realizadas mesmo após o certificado expirar.

O certificado digital pode ser revogado antes do período definido para expirar. As solicitações de revogação devem ser encaminhadas à AC que emitiu o certificado ou para quem foi designada essa tarefa. As justificativas podem ser por diversos fatores como: comprometimento da chave privada, alterações de dados do certificado ou qualquer outro motivo.

A AC, ao receber e analisar o pedido, adiciona o número de série do certificado a um documento assinado chamado Lista de Certificados Revogados (LCR) e a publica. O local de publicação das LCRs está declarado na DPC da AC que emitiu o certificado, e em muitos casos o próprio certificado possui um campo com apontador para um endereço eletrônico que contém o arquivo com a LCR. As LCRs são publicadas de acordo com a periodicidade que cada AC definir. Essas listas são públicas e podem ser consultadas a qualquer momento para verificar se um certificado permanece válido ou não.

Após a revogação ou expiração do certificado, todas as assinaturas realizadas com este certificado tornam-se inválidas, mas as assinaturas realizadas antes da revogação do certificado continuam válidas se houver uma forma de garantir que esta operação foi realizada durante o período de validade do certificado. Mas como obter essa característica?

Existem técnicas para atribuir a indicação de tempo a um documento, chamadas carimbo de tempo. Estes carimbos adicionam uma data e hora à assinatura, permitindo determinar quando o documento foi assinado. Essas práticas estão ilustradas na figura 13.

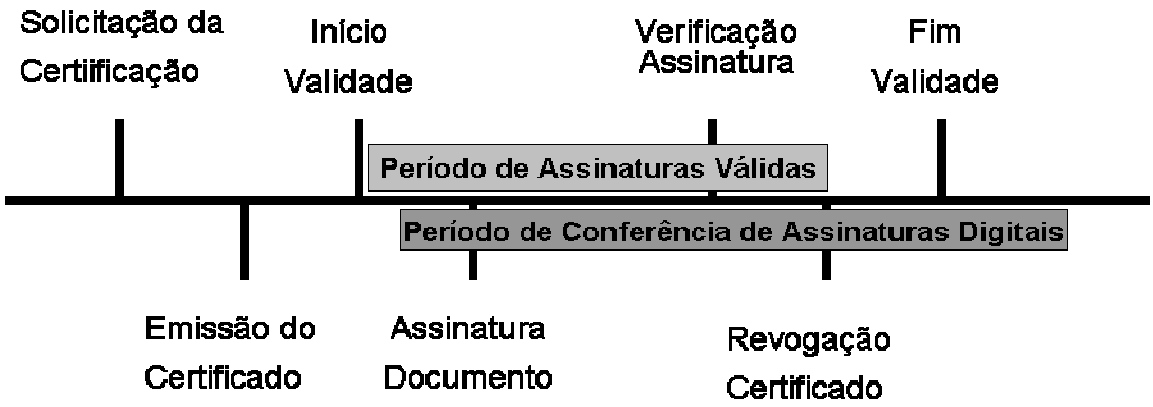

FIGURA 13 – Linha do tempo certificado e assinatura digital
Fonte: ITI, 2005

O usuário pode solicitar a renovação do certificado para a AC após a perda de validade deste. Na solicitação, o usuário pode manter os dados do certificado e até mesmo o par de chaves, se a chave privada não tiver sido comprometida.

Essa renovação pode ser necessária para a substituição da chave privada por uma outra tecnologicamente mais avançada ou devido a possíveis mudanças ocorridas nos dados do usuário. Essas alterações têm como objetivo tornar mais robusta a segurança em relação às técnicas de certificação e às informações contidas no certificado.

Toda essa infra-estrutura é válida desde 24 de agosto de 2001 com a instituição da medida provisória 2200-2, com força de lei, que instituiu o ICP-Brasil e transformou o ITI em autarquia.(MEDIDA [..], 2001)

Nos termos de seu artigo art. 1º, a finalidade da Medida Provisória é garantir a autenticidade, integridade e validade jurídica dos documentos e aplicações que utilizem certificados digitais.

A AC-Raiz brasileira determina as regras operacionais técnicas das demais entidades da ICP e exerce a função de órgão fiscalizador do cumprimento e manutenção dos procedimentos e normas, auditando as práticas das entidades que se candidatam a atuar nesta hierarquia pública, para deferir ou negar o pedido de credenciamento que autoriza a emissão de certificados na ICP-Brasil.

Não é a norma jurídica que garante integridade e autenticidade dos documentos. E sim o procedimento de identificação e associação de titulares de certificados adotado e a segurança do sistema e da tecnologia dos gerenciadores dos certificados que farão isto. Quem garante a autenticidade e a integridade do documento eletrônico é o conjunto dos sistemas e dispositivos de criação e

verificação de assinaturas apropriadas e dos procedimentos adequados para a operação de uma Infra-estrutura de Chaves Públicas (OTONNI, 2005).

A regulamentação definida pelo Comitê Gestor da ICP-Brasil é feita por meio de uma série de resoluções, numeradas de 1 a 37, até a presente data. A resolução número 2 estabelece as diretrizes de segurança que devem ser adotadas pelas entidades que participam da infra-estrutura da ICP-Brasil e fundamenta as normas e procedimentos a serem seguidos. Segundo essa resolução:

> A Política de Segurança Geral da ICP-Brasil tem os seguintes objetivos específicos:
> 2.1.1. Definir o escopo da segurança das entidades;
> 2.1.2. Orientar, por meio de suas diretrizes, todas as ações de segurança das entidades, para reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação e recursos;
> 2.1.3. Permitir a adoção de soluções de segurança integradas;
> 2.1.4. Servir de referência para auditoria, apuração e avaliação de responsabilidades. [ITI, 2001a]

A política de segurança tem, de forma resumida, a seguinte abrangência:

3.7.1 Regras Gerais

- Gestão de Segurança – deve haver uma gestão de segurança pró-ativa amplamente divulgada e conhecida por todos envolvidos de forma direta ou indireta de programas de conscientização. Plano de resposta a incidentes, bem como ativação e manutenção de trilhas de log.
- Gerenciamento de Riscos – esse processo necessita de revisão a cada 18 meses, no máximo, visando à implementação de planos de ação, mitigando os eventuais riscos que possam ser introduzidos no ambiente como, por exemplo, os advindos de novas tecnologias.
- Plano de Continuidade de Negócios – devem ser testados pelo menos 1 vez por ano, de forma a garantir a continuidade dos processos críticos.

3.7.2 Requisitos de Segurança de Pessoal

É um conjunto de medidas e procedimentos de segurança, a serem observados pelos prestadores de serviço e todos os empregados, necessário à proteção dos ativos das entidades participantes da ICP-Brasil. Tendo por objetivo evitar: erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos. Orientar e capacitar todo o pessoal envolvido na realização de trabalhos diretamente relacionados às entidades participantes da ICP-Brasil.

Principais Diretrizes:

a) Processo de Admissão – Devem ser adotados critérios rígidos para o processo seletivo dos candidatos. Devem ser pessoas idôneas e sem antecedentes que não comprometam a segurança ou credibilidade das entidades.
b) Atribuições de Função - Relacionar claramente as atribuições de cada função, de acordo com a característica das atividades desenvolvidas, a fim de determinar-se o perfil necessário do empregado ou servidor.
c) Levantamento de Dados Pessoais - Deve ser elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil.
d) Entrevista de Admissão - Deve ser realizada por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante a pesquisa para a sua admissão.
e) Desempenho da Função - Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança;
f) Credencial de Segurança - Identificar o empregado por meio de uma credencial, habilitando-o a ter acesso a informações sensíveis, de acordo com a classificação do grau de sigilo da informação e, conseqüentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada.

3.7.3 Requisitos de Segurança do Ambiente Físico

É todo ambiente composto por todo ativo permanente das entidades integrantes do ICP-Brasil.

A resolução número 8, ITI (2001b), descreve as condições mínimas para a Declaração das Práticas de Certificação (DPC), onde serão destacados os controles de segurança física, procedimental e de pessoal.

a) Construção e Localização das Instalações - A localização e o sistema de certificação da AC responsável não deverão ser publicamente identificados e internamente não deverão ser admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações deverão ser segregadas em compartimentos fechados e fisicamente protegidos.
b) Controles de segurança física:

- instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;
– instalações para sistemas de telecomunicações;
– sistemas de aterramento e de proteção contra descargas atmosféricas;
– iluminação de emergência.

c) Acesso Físico – Níveis de Acesso - Devem ser definidos pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes da AC responsável e mais 2 (dois) níveis relativos à proteção da chave privada da AC.

