JOÃO CARLOS PEREIRA JUNIOR

Aplicabilidade de um Framework para a Governança de TI

Monografia apresentada ao PECE – Programa de Educação Continuada da Universidade de São Paulo, como parte dos requisitos para obtenção do título de MBA.

Profº Orientador:
Profº Dr. Jorge Risco Becerra

SÃO PAULO
2007

MBA/TI
2007
P414a

DEDALUS - Acervo - EPEL

31500015855

FICHA CATALOGRÁFICA

M2007 C

Pereira Junior, João Carlos
Aplicabilidade de um *framework* para governança em TI / J.C. Pereira Junior. -- São Paulo, 2007.
54 p.

Monografia (MBA em Tecnologia da Informação) - Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1.Governança corporativa 2.Tecnologia da informação I.Universidade de São Paulo. Escola Politécnica. Programa de Educa-ção Continuada em Engenharia II.t.

AGRADECIMENTOS

Ao meu coordenador do Curso: Dr. Jorge Risco Becerra,

Em acreditar que por maior que sejam os desafios do dia-a-dia somos capazes de criar um trabalho de conteúdo e de importância para o fechamento de um curso de MBA !

À minha esposa e filho,

Pela compreensão e total apoio para o desenvolvimento deste trabalho, porque sem esforço e dedicação não fazemos a diferença – somos apenas um número !

Aos meus familiares,

Que sempre acreditaram na minha dedicação e esforço sobre os estudos, sobre o conhecimento e o sacrifício desempenhado para alcançar o sucesso dos objetivos traçados !

Ao meu grande amigo César Martins da Costa,

Líder nato no que diz respeito a liderança de equipes de alta performance, com sua visão de crescimento profissional bem como seu censo humano e de justiça para com seus subordinados !

RESUMO

Este trabalho visa avaliar o contexto atual do mercado em que se exige cada vez mais dos executivos, uma Governança em TI que traga confiança e credibilidade aos seus acionistas e investidores. Com este contexto foram avaliadas 3 metodologias, o que possibilitou assim criar um framework capaz de implementar processos operacionais que possam suportar uma Governança em TI voltada para as necessidades de cada corporação.

ABSTRACT

This work aims at to evaluate the current context of the market where if it demands each time more than the executives, an IT Governance that it brings each time more confidence and credibility to its stakeholders and investors. With this context 3 methodologies had been evaluated that it thus made possible to create one framework capable to implement operational processes that can support an IT Governance directed toward the necessities of each corporation.

SUMÁRIO

LISTA DE ANEXOS E FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AICPA- American Institute of Certified Public Accountants

ANO - Acordo de Nível Operacional

BI - Business Inteligence

ANS - Acordo de Nivel de Serviços

CCTA - Central Computer and Telecommunications Agency do Reino Unido

CEO - Chief Executive Officer

CFO - Chief Financial Officer

CICA - Construction Industry Computing Association

CIO - Chief Infraestructure Officer

COBIT- Control Objectives for Information and related Technology

COSO - Control Objectives for Sarbanes-Oxley

CPD - Central de Processamento de Dados

DTI - Departament of Trade and Industry

EDIFACT – EDI for Administration, Commerce and Transport

ESF - European Science Foundation

GAO - Government Accoutability Office

IFAC - International Federation of Accountants

IIA - Institute of Internal Auditors

ISO - International Organization for Standardization

ITIL - Information Technology Infrastructure Library

ITSEC - Information Tecnology System Evaluation Criteria

ITSMF- IT Service Management Forum

OCDE - Organização para a Cooperação e o Desenvolvimento Econômico

OGC - Office of Government Commerce

Mat. - Maturidade

NIST - National Institute of Standards and Technology

OPM3 - Organizational Project Management Maturity Model

PCAOB- Public Company Accounting Oversight Board

PMO - Process Management Officer

PSM - Process Safety Management

SEI - Software Engineering Institute

SPICE - Software Process Improvement and Capability dEtermination

SW-CMM- Capability Maturity Model for Software

TCSEC- Trusted Computer System Evaluation Criteria

TI - Tecnologia da Informação

1. INTRODUÇÃO

1.1. Contexto Inicial

O princípio básico das organizações é buscar a excelência no gerenciamento de seus processos operacionais internos e externos bem como os seus processos organizacionais, os quais envolvem a plena comunicação com os seus parceiros, colaboradores e fornecedores de soluções de softwares e de hardwares [2].

Esta gestão de processos operacionais e organizacionais requer: um estudo e identificação das suas entidades relacionadas entre si e dos papéis e responsabilidades das áreas que compõe a corporação, bem como o nível de uso e capacidade de mensuração e desempenho sobre os processos operacionais que a corporação possui. Com a identificação e pleno entendimento destes pontos será possível que as corporações avaliem o que possuem, façam as mudanças necessárias para uma gestão de maior controle sobre TI e possam com isso alcançar os objetivos traçados [2].

Atualmente no mercado podem ser estudadas e utilizadas guias, ferramentas ou mesmo diretrizes como COBIT (Control Objectives for Information and related Technology), ITIL (Information Technology Infrastructure Library), COSO(Control Objectives for Sarbanes-Oxley), PSM (Process Safety Management), OPM3 (Organizational Project Management Maturity Model), CMMI (Capability Maturity Management Integration), entre outras, para se fazer a gestão em TI, mas o mais importante é a criação de processos operacionais que permitam efetuar controles bem como dar direcionamentos a TI para possibilitá-la a suportar as áreas de negócios das corporações.

1.2. Objetivo

Esta monografia apresentará um framework de processos operacionais, que sejam capazes de suportar a Governança em TI nas corporações, utilizando-se as diretrizes de COBIT, ITIL e COSO.