- Nível 1 – deverá situar-se após a primeira barreira de acesso às instalações da AC. Para entrar em uma área de nível 1, cada indivíduo deverá ser identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC deverão transitar devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC deverá ser executado nesse nível. Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações da AC, a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização formal e supervisão.

- Nível 2 – será interno ao primeiro nível e deverá requerer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC. A passagem do primeiro para o segundo nível deverá exigir identificação por meio eletrônico e o uso de crachá.

- Nível 3 – deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação da AC. Qualquer atividade relativa ao ciclo de vida dos certificados digitais deverá estar localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não deverão ter permissão para acesso a esse nível. Pessoas que não possuam permissão de acesso não poderão permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão. No terceiro nível deverão ser controladas tanto

as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico e identificação biométrica. Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC, não serão admitidos a partir do nível 3.

- Nível 4 - interior ao terceiro, é onde deverão ocorrer atividades especialmente sensíveis da operação da AC tais como emissão e revogação de certificados, e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades deverão estar localizados a partir desse nível. O nível 4 deverá possuir os mesmos controles de acesso do nível 3 e, adicionalmente, deverá exigir, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas deverá ser exigida enquanto o ambiente estiver ocupado. Todas as paredes, piso e teto deverão ser revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto deverão ser inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não deverão permitir a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - deverão possuir proteção contra interferência eletromagnética externa. As salas-cofre deverão ser construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes. Poderão existir, na AC, vários ambientes de quarto nível para abrigar e segregar, quando for o caso:

a) Equipamentos de produção on-line e cofre de armazenamento;
b) Equipamentos de produção off-line e cofre de armazenamento;
c) Equipamentos de rede e infra-estrutura (*firewall*, roteadores, *switches* e servidores).

- Nível 5 - interior aos ambientes de nível 4, deverá compreender um cofre ou um gabinete reforçado e trancado. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos deverão ser armazenados em ambiente de nível 5 ou superior. Para garantir a segurança do material armazenado, o cofre ou o gabinete deverão obedecer às seguintes especificações mínimas:

a) Ser feito em aço ou material de resistência equivalente;
b) Possuir tranca com chave.

- Nível 6 - deverá consistir de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos deverá dispor de fechadura individual. Os dados de ativação da chave privada da AC deverão ser armazenados nesses depósitos.

3.8 As Certificadoras credenciadas no Brasil

De acordo com o *site* do ITI Brasil (AUTORIDADES[..], 200?) as Autoridades Certificadoras, que hoje atendem aos requisitos definidos pelo ICP-Brasil e hoje credenciadas são:

a) AC-Serpro - O Serpro foi a primeira autoridade certificadora credenciada pela ICP-Brasil. A empresa busca desde a criação de seu Centro de Certificação Digital - CCD, em 1999, divulgar o uso dessa tecnologia para os vários segmentos com que trabalha.
b) AC-Caixa - A Caixa Econômica Federal - atualmente única instituição financeira credenciada como Autoridade Certificadora ICP-Brasil - utiliza, desde 1999, a tecnologia de certificação digital para prover a comunicação segura na transferência de informações referentes ao FGTS e à Previdência Social, dentro do projeto Conectividade Social.
c) AC-Serasa - Para a Serasa, a tecnologia de certificação digital é o instrumento que viabiliza a inserção dos diversos agentes econômicos e cidadãos brasileiros em uma sociedade digital. A Serasa fornece a segurança dos certificados digitais para quase todos os grupos financeiros participantes do Sistema de Pagamentos Brasileiro (SPB).
d) AC-Receita Federal - A Secretaria da Receita Federal (SRF) disponibiliza uma grande quantidade de serviços na Internet, com o objetivo de simplificar ao máximo a vida dos contribuintes e facilitar o cumprimento espontâneo das obrigações tributárias. Por meio do serviço Receita222, a SRF presta atendimento aos contribuintes de forma interativa, via Internet, com uso de certificados digitais, garantindo a identificação inequívoca dos usuários.
e) AC-Certisign - Com o apoio da Certisign, empresa fundada em 1996 com foco exclusivamente no desenvolvimento de soluções de certificação digital para o

mercado brasileiro, importantes instituições vêm adotando a tecnologia nas mais diversas formas.

f) AC-PR - A Autoridade Certificadora da Presidência da República -ACPR foi criada em abril de 2002, por uma iniciativa da Casa Civil, no âmbito do governo eletrônico (e-Gov) e tem como objetivo emitir e gerir certificados digitais das autoridades da Presidência da República, ministros de estado, secretários-executivos e assessores jurídicos que se relacionem com a PR.

g) AC-JUS - A Autoridade Certificadora da Justiça (AC-JUS) reúne o Conselho da Justiça Federal (CJF), o Superior Tribunal de Justiça (STJ) e os cinco Tribunais Regionais Federais. Trata-se da primeira autoridade certificadora do Poder Judiciário.Sua implementação resulta da necessidade crescente de transpor a mesma credibilidade e segurança existentes hoje no mundo do papel para o mundo digital.

h) AC-Sincor - está vinculada ao Sindicato dos Corretores de Seguros do Estado de São Paulo (Sincor-SP). Seu pedido de credenciamento ao ITI foi aceito em agosto de 2005 e a intenção é fazer com que cada corretor se torne um distribuidor de certificado digital para seus clientes.

Um esquema representativo da estrutura do ICP-Brasil é o demonstrado na figura 14:

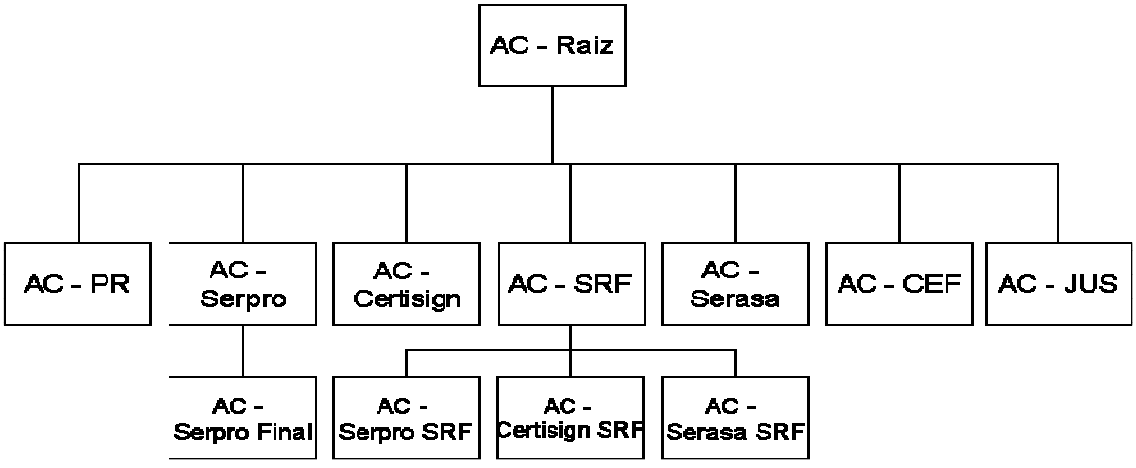

FIGURA 14 – Esquema Representativo da ICP-Brasil
Fonte: Netto,G, 2005

Em 28 de dezembro de 2005 publicou-se (ITI,2005c) que a partir de do início de 2006, a Empresa Brasileira de Correios e Telégrafos (ECT) já está também credenciada para vender certificados digitais

Um ambiente de certificação digital exige uma série de requisitos para garantir a integridade, disponibilidade e sigilo dos certificados digitais que ali foram gerados. Dessa forma, é possível concluir que os processos de tecnologia adotados necessitam ser medidos para que seja possível implementar uma estrutura de Governança de Tecnologia da Informação compatível com a complexidade e criticidade requerida.

4 RESULTADO DA PESQUISA SOBRE A IMPLANTAÇÃO DE GOVERNANÇA DE TI COM BASE EM MODELOS DE MATURIDADE

Nesse capítulo é apresentado o resultado do estudo de nível de maturidade nos processos de TI numa autoridade certificadora.

Para avaliar a aceitação da aplicação dos modelos de maturidade na implementação de um processo de governança de TI, foi desenvolvido e aplicado um questionário com base nos modelos de maturidade. A partir das respostas obtidas foi possível fazer uma análise dos processos de TI selecionados.

4.1 Processos de TI selecionados para o estudo

Medir o nível de maturidade dos processos de TI é o início da implementação de um processo sustentável de governança de TI.

A partir de uma escala de referência, que é aceita internacionalmente, é possível mapear os processos de TI em seu nível de maturidade atual e projetar o nível de maturidade a ser atingido, bem como fazer comparações com a indústria e com a região a qual a organização pertence.

O CobiT não é modelo fechado e pode ser adaptado para cada situação como mostra uma pesquisa sobre o controle e maturidade em governança realizada com base em somente 15 processos do CobiT. GULDENTOPS; GREEMBERGEN e DE HAES (2002).

Dentro do material do *IT Governance Implementation Guide*, existe uma apresentação que exibe uma tendência que aponta para 7 processos de TI dos 34 processos relacionados pelo CobiT. GULDENTOPS *et al* (2003).

São eles:

Planejamento e Organização

- PO1 - Definição do Plano Estratégico de TI
- PO9 - Gerenciamento de riscos
- PO10 - Gerenciamento de Projetos

Aquisição e Implementação

- AI6 - Gerenciamento de Mudanças

Entrega e Suporte

- DS5 - Garantia de Segurança para Sistemas
- DS11 - Gerenciamento de Dados

Monitoramento

- M1 - Monitoramento dos Processos

O modelo de maturidade é construído a partir de um modelo genérico qualitativo onde práticas e princípios são adicionados aos domínios abaixo de forma incremental por meio dos níveis.

a) Entendimento e conscientização dos riscos e controles;
b) Treinamento e comunicação aplicada;
c) Processos e práticas que estão implementados;
d) Técnicas e automação para tornar os processos mais efetivos e eficientes;
e) Grau de conformidade à política interna, leis e regulamentações;
f) Tipo e medida da competência empregada.

O quadro 6 descreve essa aplicação incremental sobre os níveis de maturidade para os diferentes tópicos. Junto com o modelo qualitativo constitui-se um modelo genérico de maturidade aplicável à maioria dos processos de TI.

Segundo Guldentops *et al* (2003b), existem alguns cuidados a serem tomados na utilização do modelo de maturidade. É necessário ter definido o propósito da medição, ou seja, entender claramente o que precisa ser medido e o que fazer com a medida. O modelo não deve ser uma meta, mas deve dar suporte para:

a) Aumentar a conscientização;
b) Identificar os pontos fracos;
c) Identificar as melhorias prioritárias.

Uma abordagem comum é por meio de um grupo multidisciplinar que se reúne, debate e em consenso define o nível de maturidade da empresa, não esquecendo que para atingir um nível acima é necessário que os itens do nível atual sejam totalmente atingidos.

Outra abordagem adotada (PEDERIVA, 2003) é decompor as descrições do nível de maturidade em sentenças em que os envolvidos definem seu nível de acordo por meio das opções: completamente, quase tudo, pouco e nada. O refinamento consiste em adaptar as sentenças de acordo com o ambiente da organização.

4.2 Abordagem

A abordagem adotada para o estudo de caso foi a seguinte:

a) Seleção de uma Autoridade Certificadora;
b) Seleção dos entrevistados relacionados à gestão e operação de uma Autoridade Certificadora:

- Gerente do Centro de Certificação Digital;
- Administradores do Sistema de Certificação Digital;
- Administrador de Sistemas Operacionais;
- Administrador de Segurança.

c) A seleção dos principais processos de TI

- PO1 - Definição do Plano Estratégico de TI;
- PO9 - Gerenciamento de riscos;
- PO10 - Gerenciamento de Projetos;
- AI6 - Gerenciamento de Mudanças;
- DS5 - Garantia de Segurança para Sistemas;
- DS11 - Gerenciamento de Dados;
- M1 - Monitoramento dos Processos.

d) Escolha das dimensões Entendimento & Conscientização e Processos & Práticas do modelo genérico de maturidade;
e) Aplicação de questionário para classificação do nível atual de maturidade dos processos de TI (PO1,PO9, PO10, AI6, DS5, DS11 e M1) e questão formulada para projetar o nível de maturidade desejado (extraída do modelo genérico).

O questionário desenvolvido aborda as principais dimensões do modelo de maturidade, são elas: Entendimento & Conscientização que aborda, de forma resumida, desde o simples reconhecimento da necessidade até a preocupação futura. Já na dimensão Processos & Práticas a variação ocorre desde a abordagem improvisada até as melhores práticas adotadas. No quadro 6 estão destacadas as dimensões selecionadas em termos de modelo genérico de maturidade.

Quadro 7 - Dimensões selecionadas do Modelo Genérico de Maturidade

	Entendimento & Conscientização	**Treinamento & Comunicação**	**Processos & Práticas**	**Técnicas & Automação**	**Conformidade**	**Competência**
1	Reconhecimento	Comunicações esporádicas das questões	Abordagem improvisada para os processos e práticas			
2	Conscientização	Comunicação de todas as questões e necessidades	Processos comuns e similares emergem de forma intuitiva	Ferramentas comuns emergem.	Monitoração inconsistente em áreas isoladas.	
3	Entendimento e necessidade de agir	Treinamento informal dá suporte às iniciativas individuais	Existem práticas definidas, padronizadas e documentadas, compartilhando das melhores práticas.	Técnicas disponíveis correntemente são utilizadas, práticas mínimas são reiteradas; o conjunto de ferramentas torna-se padronizado.	Monitoração global inconsistente; emergem os processos de mensuração; as idéias de *IT Balanced Scorecard* são adotadas; aplicação intuitiva e ocasional de análise de causa.	Envolvimento de especialistas de TI nos processos de negócio.
4	Entendimento completo dos requerimentos	Treinamento formal dá suporte para um programa gerenciado	Proprietários e responsabilidades assinaladas; o processo parece completo; as melhores práticas internas são aplicadas	Técnicas amadurecidas são aplicadas, ferramentas padronizadas são reiteradas; uso limitado de tecnologia.	*Balanced Scorecards* implementados em algumas áreas com exceções notadas pela gerência. Análise de causa padronizada.	Envolvimento de especialistas internos de todos os domínios.

5	Entendimento avançado e preocupado com o futuro	Treinamento e comunicação dão suporte às melhores práticas externas e uso de conceitos e técnicas aprimoradas	Melhores práticas externas aplicadas.	São empregadas técnicas sofisticadas; uso amplo e otimizado de tecnologia.	Aplicação global de IT *balanced scorecard* e exceções consistentemente notada pela gerência. Análise de causa consistentemente aplicada.	Uso de especialistas externos e líderes da indústria.

Fonte: Guldentops *et al*, 2000 - GRIFO NOSSO

4.3 Plano de Implementação de Governança de TI

Situando o estudo de acordo com Guldentops *et al* (2003b) *IT Governance Implementation Guide*, o estudo está na fase: Idealização da Solução.

A fase de idealização da solução é composta de três passos. Primeiramente define-se a situação do processo atual de TI, em seguida define-se em que situação deseja-se estar no processo atual de TI. Finalmente, realiza-se a análise de *gap* entre as situações analisadas e faz-se a tradução para as oportunidades de melhoria.

O CobiT dá suporte para essa fase de idealização da solução por meio:

- Dos fatores críticos de sucesso (CSF) do *Management Guidelines* e modelos de maturidade para avaliação dos níveis de maturidade e definição desses níveis a serem atingidos.
- Dos objetivos de controle e práticas de controle para análise dos atributos de maturidade, análise de *gap* e determinação de oportunidades de melhoria.

4.4 Resultados

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, no quadro 8 segue o perfil de cada um dos participantes selecionados.

Quadro 8 - Perfil dos participantes do estudo

Cargo	**Formação**	**Idade**
Administrador de Segurança	Superior Completo	23
Gerente de Centro de Certificação Digital	Superior Completo	46
Administrador de Sistema de Gerenciamento de Certificação Digital	Superior Completo	51
Administrador de Sistema de Gerenciamento de Certificação Digital	Técnico	46
Administrador de Sistema Operacional	Técnico	52

Fonte: O Autor

A média de idade dos participantes é de 43,6 anos, onde 60% possui formação de nível superior.