Há atualmente no mercado ferramentas que auxiliam no papel dos gestores, em fazer controles operacionais, obtenção de informações consolidadas sobre as operações realizadas de forma setorial ou mesmo departamental, mas nem sempre estes controles

permitirão tomadas de decisões que estejam agregando valores com os objetivos corporativos. Isto significa que há uma necessidade da corporação ter uma visão de informações executivas, gerenciais e operacionais de âmbito geral e total do andamento da empresa e de seus colaboradores. Antes de se associar os processos operacionais da corporação com ferramentas de gestão disponível no mercado, deve-se entender em primeiro lugar que a gestão operacional da corporação requer uma outra visão:

- Se os resultados obtidos com os processos operacionais estão agregando valores aos objetivos traçados pela diretoria da empresa;
- Se os resultados obtidos com os relatórios gerenciais permitem uma avaliação se os objetivos da corporação serão alcançados no final de um período de apuração;
- Se os sistemas de informação permitem que sejam feitas auditorias;
- Se a corporação possui processos de coleta de informações capazes de espelharem a realidade dos processos operacionais da corporação;
- Se as demandas feitas foram devidamente atendidas com as exigências expostas pelos clientes;
- Se há meios de garantir que os resultados que estão sendo esperados pelos acionistas e investidores sejam alcançados no final de um período de apuração.

Estas são alguns pontos que os executivos que estão à frente das corporações refletem no decorrer de sua gestão. O Framework que será apresentado permitirá criar um modelo que possibilite orientar na implantação de processos operacionais voltados a suportar a gestão em TI numa determinada corporação que está sendo avaliada.

O Framework permitirá que seus processos operacionais tragam visões executivas e gerenciais sobre os processos de negócios, bem como a gestão de TI para suportar os objetivos da corporação.

1.3. Justificativa

Conforme citado anteriormente, há várias diretrizes, guias de boas práticas ou mesmo metodologias que podem ser seguidas com o objetivo de suportar a gestão em TI, mas não necessariamente deve-se utilizar todas ou mesmo grande parte destas, mas

com uma combinação de três destas "diretrizes" pode-se obter esta gestão em TI, de forma que CIO (Chief Infraestructure Officer), CFO (Chief Financial Officer) e CEO (Chief Executive Officer) tenham uma visão estratégica da empresa e que possam tomar decisões corporativas e ganhar de seus investidores e acionistas alto nível de confiança e credibilidade frente a gestão que está executando sobre a corporação[2].

A utilização do COBIT está voltada a controles, mensurações e avaliações dos processos operacionais das unidades de negócios da corporação, enquanto que o ITIL está voltado para os processos operacionais da área de infraestrutura, tratando de uma visão voltada para o atendimento a serviços e suporte.

A utilização do COSO está voltada para controles de auditoria e monitoração dos processos operacionais das unidades de negócios, ou seja, auditoria e monitoração dos processos operacionais implementados com base no COBIT.

Os fatores críticos de sucesso sobre este Contexto de Governança em TI suportada pelo COBIT, ITIL e COSO, devidamente aplicadas são:

- A partir de um Modelo Referencial (um framework), será possível implantar processos operacionais numa empresa de forma corporativa ou mesmo de forma setorial (de acordo com as necessidades);
- Manutenção dos processos operacionais baseando-se nos "deliveriables" de cada parte deste framework;
- Aculturamento de todos os colaboradores da corporação, frente as mudanças que ocorrerão no dia-a-dia com a implementações de processos operacionais.

1.4. Metodologia

Esta monografia foi composta pelas seguintes fases:

- Fase 1 – Identificação do tema voltado a gestão de TI
    - Identificação através de periódicos, artigos e palestras de um contexto do mercado envolvendo a Governança em TI – assunto pelo qual vem sendo difundido e buscado pelas empresas;
    - Fazer o entendimento das necessidades das empresas para se implementar processos que garantam a Governança em TI;

- Estudar as diretrizes de COBIT e ITIL para se alcançar a Governança em TI;
- Estudar sobre o Ato Sarbanes-Oxley como forma de auditoria e monitoria dos processos do COBIT;

- Fase 2 – Criação de um Framework
  - Criação de um Framework capaz de implementar processos operacionais voltados para as empresas que necessitam ter uma Governança de TI;
    - Foram obtidos todos os processos de COBIT necessários para controle dos processos de negócios;
    - Foram obtidos também os processos de ITIL necessários para a prestação de serviços (entrega e suporte) voltados para Gestão da Infraestrutura de TI;
    - A unificação destes processos e dividindo-os em níveis de maturidade para serem implementados em fases e em conjunto.
  - A Composição do Framework:
    - Processos que estejam voltados à visão de Negócios e aderentes as diretrizes do COBIT;
    - Processos que estejam voltados a serviços e suporte, com aderência as diretrizes do ITIL;
    - Processos que permitam auditoria e monitoração dos processos de negócios – aderência ao Ato Sarbanes-Oxley.
- Fase 3 – Como Implementar os Processos do Framework

1.5. Resumo do Conteúdo

Primeiramente será descrito o contexto da Governança em TI no que diz respeito a princípios fundamentais e um conteúdo teórico no capítulo 2.

Após a descrição deste contexto o capítulo 3 apresentará as diretrizes do COBIT, ITIL e COSO e o que cada um deles se referem na gestão de processos operacionais de TI e organizacionais envolvendo suas respectivas visões.

No capítulo 4 será apresentado o Framework aderente a estas diretrizes e mostrando que com sua implementação é possível se ter uma Governança de TI na corporação.

No capítulo 5 será descrito como devem ser implantados os processos operacionais do Framework capazes de suportar a Governança em TI. Neste último capítulo será apresentado também a importância de se manter o modelo de processos implementados através da monitoração e das auditorias tanto internas quanto as independentes realizadas por empresas externas.

2. GOVERNANÇA DE TI

2.1. Definições

As empresas que implementaram a Governança Corporativa possuem um diferencial no mercado em que atuam, porque há uma atenção maior pelos investidores em analisar as empresas que estarão empregando seus investimentos. Há casos em que as empresas que possuem uma Governança Corporativa, tem seus valores de mercados mais altos e os investidores acabam por pagar ágios sobre os valores reais, porque os padrões de Governança seguidos pelas empresas asseguram a confiabilidade destes investidores e acionistas [2].