A tabulação das respostas do questionário está apresentada no quadro 9.

Quadro 9 - Tabulação das respostas dos participantes

Questões	**1**	**2**	**3**	**4**	**5**	**6**	**7**		**8**
Entrevistados	**PO1**	**PO9**	**PO10**	**AI6**	**DS5**	**DS11**	**M1**	**Média**	**Genérico**
Administrador de Segurança	4	2	4	3	3	1	3	2,9	4
Administrador de SGCD	4	4	4	5	3	3	5	4,0	5
Administrador de SGCD	3	1	1	1	5	5	1	2,4	4
Administrador de SO	3	2	2	2	5	1	1	2,3	3
Médias	**3,5**	**2,3**	**2,8**	**2,8**	**4,0**	**2,5**	**2,5**	**2,9**	**4,0**

Fonte: O Autor

Na figura 15, 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.

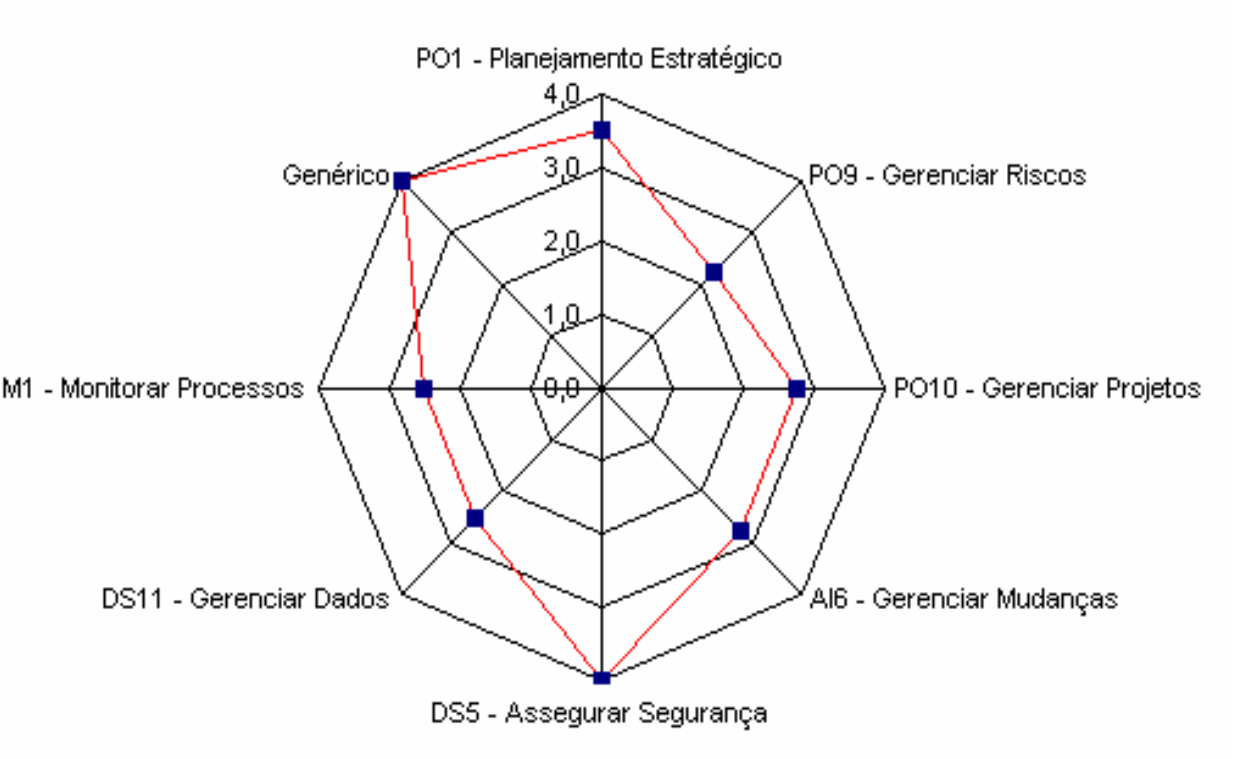

FIGURA 15 - Estudo do nível de maturidade dos processos de TI em uma Autoridade Certificadora
Fonte: o Autor

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 3 e 4, totalizando uma média de 3,5; onde o nível 3 diz que existe uma política que define como realizar o planejamento estratégico e segue uma abordagem estruturada. O processo atual tem embasamento e assegura que um plano está sendo realizado de maneira apropriada.

O nível 4 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. Vide figura 16.

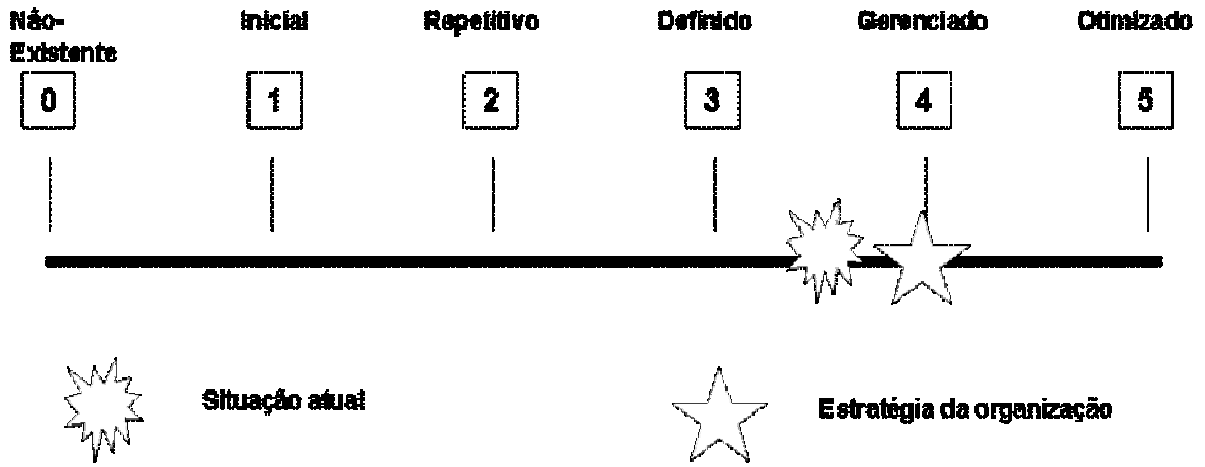

FIGURA 16 – Planejamento Estratégico – PO1
Fonte: o Autor

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 2 define que existe um emergente entendimento que o gerenciamento dos riscos de TI é importante e deve ser considerado. Hoje existe uma abordagem, mas o processo ainda é imaturo, pois é realizado sem muita profundidade e somente em projetos maiores. Vide figura 17.

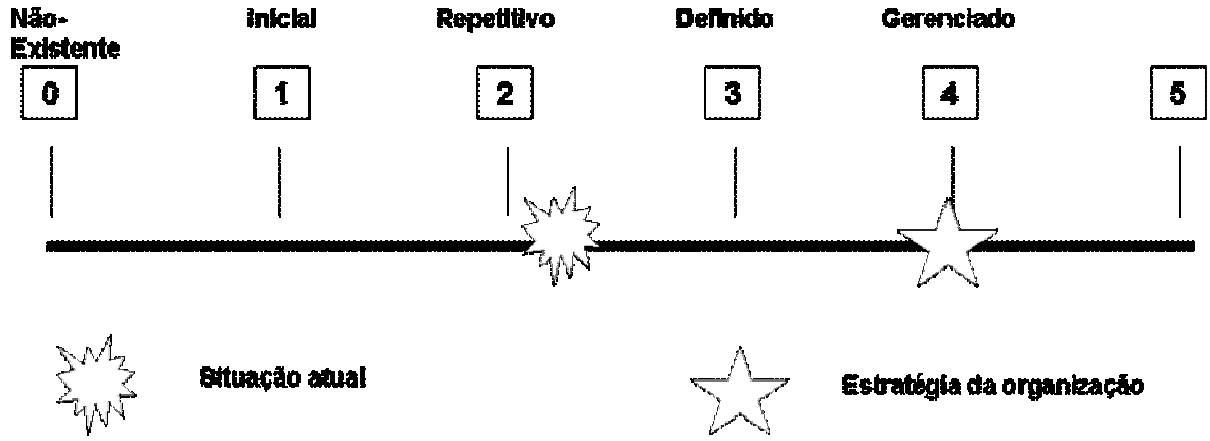

FIGURA 17 – Gerenciamento de Risco – PO9
Fonte: O Autor

O gerenciamento de projeto (PO10) atende a todos os requisitos de nível 2 e quase todos de nível 3. Esse processo foi avaliado com média 2,8, ou seja, com pequenos ajustes teremos o processo com as seguintes características de nível 3 - o processo e metodologia estarão definidos, estabelecidos e comunicados. Os projetos de TI estarão definidos com objetivos técnicos e de negócios apropriados. Vide figura 18.