A OCDE (Organização para a Cooperação e o Desenvolvimento Econômico) publicou em 1999 "Princípios de Governança Corporativa", definindo-a como: "*a criação de uma estrutura que determina os objetivos organizacionais e que deve haver um monitoramento do desempenho para assegurar a concretização dos objetivos da empresa* " [2]. Isto significa que as empresas que possuem Governança Corporativa possuem uma estrutura de processos que assegurará que os objetivos organizacionais sejam alcançados, principalmente pelo monitoramento do desempenho da empresa sobre o mercado em que atua.

A OCDE enfatiza que não há um modelo único de uma boa Governança Corporativa, mas faz uma observação: esta Governança cabe a um conselho supervisor responsável pela proteção dos direitos dos acionistas e investidores, ou seja, deve haver uma equipe da alta gerência que trabalhe para implementar os princípios de Governança que assegurem a eficiência dos processos organizacionais [2].

Um elemento fundamental da Governança Corporativa é a Governança em TI, responsável em fazer a gestão de tecnologia da empresa no que diz respeito a investimentos, projetos, gerar indicadores de desempenho e principalmente suportar os processos de negócios da empresa.

Uma definição sobre Governança em TI foi feita no artigo [6]: "*Governança em TI é uma estrutura de relações e processos que dirige e controla uma organização a fim*

de atingir seu objetivo de adicionar valor ao negócio através do gerenciamento balanceado do risco com o retorno do investimento de TI' [6].

A gestão sobre o empregro da tecnologia para suportar processos de negócios representa o mais valioso recurso das empresas. Além disso, num ambiente de negócios altamente competitivo e dinâmico é requerida uma excelente habilidade gerencial em TI para suportar as tomadas de decisões de forma rápida, constante e com custos cada vez mais baixos [3].

Desta forma somente com a gestão de recursos tecnológicos é que se pode ter uma Governança Corporativa. Esta afirmação pode ser melhor explicada através da figura 1 que identifica a atuação e o controle de cada Governança.

A Governança Corporativa necessita de uma visão total e geral da corporação e através desta visão, os executivos tem condições de dar os devidos direcionamentos e traçar os objetivos para atuação da empresa no mercado. A Governança em TI suportará a Governança Corporativa, pois estará ciente dos objetivos corporativos traçados e fará a gestão dos recursos tecnológicos necessários para suportar todo o negócio da empresa.

Este trabalho fará apenas algumas considerações sobre a Governança Corporativa, mas este tem por objetivo a implantação de um Framework que acarretará na prática da Governança em TI.

2.2. Elementos

As empresas atualmente possuem muitos elementos à administrar como: colaboradores, dinheiro, instalações, bom relacionamento com o cliente, mas o maior esforço despendido pelo CEO são os itens "informações" e "tecnologia", porque enquanto uma área de negócios requer mudanças constantes para manter vivo seus processos as áreas de tecnologia buscam manter os sistemas implantados com o menor impacto possível de alterações, às vezes, rígidos as mudanças [2].

A figura 1 permitirá visualizar a abrangência da Governança Corporativa bem como a de TI, assim como identificar a abrangência que esta monografia tratará sobre a Governança em TI.

Os elementos que compõe a Governança Corporativa são:

- Os acionistas e os investidores que possuem expectativas e objetivos voltados para a maximização de lucros das empresas;
- Um conselho executivo que garanta os interesses dos acionistas e investidores, e também garanta o direcionamento da empresa. Este conselho executivo mantém dois canais de comunicação:
    - Um canal de monitoração que permite avaliar e analisar os resultados da empresa, dos problemas ocorridos e soluções de contorno bem como acompanharem o desempenho da empresa;
    - Um canal de divulgação entre os executivos e os demais níveis da empresa. As divulgações de comunicados e de normas são feitas por este canal – assim como os executivos, os gerentes e diretores fazem comunicados sobre as diretrizes táticas tomadas para alcançar os objetivos estratégicos traçados;
- A equipe Executiva Sênior, formada por diretores e gerentes, possuem a responsabilidade de transformar as expectativas e objetivos do conselho executivo e dos acionistas em estratégias de implementações, utilizando-se os colaboradores da empresa. Esta equipe tem também a responsabilidade sobre a gestão destes colaboradores que fazem parte da empresa.
- Elementos da empresa: É tudo que realmente a empresa representa, ou seja, sua existência se faz jus a estes elementos que concretizam as estratégias táticas traçadas e que acabam gerando valor ao negócio da empresa. Os principais elementos são:
    - Humanos.: São todos os colaboradores que trabalham no dia-a-dia do funcionamento da empresa;
    - Financeiros.: Recursos e verbas disponíveis para a execução e implantação de projetos, para atender as estratégias da corporação;

- Físicos.: Recursos necessários para os colaboradores (desde papéis para impressoras até os equipamentos de hardware e software utilizados na produção);
- Propriedade Intelectual.: Colaboradores e prestadores de serviços que além de deter o domínio tecnológico e de funcionamento do negócio da corporação, prospectam melhorias e mudanças sobre a corporação;
- Informações de TI.: São dados que ao serem trabalhados podem informar como está o andamento da corporação, seja com uma visão operacional ou mesmo com uma visão executiva;
- Relacionamento.: Parte em que há uma atuação forte da da área de RH, pois o relacionamento entre setores ou mesmo entre níveis hierárquicos deve existir de forma mais transparente possível.