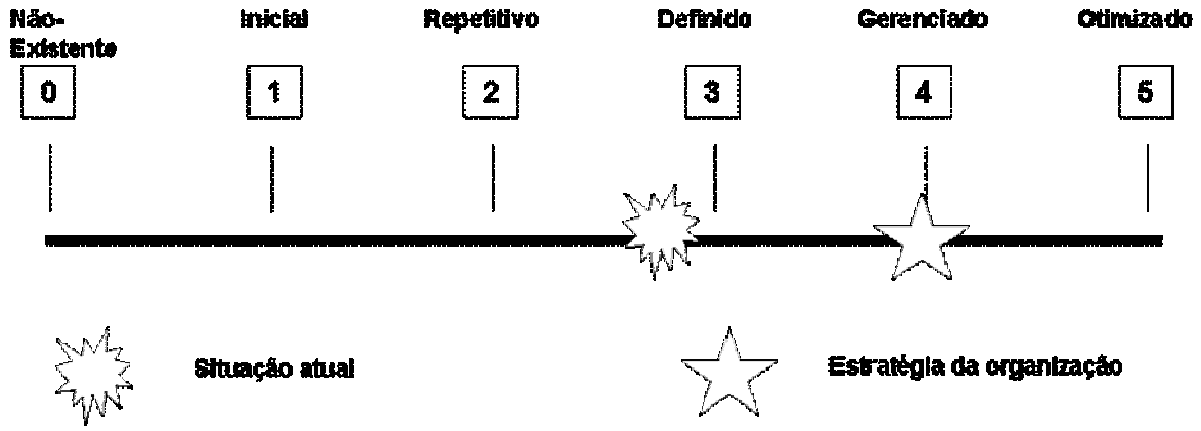

FIGURA 18 – Gerenciamento de Projetos – PO10
Fonte: o Autor

O processo de gerenciamento de mudanças (AI6) tem a mesma média apontada no processo anterior 2,8. Após alguns ajustes o processo estará definido o que inclui: categorização, priorização, procedimentos de emergência, autorização de mudanças e gerenciamento de versões, mas não haverá total aderência e erros ainda poderão ocorrer. Vide figura 19.

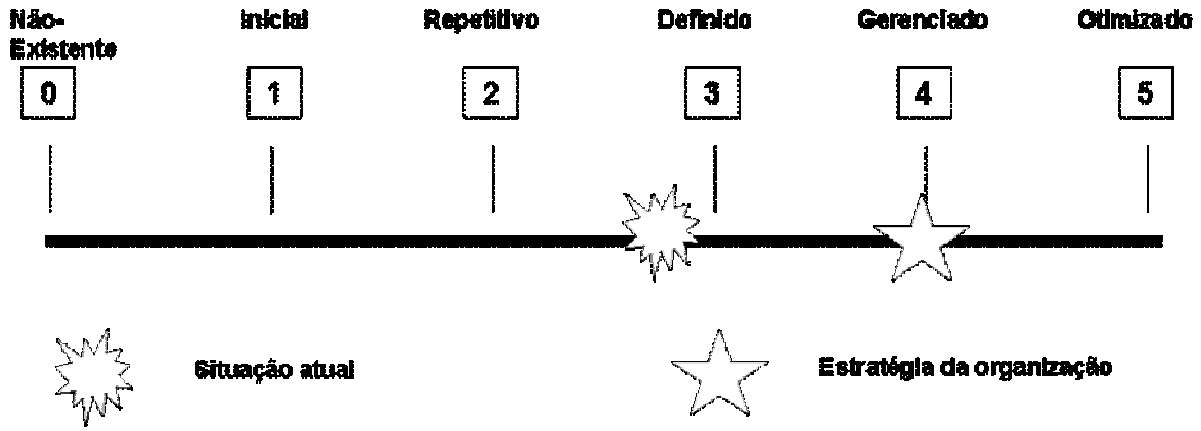

FIGURA 19 – Gerenciamento de Mudanças – AI6
Fonte: o Autor

O processo relacionado à segurança dos sistemas (DS5) foi o item que recebeu a maior classificação do nível de maturidade, recebendo média 4. O principal motivo são os inúmeros itens de segurança física, definidos pelo ITI, que as autoridades certificadoras devem atender. Assim por definição o nível de maturidade 4 possui as seguintes características: 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. Vide figura 20.

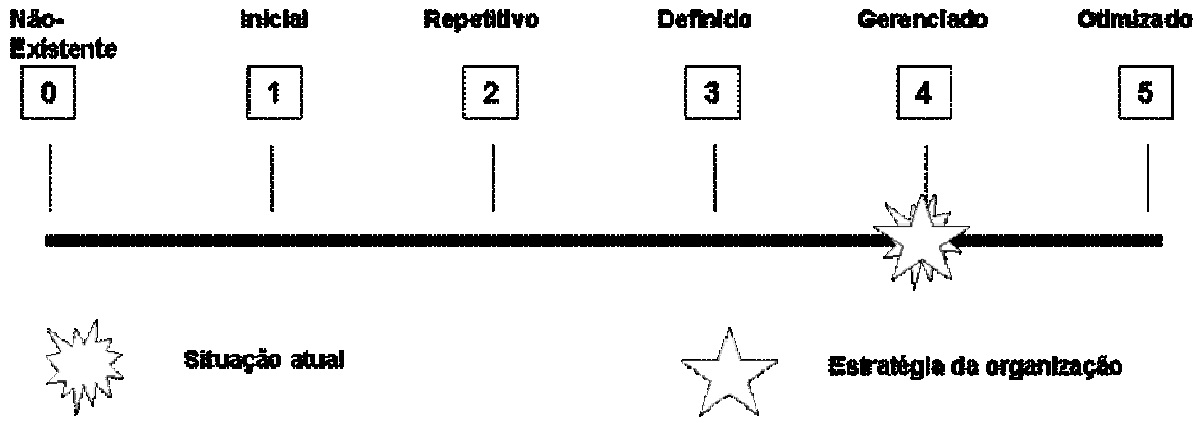

FIGURA 20 – Assegurar Segurança – DS5
Fonte: o Autor

O gerenciamento de dados (DS11) foi classificado com nível de maturidade entre 2 e 3, pois atingiu média 2,5. Atende a todos requisitos de nível 2 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. Atende a alguns requisitos de nível 3, necessitando de um esforço médio para se ajustar aos seguintes requisitos: a necessidade da integridade dos dados dentro da empresa é entendida e aceita. Os padrões de entrada dos dados, processamento e saída estão formalizados e são reiterados. Vide figura 21.

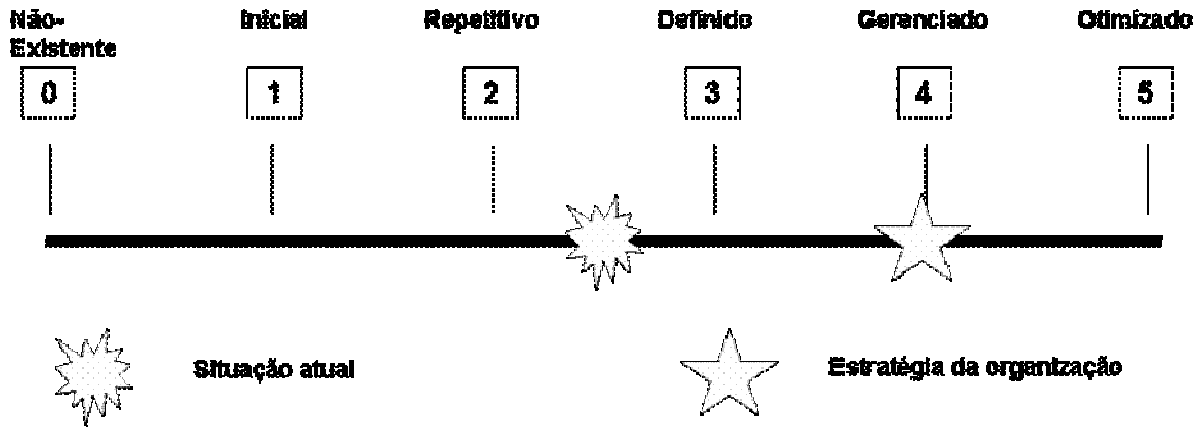

FIGURA 21 – Gerenciamento de Dados – DS11
Fonte: o Autor

A monitoração dos processos (M1) obteve uma média 2,5 entre os níveis de maturidade 2 e 3. Atualmente, o nível de maturidade possui as seguintes características: medidas básicas de monitoração são identificadas. Técnicas e métodos de avaliação e coleta estão definidos, mas o processo de monitoração não foi adotado por toda a organização. Vide figura 22.

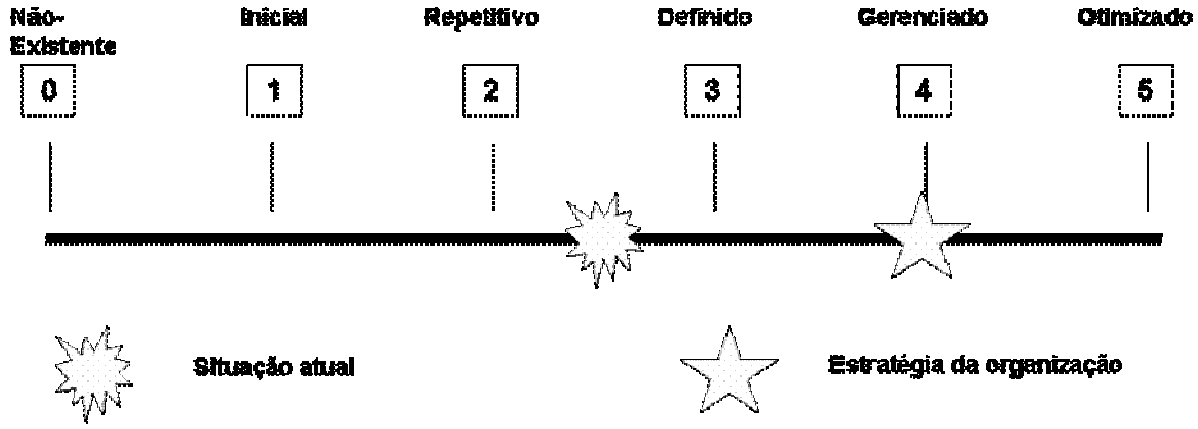

FIGURA 22 – Monitoração dos Processos – M1
Fonte: o Autor

De maneira geral todos os participantes entendem que devem evoluir para um nível de maturidade 4 nos processos avaliados. O modelo genérico de maturidade nível 4 sugere que deve ser possível monitorar os processos, medir sua aderência com os procedimentos e tomar ações onde pareçam não funcionar de maneira efetiva. Devem estar em constante melhoria e provendo boas práticas. 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 há necessidade de se atender a todos requisitos de um nível para atingir o próximo nível.

CONCLUSÃO

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.

Esse estudo de caso intitulado “UM ESTUDO SOBRE A IMPLANTAÇÃO DA GOVERNANÇA DE TI COM BASE EM MODELOS DE MATURIDADE” explorou os seguintes itens:

a) Avaliação dos processos do CobiT versão 3:
   - PO1 - Definição do Plano Estratégico de TI;
   - PO9 - Gerenciamento de riscos;
   - PO10 - Gerenciamento de Projetos;
   - AI6 - Gerenciamento de Mudanças;
   - DS5 - Garantia de Segurança para Sistemas;
   - DS11 - Gerenciamento de Dados;
   - 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 limitação 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 do processo de TI avaliado.

Em uma autoridade certificadora, os processos de TI são fundamentais para a credibilidade do 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 como pudemos observar no quadro 8. Alguns dos participantes não se sentiram confortáveis ao responder algumas das questões propostas, pois como não participam direta ou indiretamente de alguns processos 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).

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.

Esse estudo não teve pretensão de esgotar esse assunto e sim contribuir para os estudos relativos à governança de TI, como por exemplo, indicar uma 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, poderá haver um aprofundamento e novas contribuições nos estudos em Governança de TI.

REFERÊNCIAS

BRASIL. **Medida Provisória 2200-2** – 24/08/2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.Brasília, 2001. Disponível em <http://www.certisign.com.br/companhia/legislacao\index.jsp>, acesso em 01/11/2005

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

Faixa e o Cartão, In: Tema Revista do Serpro**.** Ano XXVII, 164 ed.dez.2002, disponível em <http://www1.serpro.gov.br/publicacoes/tema/164/index.htm>, acesso em 10/11/2005

FERREIRA, A. B.de H. **Dicionário Aurélio Básico da Língua Portuguesa**. Rio de Janeiro: Nova Fronteira, 1995

GRAY,H. **Is there a relationship between IT governance and corporate governance? What improvements (if any) would IT governance bring to the LSC?** 2004. 140f. Tese (MBA), Chartered Management Institute , Londres: 2004

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

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

_____.**IT Control Maturity Survey**. In: IG_Surveys.CD Supplemental Tools and Materials. (Transparência). IT Governance Implementation Guide. IT Governance Institute, 2003.

_____.**IT Governance Implementation Guide**, Rolling Meadows, Ilinois – USA. IT Governance Institute, 2003b.

GULDENTOPS, E. **Maturity Measurement – First the Purpose Then the Method**,.In: Information Systems Control Journal. Rolling Meadows, Ilinois-USA. Volume 4.p.15 -16. jul.2003.

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, Ilinois – USA,.Volume 6. p.32 -35.nov.2002

GULDENTOPS, E. e HAES S.DE. **CobiT 3rd Edition Usage Survey: Growing Acceptance of Cobit.** In:Information Systems Control Journal.Rolling Meadows. Ilinois – USA.., Volume 6. p.25-26. nov.2002

HAMAKER, S. e HUTTON, **A. Principles of IT Governance.** In:Information Systems Control Journal. Rolling Meadows, Ilinois – USA.**,**. Vol 3, p.44 -49. mai.2003

O que é Benchmarking? IAPMEI - INSTITUTO DE APOIO ÀS PEQUENAS E MÉDIAS EMPRESAS E AO INVESTIMENTO, 1996, disponível em <http://www.iapmei.pt/iapmei-bmkartigo-01.php?temaid=2>, acesso em 01/11/2006

IBOPE, In: Pesquisas, **Relatório analisa uso da Internet no Brasil**, **Estados Unidos e Espanha**, 2005a, disponível em <http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=6&proj=PortalIBOPE&pub=T&db=caldb&comp=pesquisa_leitura&nivel=null&docid=4325C3D9D3EDC9998325703E00567FC7>, acesso em 25/11/2005

IBOPE, In: Pesquisas**, Comércio online cresce no Brasil**, 2005b, disponível em <http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=6&proj=PortalIBOPE&pub=T&db=caldb&comp=pesquisa_leitura&nivel=null&docid=031FA8323986190D832570A0006DC058>, acesso em 25/11/2005

ITI - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Resolução no. 2** – 25/09/2001a. In: Legislação. Estabelece as diretrizes de segurança que deverão ser adotadas pelas entidades participantes da Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil.. Brasília, 2001. Disponível em <http://www.iti.br/resolucoes.htm >, acesso em 01/11/2005

ITI - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Resolução no. 8** – 12/12/2001b. In: Legislação. Estabelece requisitos mínimos de observância obrigatória pelas Autoridades Certificadoras (AC) integrantes da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) na elaboração de suas Declarações de Práticas de Certificação (DPC). Brasília, 2001. Disponível em <http://www.iti.br/resolucoes.htm>, acesso em 01/11/2005

ITI - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO**, Autoridades Certificadoras credenciadas pela ICP-Brasil,** 200?a. In: Autoridades Certificadoras**,** disponível em <http://www.iti.br/twiki/bin/view/Main/AutCerti>, acesso em 01/11/2005

ITI - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO**, Cartilha Certificação Digital. Entenda e Use,** 200?b. In:Perguntas Freqüentes, disponível em <http://www.iti.br/twiki/pub/Main/IndiceDasFaqs/CertificacaoDigital.pdf >, acesso em 01/11/2005