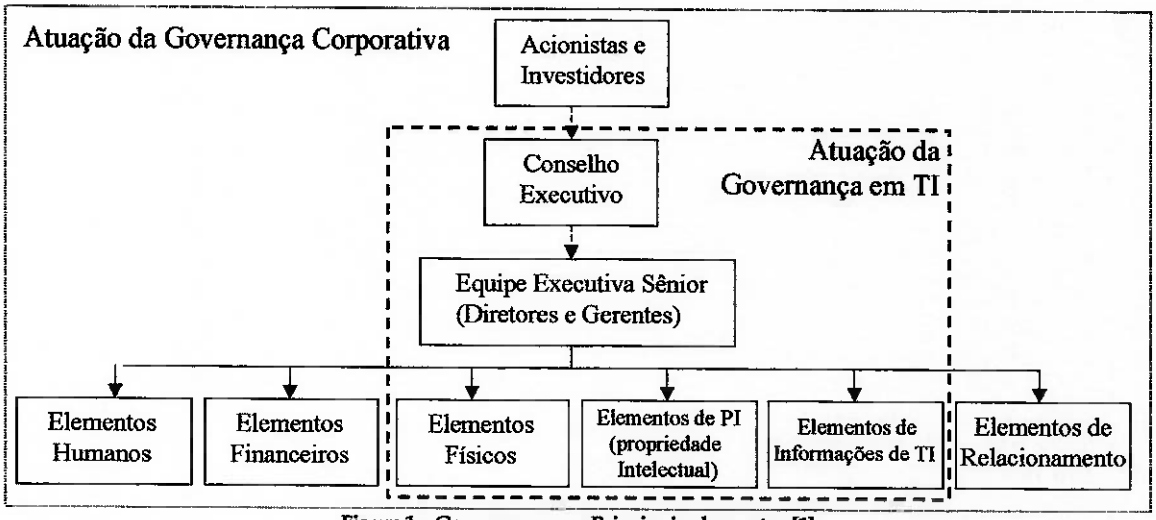

Figura 1 – Governança e os Principais elementos [1]

Por muitos anos as empresas prosperaram no mercado com práticas ineficientes de administração em TI, mas a informação é um elemento fundamental e a cada dia torna-se mais importante para os produtos e serviços organizacionais [1].

A ligação entre os processos de negócios e TI é muito forte, porém não se pode considerar a gestão de TI como sendo a única ou a principal parte deste elo, mas como poderá ser maximizado o uso da TI para suportar as estratégias de negócios das empresas [1].

Para que isto seja possível há necessidade de se ter um elo entre o âmbito da Governança corporativa que dará as devidas diretrizes para a Governança em TI. Os elementos envolvidos na Governança de TI são:

- O conselho executivo;
- A equipe Executiva Sênior;
- Elementos da empresa: Físicos; de Propriedade Intelectual e de Informações de TI.

2.3. Benefícios

Uma pesquisa feita no livro [2] identifica que as empresas que possuem melhores retornos sobre os investimentos feitos em TI agregam este valor de formas diversificadas em seus processos de negócios através:

- Da transparência em deixar claro as estratégias de negócios e o papel de TI para concretizar os objetivos da empresa;
- Mensuram e gerenciam gastos e ganhos com a TI;
- Atribuem responsabilidades pelas mudanças organizacionais necessárias para maximizar cada vez mais os recursos de TI;
- Através de um histórico de conhecimento feito a cada implantação de projetos, tiram lições aprendidas tornando-se mais hábeis no compartilhamento e no reaproveitamento de recursos de TI.

As empresas alcançam o sucesso sobre melhores desempenhos porque implementam a Governança em TI de forma eficiente voltada sempre para sustentar as estratégias corporativas da empresa.

Não existem dúvidas sobre os benefícios da tecnologia aplicada aos negócios, porém para se ter sucesso as organizações devem sempre compreender e controlar os recursos investidos em TI e também avaliar os riscos associados quanto ao uso de novas tecnologias [4]. Isto significa que os investimentos sobre TI devem ser utilizados de forma racional e bem avaliadas principalmente quanto as inovações tecnológicas.

2.4. Diretrizes

A Governança em TI integra e institucionaliza as melhores práticas de planejamento, organização, aquisição, execução e monitoração do desempenho de TI assim como a entrega e suporte aos serviços implementados.

A Governança em TI permite também que avaliações periódicas sejam efetuadas de modo que as vantagens sobre as informações permitam maximizar benefícios e capitalizar oportunidades e vantagens competitivas [2].

A Governança de TI não consiste na tomada de decisões específicas sobre TI, mas se concentra em administrá-la e utilizá-la para concretização das metas de desempenho de âmbito corporativo da empresa, ou seja, estimula e amplifica a engenhosidade de seus colaboradores em empregar a TI voltada para a visão e valores gerais da empresa [1].

Todas as empresas que possuem uma Governança em TI, implementaram um conjunto de mecanismos que estimularam comportamentos ligados diretamente à missão, à estratégia, aos valores, às normas e à cultura da organização [1].

A Governança de TI sempre terá uma lista de demandas interna e externa, e que independente do tamanho e da prioridade destas demandas, estarão sempre acompanhando os princípios da Governança Corporativa: garantia do uso correto de investimentos para TI e a garantia do retorno destes investimentos agregados ao negócio da empresa[2].

Estas garantias traçadas conduzem ao uso da Governança de TI tanto para os controles de recursos tecnológicos quanto à monitoração e gestão das operações de negócios e a sua a capacidade de suporte e entrega de serviços [5].

2.5. Problemas

As empresas que exercem a Governança em TI possuem controles sobre os investimentos de capital voltados para TI, uma monitoração sobre o desempenho de TI, a garantia de que os acordos de serviços para os clientes estão sendo atendidos e também possuem visões que permitam tomar decisões estratégicas para a empresa como um todo frente ao que TI proporciona.

Mas alguns cuidados devem ser tomados pelo fato de que não bastam as empresas terem a Governança em TI como algo que fora estudado e certificado. Deve-se ter a responsabilidade de que a Governança em TI agrega valores aos procesos da empresa. A seguir serão descritos pontos importantes que as empresas se deparam e que causam ineficiência na Governança em TI:

- **A Alta Gerência não vê valor nos investimentos de TI:** Este desentendimento é originado pelas dúvidas e desconhecimentos que os administradores seniores possuem quanto ao valor agregado de TI sobre os negócios das empresas, ou seja, os negócios das empresas só sobrevivem devido aos investimentos de TI que foram efetuados. Diante deste fato, o CEO deve se aprofundar no assunto e se fazerem entender, pois isto possibilitará tomadas de decisões precisas com uma visão da empresa como um todo. O problema surge porque frente a esta dificuldade o CEO acaba abdicando desta responsabilidade, deixando que a diretriz e monitoração dos investimentos de TI fiquem sobre a responsabilidade dos gerentes de TI. Isto poderá acarretar em tomadas de decisões de TI erradas ou mesmo tomadas de decisões divergentes ao direcionamento de negócio da empresa [2];
- **TI torna-se uma barreira para novas implementações estratégicas da empresa:** Como já dito anteriormente, TI não caminha por si só, ou mesmo possui independência das decisões estratégicas do conselho executivo da empresa. A área de TI necessita, principalmente de seu envolvimento com as demais unidades da empresa quando se tratam de implantações de novas tecnologias ou mesmo de crescimento tecnológico. Isto é necessário porque a área de TI mantém todo um "legado" que suporta os negócios das empresas e se numa estratégia executiva é dada a diretriz para mudança da plataforma de TI, isto poderá gerar um impacto tão grande, um risco tão grande para o negócios que impossibilitará a efetivação de um objetivo da empresa [2];
- **Os Mecanismos para se tomar decisões são lentos e contraditórios:** A Governança em TI deve prover consistência para a Gestão de Projetos, pois a Gestão de Projetos deve assegurar a alocação de recursos dedicados, com uma

seqüência disciplinada de realização, com estágios e rastreamento do andamento de projetos – a Gestão sobre projetos permitirá a visualização por parte dos executivos das empresas em avaliar o andamento dos mesmos e se estes projetos não estiverem seguindo as diretrizes estratégicas da empresa como um todo, de nada adiantará serem implantados projetos com objetivos que não estejam alinhados com as estratégias de negócios [2];

- **A Alta gerência vê a terceirização como um reparo aos problemas de TI:** Muitas vezes a terceirização é vista como um reparo rápido das unidades de negócios frente a algum desentendimento ou frustração dos resultados apresentados pela área de TI. Esta atitude se dá pelo fato principalmente porque as áreas de negócios não se preocupam com o valor que possuem em TI, simplesmente estão voltados para a análise de custos. Muitas vezes por agilidade e por custos mais baixos os CEO's acabam por contratar provedores de serviços, porém não para que estes agreguem serviços à TI existente, mas como uma válvula de escape voltada pela redução de custos em sua TI e em tempo de implantação. Isto acarretará num problema que as áreas de negócios deverão garantir contratualmente detalhes técnicos dos serviços dos provedores de TI, que poderão afetar os negócios das empresas [2].

3. DIRETRIZES QUE SUPORTAM A GOVERNANÇA EM TI

Para que as empresas possam suportar a Governança sobre TI, há necessidade principalmente de se ter uma visão do que está se implementando, capaz de suportar os negócios das empresas e como se certificar que estes investimentos agregam valores aos negócios.

Além desta visão deverá ser feito um acompanhamento sobre o desempenho dos processos que suportam os negócios da empresa e assegurar que as diretrizes corporativas serão alcançadas, ou seja, deve ser verificado que os processos de negócios da empresa estão realmente seguindo as diretrizes corporativas dadas pelo alto escalão de executivos.

Estes acompanhamentos e verificações devem se basear em relatórios executivos gerados pelos sistemas de informações, porque sem estes relatórios os executivos não tem condições de avaliar a empresa de uma forma mais precisa e que se permita tomar decisões acertivas.

As diretrizes atualmente publicadas no mercado são variadas conduzindo a forma de gestão da empresa com visões, mas esta monografia utilizará as seguintes diretrizes:

- COBIT: Voltado para controles de processos de negócios;
- ITIL: Voltado para prestação de serviços para suportar os processos de negócios;
- COSO: Auditoria e aderência sobre os processos de negócios.

3.1. COBIT – Control Objectives for Information and Related Tecnology

3.1.1. Definições

O COBIT é um guia para a gestão de TI recomendado pelo ISACF (Information Systems Audit and Control Foundation) e que possui recursos como: um sumário executivo, um framework, controle de objetivos, mapas de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento [3].

As práticas de gestão do COBIT são recomendadas pelos peritos em gestão de TI que ajudam a otimizar os investimentos de TI e fornecem métricas para avaliação dos resultados. O COBIT independe das plataformas de TI adotadas nas empresas [3].

O COBIT é orientado ao negócio. Fornece informações detalhadas para gerenciar processos baseados em objetivos de negócios. O COBIT é projetado para auxiliar três audiências distintas [10]:

- Gerentes que necessitam avaliar o risco e controlar os investimentos de TI em uma organização.
- Usuários que precisam ter garantias de que os serviços de TI suportam os seus produtos e seus negócios para os clientes internos e externos, e que estão sendo bem gerenciados.
- Auditores que podem se apoiar nas recomendações do COBIT para avaliar o nível da gestão de TI e aconselhar o controle interno da organização.

O COBIT recebe um conjunto de contribuições de várias empresas e organismos internacionais, entre eles [10]:

- Padrões técnicos da ISO, EDIFACT;
- Os códigos de conduta emitidos pelo Conselho de Europa, OCDE, ISACA;
- Critérios de qualificação para TI e processos: ITSEC, TCSEC, ISO 9000, SPICE;
- Padrões profissionais para controle internos e auditoria: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO;
- Práticas e exigências dos fóruns da indústria (ESF) e das plataformas recomendadas pelos governos (NIST, DTI);
- Exigências das indústrias emergentes como operação bancária, comércio eletrônico e engenharia de software.

3.1.2. Elementos

O COBIT está dividido em quatro domínios: Planejamento e organização; Aquisição e implementação; Entrega e suporte; Monitoração [10].

A figura 2 ilustra a estrutura do COBIT com os quatro domínios, onde claramente está ligado aos processos de negócio da organização. Os mapas de controle fornecidos pelo COBIT auxiliam os auditores e gerentes a manter controles suficientes para garantir o acompanhamento das iniciativas de TI e recomendar a implementação de

novas práticas, se necessário. O ponto central é o gerenciamento da informação com os recursos de TI para garantir o negócio da organização [10].

Os processos de COBIT possuem seu início a partir de uma necessidade das unidades de negócios da empresa que por sua vez efetiva esta necessidade para TI e esta por sua vez inicia primeiramente:

- O planejamento e organização de recursos para atender esta necessidade;
- Efetua aquisições e implantações de recursos para suportar esta necessidade de negócios;
- A entrega e suporte estão relacionados aos serviços que irão compor esta necessidade de negócios, visto que depois de implementado um novo processo de negócio, ou mesmo uma manutenção este deverá ser mantido por acordos de serviços bem como processos de suporte que por ventura necessitarão;
- A monitoração está voltada não somente para acompanhamento do processo de negócios, mas possui outro objetivo que é permitir que este processo de negócios seja auditado, seja para a funcionalidade do negócio, seja para comprovar a confiabilidade das informações e do negócio.

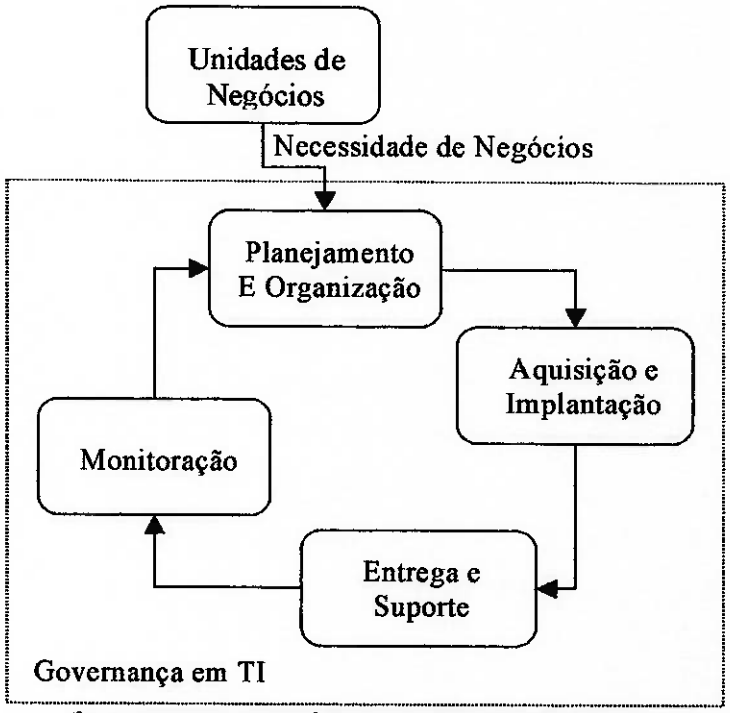

Figura 2: Os quatro domínios do COBIT (traduzido) [10]

A tabela 1 apresenta cada domínio do COBIT que cobre um conjunto de processos para garantir a completa gestão de TI, somando 34 processos [10]:

Tabela 1 – Todos os processos que compõe o COBIT [2]

Planejamento e Organização	**Aquisições e Implantação**
Define o plano estratégico de TI	Identifica as soluções de automação
Define a arquitetura da informação	Adquire e mantém os softwares
Define a direção tecnológica	Adquire e mantém a infra-estrutura tecnológica
Define a organização de TI e seus relacionamentos	Desenvolve e mantém os procedimentos
Gerencia os investimentos de TI	Instala e certifica softwares
Gerencia a comunicação das direções de TI	Gerencia as mudanças
Gerencia os recursos humanos	**Entrega e Suporte**
Assegura o alinhamento de TI com os requerimentos externos	Define e mantém os acordos de níveis de serviços (ANS)
Avalia os riscos	Gerencia os serviços de terceiros
Gerencia Projetos	Gerencia a performance e capacidade do ambiente
Gerencia Qualidade	Assegura a continuidade dos serviços
Monitoração	Assegura a segurança dos serviços
Monitora os processos	Identifica e aloca custos
Analisa a adequação dos controles internos	Treina os usuários
Prove auditorias independentes	Assiste e aconselha os usuários
Prove segurança independente	Gerencia a configuração
	Gerencia os problemas e incidentes
	Gerencia os dados
	Gerencia a infra-estrutura
	Gerencia as operações

A edição atual, coordenada pelo **IT Governance Institute**, introduz as recomendações de gerenciamento de ambientes de TI dentro do modelo de maturidade

de governança. Os modelos de maturidade de governança são usados para o controle dos processos de TI e fornecem um método eficiente para classificar o estágio da organização de TI. A governança de TI e seus processos com o objetivo de adicionar valor ao negócio através do balanceamento do risco e retorno do investimento podem ser classificados da seguinte forma [10]:

- 0 – Inexistente;
- 1 - Inicial / Ad Hoc;
- 2 - Repetitivo mas intuitivo;
- 3 - Processos definidos;
- 4 - Processos gerenciáveis e medidos;
- 5 - Processo otimizados.

Essa abordagem é derivada do modelo de maturidade para desenvolvimento de software, Capability Maturity Model for Software (SW-CMM), proposto pelo Software Engineering Institute (SEI) [10].

3.1.3. Benefícios

Devido a dependência eletrônica do negócio e da tecnologia, as organizações devem demonstrar controles crescentes em termos de segurança, compreender seus próprios desempenhos e medir seus progressos. O benchmarking com outras organizações deve também fazer parte da estratégia da empresa para conseguir a melhor competitividade em TI [10].

O COBIT possui foco de controle sobre os processos de negócios da empresa suportada por TI. Desta forma os benefícios de se executar o COBIT como uma estrutura de governança em TI voltada para controle sobre os processos de negócios da empresa é:

- Permitir o desenvolvimento de uma política desobstruída quanto ao uso de boas práticas de TI e no controle dos processos organizacionais;
- Permitir a integração sobre a estrutura da Governança em TI, ou seja, é possível integrá-lo a outros padrões de gestão, como CMMI, auxiliando na compreensão e no controle de riscos e benefícios associados a TI;

- Ter uma visão dos controles sobre os processos de negócio de acordo com os níveis hierárquicos da empresa (gerentes e diretores);
- Boa aceitação com empresas terceiras e agentes reguladores;
- Permitir aderência as exigências de COSO sobre o controle do ambiente de TI.