ITI - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, In: Certificação Digital**, Correios é a mais nova autoridade registradora do Brasil,** dez/2005c**,** disponível em <http://www.iti.br/twiki/bin/view/Main/AutCerti>, acesso em 14/01/2006

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

JOHNSON, E.*at al*. **IT Governance Global Status Report - 2006**, Rolling Meadows. Ilinois – USA.. 2006

MAGALHÃES, A. **A Internet brasileira tem a cara de seu povo,** 2005.Disponível em <http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=0&proj=PortalIBOPE&pub=T&db=caldb, WNews>, acesso em 26/11/2005

NETTO, G. **Serpro implanta novo software de certificação digital e aumenta a confiabilidade da ICP-Brasil**.In: Tematec encarte da Revista Tema do Serpro. Brasília – Brasil .Volume 81.Ano IX, p.1 – 4. dez.2005

OTONNI, M. B. **Certificação Digital e Segurança**, disponível em <https://www.certisign.com.br/treinamento/guias/pdf/Certificacao_Digital_e_seguranca.pdf>, acesso em 05/11/2005

PAULK, M. C. *et al*, **The Capability Maturity Model: Guidelines for Improving the Software Process,** 19 ed. Pittsburgh, PA – USA: Carnegie-Mellon University, p.3-10, 15-20 e 93 -98, 2003.

PEDERIVA, A. **The CobiT Maturity Model in a Vendor Evaluation Case**. In:Information. Systems Control Journal. Rolling Meadows, Ilinois – USA.. Vol. 3. p.26 -29. jun.2003

Recomendações da CVM sobre Governança Corporativa Comissão de Valores Mobiliários, 2002. Disponível em < http://www.cvm.gov.br/port/public/publ/cartilha/cartilha.doc>, acesso em 21/04/2005

SILVEIRA, A. DI M. **Governança Corporativa Desempenho e Valor da Empresa no Brasil.** 2002. 165f. Tese (Mestrado) - Universidade de São Paulo, São Paulo, 2002

STEINER, P. **On Internet nobody knows you´re a dog**. In: The New Yorker, Vol.69, pág.61.1993, disponível em <http://www.cartoonbank.com/product_details.asp?mscssid=D61394V2K4Q28LKSPVV82XW8B8K660A1&sitetype=1&did=4&sid=22230&whichpage=1&sortBy=popular&keyword=on+internet+nobody+knows&section=cartoons>, acesso em 12/11/2005, 1 charge preto e branco.

TRAIN, S. **Certificação Digital – Conceitos Básicos e Aplicações**, São Paulo: Imprensa Oficial do Estado de São Paulo, 2005

The Development of Hal/S, 199?.UNIVERSITY OF TORONTO. Department of Computer Science disponível em. <http://www.cs.toronto.edu/XPL/hal.html>, acesso em 02/09/2005

YIN, R. K. . **Estudo de Caso: Planejamento e Métodos**. 3 ed. Porto Alegre: Bookman, 2005

BIBLIOGRAFIA COMPLEMENTAR

BERKHOUT, M. *et al*. **ITIL - IT Infrastructure Library – Service Support**. CD. OGC - the Office of Government Commerce.London: 2000

GIL, A.C. **Como Elaborar Projetos de Pesquisa**. 4 Ed. São Paulo: Atlas 2003

HAMILTON, M e KERN, H. **The Software Life Cycle**, In: Articles, disponível em <http://www.informit.com/articles/article.asp?p=24016>, acesso em 02/09/2005

ITI - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO**, O que é Certificação Digital**, In: Cartilhas, 2005, disponível em < http://www.iti.br/twiki/pub/Main/Cartilhas/brochura01.pdf >, acesso em 01/11/2005

KORDEL, L. **IT Governance Hands-On: Using CobiT to Implement IT Governance**. In:Information Systems Control Journal. Rolling Meadows, Ilinois – USA. Volume 2, p.39 – 46, mar.2004

OLIVEIRA, N.M.; ESPINDOLA, C.R. **Trabalhos Acadêmicos:** Recomendações Práticas. São Paulo: Copidart, 2003

ROSSI, R. P. R. **Modelo de Governança de TI para Organizações Brasileiras.** 2004. 226f. Tese (Doutorado) - Universidade Federal de Santa Catarina, Florianópolis, 2004

WRIGHT, J T C e GIOVINAZZO, R A, **Delphi – Uma Ferramenta de Apoio ao Planejamento Prospectivo.** In: Caderno de Pesquisas em Administração, Volume 1, 2000. São Paulo, disponível em <http://www.usp.br/iea/futuro/delphi.pdf>, acesso em 07/11/2005,p.55-57.

GLOSSÁRIO

AC : Autoridade Certificadora é uma entidade de confiança que administra a gestão de certificados digitais por meio da emissão, revogação e renovação dos mesmos por aprovação individual.

AC Raiz: tem como função básica a execução das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor

Análise de *Gap* : processo que compila a lista de todas as ações necessárias para eliminar o intervalo entre a “a posição atual” e a “marca estratégica”

CSF: Critical Success Factores, definem as mais importantes questões ou ações de gerenciamento para atingir os controles de TI Estratégias, técnicas, organizações e procedimentos.

CMM: Capability Maturity Model

CVM : Comissão de Valores Mobiliários.

DPC: Declaração de Práticas de Certificação, documento que descreve deveres e obrigações da autoridade certificadora.

e-GOV: Tem como diretriz estimular o acesso àInternet seja individual, público, ou ainda coletivo e comunitário. A meta é colocar o governo ao alcance de todos, ampliando a transparência das suas ações, e incrementando a participação cidadã.

Hash: Um hash é uma seqüencia de letras ou números geradas por um algorítmo de hashing. Essa seqüencia busca identificar um arquivo ou informação unicamente

LSC : Learning and Skills Council, orgão governamental inglês responsável por financiar, planejar educação e treinamento para maiores de 16 anos.

Telecentros: integram o Projeto de Inclusão Digital criado e mantido pela Coordenadoria do Portal Eletrônico e de Inclusão Digital - Prefeitura de São Paulo. Instalados em áreas periféricas do município, hoje mais de 550 mil usuários estão cadastrados. A primeira unidade desse projeto foi implantada em junho de 2001, na Cidade Tiradentes, zona leste da capital e hoje funcionam 116 Telecentros espalhados por toda São Paulo.

APÊNDICE A

Questionário utilizado para estudo dos níveis de maturidade em processos de TI

Questionário sobre Governança de Tecnologia da Informação

Função:

Formação:

Idade:

1 - O processo de planejamento estratégico de TI tem como objetivos alcançar um balanço ideal entre a melhoria de tecnologia da informação, os requerimentos de negócio e alcance de metas, como você vê o processo de planejamento estratégico de TI de sua empresa?

a. Não é realizado. Não há conscientização da alta administração de que o planejamento estratégico de TI seja necessário para dar suporte aos objetivos de negócio.

b. A necessidade é conhecida pela alta administração.Mas não há uma estrutura de decisão. É realizado conforme necessário, muitas vezes em resposta a um requerimento de negócio e os resultados são esporádicos e inconsistentes.

c. É entendido pela alta administração, mas não é documentado. É realizado pela gerência de TI, mas só é compartilhado com a gerência de negócios se necessário.

d. Existe uma política que define como realizar o planejamento estratégico e segue uma abordagem estruturada. O processo tem embasamento e assegura que um plano apropriado está sendo realizado.

e. É uma prática padrão, mas exceções podem ser notadas. Está definido para uma função sênior. Pode ser monitorado e as informações relativas a decisões são feitas com base em medições de eficácia.

f. É documentado, vivo e continuamente considerado na definição dos objetivos de negócio e os resultados em valores de negócio por meio de investimentos de TI. É feita uma comparação do processo em relação às normas da indústria onde atua. Tem um processo bem definido e é integrado com o processo de planejamento estratégico.