3.1.4. Diretrizes

Os fatores críticos de sucesso definem os desafios mais importantes ou ações de gerenciamento que devem ser adotadas para colocar controles na gestão de TI. São definidas as ações mais importantes do ponto de vista do que fazer a nível estratégico, técnico, organizacional e de processo [10].

Os indicadores de objetivos definem como serão mensurados os progressos das ações para atingir os objetivos da organização, usualmente expressos nos seguintes termos [10]:

- Disponibilidade das informações necessárias para suportar as diretrizes e expectativas de negócios;
- Riscos de falta de integridade e confidencialidade das informações;
- Eficiência nos custos dos processos e operações;
- Confiabilidade, efetividade e conformidade das informações.

A avaliação de desempenho define medidas para:

- Determinar como os processos de TI estão sendo executados e se eles permitem atingir os objetivos planejados;
- Definir se os objetivos serão atingidos ou não;
- Avaliam as boas práticas utilizadas e na habilidade da Gestão sobre a TI [10].

3.1.5. Problemas e Restrições

O COBIT possui uma diretriz de implementação, porém não é de fácil entendimento para as empresas porque o COBIT não instrui como fazer a implementação de seus processos, ou seja, ele apenas diz o que fazer.

Outra dificuldade que muitas vezes é encontrada pelas empresas é que o COBIT não trata com desenvolvimento de software ou mesmo com serviços de TI, bem como não fornece um mapa capaz de auxiliar no aprimoramento contínuo de seus processos.

O CobiT demanda um esforço considerável para ser integrado aos processos de uma empresa, porque suas diretrizes por serem muito genéricas acabam obrigando que as empresas acabem por contratar prestadores de serviços com o objetivo de auxiliar no entendimento dos processos.

Foi constatado que o problema maior não está na dificuldade de entendimento e da implementação do COBIT, mas está relacionado principalmente a cultura da empresa, ou seja, relacionado ao fato de que os colaboradores que compõe a empresa como um todo necessitarão mudar o seu modelo operacional de trabalho, passarão a ter mais controles, avaliações e auditorias para se certificarem que a empresa está trabalhando conforme relatórios informativos passado para os executivos.

3.2. ITIL – IT Infraestructure Library

3.2.1. Definições

O ITIL é um conjunto de padrões de "melhores práticas" para o gerenciamento de serviços de Tecnologia da Informação e foi criado nos anos 80 pela CCTA (Central Computer and Telecommunications Agency do Reino Unido). Atualmente é desenvolvido e mantido pelo OGC (Office of Government Commerce) e é sem dúvida a mais completa e consistente documentação de "melhores práticas" para o Gerenciamento de Serviços de TI [6].

Desde os anos 90 o ITIL se tornou um Padrão mundial para o Gerenciamento de serviços, porque além de ser um "framework" de domínio público, possui como foco as melhores práticas e pode ser adotado e adaptado em diferentes formas, de acordo com as necessidades individuais de cada Organização.

O ITIL é adotado e utilizado por várias empresas do mundo e tem crescido como um conjunto de orientações aceita no mercado e estão voltadas para a provisão da qualidade dos serviços de TI e para a administração de instalações do ambiente para dar suporte às operações de negócios [6].

Por este reconhecimento mundial o ITIL tem se desenvolvido para atender as necessidades de TI das empresas incorporando as melhores práticas do ITSM (Information Technology Service Management) [6].

3.2.2. Elementos

Os Processos de Suporte a Serviços

Gerenciamento de Mudanças: É o processo de Planejamento, Controle e Suporte às implantações de mudanças na Planta de TI e tem por principal finalidade a identificação, eliminação de potenciais riscos e impactos que possam gerar indisponibilidade das funções, serviços e infra-estrutura que suportam as operações de negócios da empresa [6].

Gerenciamento de Configuração: É o processo de controle dos Itens de Configuração que compõem a infra-estrutura de Tecnologia da Informação, considerando suas características físicas, conexões e configurações lógicas, desde seu recebimento até sua ativação no ambiente a ser disponibilizado [6].

Gerenciamento de Versões: É o processo que visa assegurar que somente versões autorizadas e corretas serão disponibilizadas para utilização [6].

Gerenciamento de Incidentes: É o processo que define as atividades e responsabilidades para o prosseguimento da disponibilidade dos serviços, caso um incidente ocorra, minimizando impactos nas operações de negócios e atendendo aos níveis de serviços acordados [6].

Gerenciamento de Problemas: É o processo de Encaminhamento, Tratamento e Solução de Problemas relacionados com todas as funções, serviços e toda a infra-estrutura de TI da empresa, buscando a sua solução dentro de níveis de serviços acordados e a diminuição dos tempos médios de finalização dos problemas, de forma a minimizar seus impactos para os clientes internos e externos e visando a máxima disponibilidade para os negócios da empresa [6].

O Service Desk: Ponto único de contato para o cliente no que tange ao atendimento de incidentes e ao encaminhamento de solicitações [6].

Os Processos de Serviços de Entrega

Gerenciamento de Disponibilidade: É o processo que visa otimizar a capacidade da infra-estrutura de TI, serviços e suporte para prover, a custo efetivo, um nível de disponibilidade que permita ao negócio atender seus objetivos. Isto é obtido através da determinação dos requerimentos de disponibilidade do negócio e análise da capacidade da infra-estrutura de TI para atender a estes requerimentos. As lacunas entre requerimento e capacidade são preenchidas através das alternativas disponíveis e opções de custos associados.

Gerenciamento de Continuidade: É o processo de Gerenciamento dos recursos – organizacionais, técnicos e humanos - que logicamente ordenados, garantam a manutenção dos serviços que suportam os negócios da organização, dentro de níveis de serviço acordados, incluindo o suporte mínimo necessário para a continuidade das operações no caso de uma interrupção. Este processo inclui o ciclo contínuo de avaliação de risco e adoção de medidas de contorno, revisão dos cenários e planos de contingenciamento, bem como garantia de aderência às orientações corporativas quanto ao estabelecimento de Planos de Continuidade de Negócios.