2 - O processo de avaliação de riscos dá suporte às decisões gerenciais para atingir os objetivos de TI e responder à ameaças e identificar importantes fatores de decisão. Classifique o processo atual de avaliação de riscos da empresa.

a. Não ocorre e a empresa não considera os impactos de negócio associados às vulnerabilidades de segurança e com as incertezas advindas de projetos.

b. A empresa está consciente de suas responsabilidades contratuais, mas considera os riscos de TI de maneira improvisada sem seguir processos e políticas definidas. Avaliações informais de risco acontecem isoladamente para cada projeto.

c. Existe um emergente entendimento que os riscos de TI são importantes e devem ser considerados. Existe uma abordagem, mas o processo ainda é imaturo, pois é realizado somente em projetos maiores e sem muita profundidade.

d. Existe uma estrutura e um processo documentado que define quando e como conduzir avaliações de risco.

e. É um procedimento padrão e exceções podem ser notadas. O processo é avançado e o risco é avaliado individualmente por projeto e considera-se toda operação de TI. As mudanças no ambiente de TI que podem afetar o cenário de risco são comunicadas.

f. A estrutura de avaliação de risco está num estágio onde é reiterada, seguida regularmente e bem gerenciada.

3 - O processo de gerenciamento de projetos em TI alinha-se com os objetivos de negócio, define prioridades, entrega produtos no prazo e dentro do orçamento, dessa forma como você vê esse processo na empresa?

a. Técnicas de gerenciamento de projetos não são usadas na empresa e não são considerados os impactos no negócio.

b. A empresa geralmente tem consciência da necessidade da estruturação dos projetos e dos riscos de projetos mal gerenciados. O uso de técnicas de gerenciamento de projeto e abordagem dentro de TI é uma decisão tomada individualmente pelos gestores de TI.

c. Percebe-se a necessidade de gerenciamento de projeto de TI, que tem objetivos técnicos e de negócios definidos informalmente.

d. O processo e metodologia estão definidos, estabelecidos e comunicados. Os projetos de TI estão definidos com objetivos técnicos e de negócios apropriados.

e. São requeridas métricas de projeto padronizadas, formalizadas para completar a revisão do projeto, incluindo as “lições aprendidas” . A avaliação é feita em toda empresa e não somente dentro de TI.

f. Está implementado um ciclo completo e comprovado da metodologia de forma reiterada na cultura da organização.

4 - O processo de gerenciamento de mudanças minimiza a probabilidade de interrupção, alterações não autorizadas ou erros. Como você classificaria esse processo na empresa?

a. Não há um processo definido e as mudanças podem ser feitas sem nenhum controle. Não há consciência que as mudanças podem ser prejudiciais para TI e para os negócios.

b. É reconhecido que as mudanças devem ser gerenciadas e controladas, mas o processo não é consistente para ser seguido, pois existem variações e mudanças não autorizadas podem ocorrer.

c. Existe um processo informal e a maioria das mudanças segue a uma abordagem desestruturada, rudimentar e sujeita a erros.

d. Existe um processo definido que inclui categorização, priorização, procedimentos de emergência, autorização de mudanças e gerenciamento de versões, mas não há total aderência e erros ainda podem ocorrer.

e. O processo é bem desenvolvido e consistentemente seguido para todas as mudanças e não há exceções. O processo é eficiente e eficaz, mas ainda existem procedimentos e controles manuais.

f. O processo é regularmente revisto e atualizado para manter-se em linha com as melhores práticas. É integrado com os negócios para assegurar que TI é um viabilizador de produtividade e criador de novos negócios.

5 - O processo de segurança de TI protege as informações contra uso não-autorizado, revelação ou modificação, danos e perda. Como você classificaria esse processo na empresa?

a. A empresa não reconhece a necessidade da segurança em TI e não existem responsáveis por assegurar segurança de sistemas.

b. A empresa reconhece a necessidade por segurança em TI, mas a conscientização depende de cada um. É realizado reativamente e não é medido, provocando a indicação de culpados porque as responsabilidades não estão claras.

c. As responsabilidades são definidas para um coordenador de TI sem autoridade gerencial. A conscientização é limitada. As soluções de segurança não atendem

necessidades específicas e tendem a responder reativamente aos incidentes de segurança, adotando as ofertas feitas por fornecedores.

d. Existem sessões de conscientização padronizadas e formalizadas que são promovidas por uma gerência. Os procedimentos de segurança de TI estão definidos e atendem a uma estrutura de políticas e procedimentos. As responsabilidades estão definidas, mas não de maneira consistente.

e. 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.

f. Segurança em TI é uma responsabilidade conjunta entre as áreas de negócios e TI e é integrada com os objetivos corporativos de segurança. Os requerimentos estão claramente definidos, otimizados e incluídos na avaliação periódica da implementação do plano de segurança.

6 - O processo de gerenciamento de dados tem como objetivo assegurar que os dados mantenham-se completos, exatos e válidos durante sua entrada, atualização e armazenamento nos sistemas. Classifique como esse processo ocorre na empresa?

a. Os dados não são reconhecidos como um recurso ou bem corporativo. A qualidade e segurança dos dados é ruim ou não-existente

b. A empresa reconhece a necessidade por dados precisos. O processo de detecção de erros e correção depende de atividades manuais ou individuais que não são previamente aprovadas por um comitê. Assume-se que os dados são precisos porque um computador está envolvido no processo.

c. A conscientização da necessidade da precisão dos dados e manutenção da integridade prevalece por toda organização. As regras e requerimentos estão documentados por indivíduos-chaves e não estão consistentes pela organização e plataformas.

d. A necessidade da integridade dos dados dentro da empresa é entendida e aceita. Os padrões de entrada dos dados, processamento e saída estão formalizados e são reiterados.

e. Os dados estão definidos como um recurso e um bem corporativo. Métodos padronizados estão documentados, mantidos e usados para controlar a qualidade dos dados, os dados são consistentes entre as plataformas e unidades de negócio.

f. O gerenciamento dos dados é maduro, integrado e tem um processo aprimorado, claramente definido e tem objetivo de entregar informação com qualidade ao usuário mantendo os critérios de integridade, disponibilidade e confiabilidade.

7 - A monitoração dos processos tem como objetivo assegurar que o desempenho definido para TI seja atingido. Como esse processo é tratado na empresa?

a. A empresa não tem um processo de monitoração implementado. TI não realiza a monitoração dos processos ou projetos.

b. Entende-se a necessidade de coletar e avaliar informações sobre monitoramento dos processos. A monitoração é, em geral, implementada reativamente para um incidente que tenha causado alguma perda ou embaraço para a empresa.

c. Medidas básicas de monitoração são identificadas. Técnicas e métodos de avaliação e coleta estão definidos, mas o processo de monitoração não foi adotado por toda a organização.

d. O processo de monitoração é comunicado e padronizado na empresa. A avaliação ainda é realizada em processos individuais e em nível de projeto e não há integração aos demais processos.

e. As tolerâncias estão definidas dentro de cada processo e existe uma integração de métricas entre todos os processos e projetos.

f. Um processo contínuo de melhorias é desenvolvido para atualizar os padrões e políticas da empresa e incorporar as melhores práticas de mercado. Todos os processos são otimizados e dão suporte para os objetivos da empresa.

8 - Na sua opinião, qual das alternativas abaixo representa o nível ideal em que seus processos deveriam estar para que TI seja um diferencial competitivo, considerando que quanto maiores as exigências, maior será o custo financeiro associado.

a. Não há necessidade de aprimorar processos.

b. A empresa deve reconhecer que existem preocupações a serem tratadas, abordando-os caso-a-caso, sem a necessidade de padronizar os processos.

c. Os processos devem estar num estágio onde procedimentos similares devem ser seguidos, mas não padronizados e não importando quem irá conduzi-los, deixando a responsabilidade para cada indivíduo, dessa forma existe um alto grau de confiança no conhecimento destes.

d. Procedimentos devem estar padronizados, documentados e comunicados por meio de treinamento. Devem ser deixados para que cada um siga esses procedimentos, onde é provável que desvios sejam detectados. Os procedimentos não são sofisticados, mas há formalização das práticas existentes.

e. Deve ser possível monitorar os processos, medir sua aderência com os procedimentos e tomar ações onde pareçam não funcionar de maneira efetiva. Devem estar em constante melhoria e provendo boas práticas. Automação e ferramentas devem ser usadas de maneira limitada.

f. Os processos devem ser refinados ao nível de melhores práticas, com base nos resultados de melhoria contínua e modelos de maturidade comparado-os com outras empresas. TI é usado como forma integrada de automatizar o fluxo de trabalho, provendo ferramentas para melhorar a qualidade e efetividade.