Gerenciamento de Capacidade: É processo de monitoração, análise e planejamento do efetivo uso dos recursos computacionais, visando definir e estabelecer uma metodologia apropriada para o acompanhamento e projeção da utilização dos recursos computacionais, incluindo os meios de transmissão de dados e a especificação das métricas e condições ótimas de operação destes recursos.

Gerenciamento de Níveis de Serviço: É o processo de planejamento, coordenação, elaboração, monitoração e reporte dos Acordos de Níveis de Serviço (ANS) e, adicionalmente, às revisões dos indicadores constantes dos acordos celebrados de forma a garantir que os requerimentos de qualidade e custos estão mantidos e gradualmente melhorados. Um ANS deve prover a base para o gerenciamento do relacionamento entre o provedor do serviço e seu usuário.

Gerenciamento de Finanças: É o processo que define o método e as atividades para especificação das peças orçamentárias e seu acompanhamento.

O Gerenciamento de Aplicações

O Gerenciamento de Aplicações refere-se ao complexo assunto de gerenciar aplicações, desde a necessidade inicial do negócio através do ciclo de vida do Gerenciamento de Aplicações até a sua a desativação.

Além disso, o Gerenciamento de Aplicações inclui a interação com as disciplinas do Gerenciamento de Serviços em TI contidas na Entrega de Serviços, no Suporte a Serviços e no Gerenciamento da Infra-estrutura.

O Gerenciamento de Infraestrutura Tecnológica

O ITIL adota uma estratégia orientada a processos que é escalável para atender tanto a grandes, quanto a pequenas organizações de TI e considera o Gerenciamento de Serviços em TI como um conjunto de processos relacionados e integrados.

Para se atingir os objetivos do Gerenciamento de Serviços em TI esses processos devem usar os três P's (pessoas, processos e produtos) de forma eficaz, eficiente e econômica.

Pessoas.: Usuários, Clientes, Equipe de TI e Gerentes, incluídos no contexto de TI, bem como a devida definição dos papéis e responsabilidade de cada um, um bom processo de comunicação e de treinamento.

Processos.: são o coração do ITIL, e considerados como duas áreas principais: o suporte aos serviços e a entrega de serviços.

Produtos: Este item é apenas para completar o tripé da Gestão de Serviços em TI, onde existem atualmente ferramentas disponíveis para as organizações de TI, que são consideradas "aderentes a ITIL"ou seja, que podem auxiliar na implementação e execução dos serviços em TI.

Figura 3: elementos do ITIL [6]

3.2.3. Benefícios

O ITIL está Organizado em um conjunto de textos que são definidos por funções relacionadas: Suporte a Serviços, Entrega de Serviços, Gerenciamento de Aplicações, Gerenciamento de Mudanças e Gerenciamento de infraestrutura. Adicionalmente a esses textos, os serviços e produtos do ITIL, incluindo treinamento e qualificação de pessoal, ferramentas de suporte, e grupos de usuários, tais como o IT Service Management Forum (itSMF), trazem benefícios para as Organizações, tais como [6]:

- Fortalecimento dos Controles e do Gerenciamento dos ambientes de TI;
- Orientação a processos com significativa redução nos tempos de execução e distribuição de serviços;
- Diminuição gradativa da indisponibilidade dos recursos e sistemas de tecnologia da informação, causados por falhas no planejamento de mudanças e implantações em TI;
- Redução dos tempos médios de solução de problemas de TI;
- Atuação na causa raiz dos problemas, com foco no negócio;
- Elevação dos níveis de satisfação dos usuários internos e clientes com relação à disponibilidade e qualidade dos serviços de TI;
- Redução dos custos operacionais de TI;
- Diferencial competitivo;
- Reconhecimento da capacidade de Gerenciamento pelos acionistas, colaboradores e clientes;
- Aderência às instruções normativas das entidades reguladoras e certificadoras.

3.2.4. Diretrizes

A estratégia de implantação do ITIL, voltada para o Gerenciamento de Serviços, é uma diretriz que está orientada a processos para a entrega e suporte de serviços em TI, com foco no cliente. Este foco atende as metas de custo e performance estabelecidos em conjunto com os clientes, ligando os processos de Negócios aos Acordos de Níveis de Serviços (ANS´s) e Acordos de Níveis Operacionais (ANO's).

As implementações dos processos de ITIL voltados a suportar os processos de negócio de uma organização requer conhecimento e domínio total sobre seus processos que permitam responder de forma rápida e eficiente as demandas de negócios bem como ser flexível o bastante para se adaptar as mudanças, sem causar interrupção no fluxo dos negócios.

A Entrega de Serviços tem relação com o Gerenciamento do Relacionamento com o Cliente (CRM – Customer Relationship Management) e faz a ligação entre a organização de TI e o Negócio que deseja atingir seus objetivos empresariais. Para o Cliente, o CRM é a forma de acesso a área de TI. Já a parte de Suporte a Serviços preocupa-se em garantir que o Cliente tenha acesso aos serviços apropriados para sustentar as funções de negócio.

3.2.5. Problemas e Restrições

Em muitas organizações de TI não existe um mecanismo estruturado de suporte ao cliente porque normalmente são implementadas Centrais de Serviços com suportes de Segundo e Terceiro nível. Mas, todos esses departamentos ficam tentando resolver os mesmos incidentes, cada ligação.

Freqüentemente há um problema com a comunicação e cooperação entre os departamentos, resultando em lentidão na solução de incidentes e na qualidade dos tempos de resposta. Isto faz com que haja uma baixa confiança dos Clientes, e que os mesmos tentem resolver pessoalmente seus problemas com telefonemas.

A maioria das organizações é muito reativa e orientada a interrupções. Os recursos de suporte não são gerenciados adequadamente e ficam, apagando incêndios, resolvendo incidentes e problemas repetidamente, ao invés de eliminá-lo.

Um outro problema é a falha das equipes de TI em focar nas necessidades e questões dos Clientes. Os recursos da equipe de TI e custos relacionados não são, na maioria das vezes, muito claros, e nem sempre se sabe o que as pessoas fazem e porque elas estão ali. Nem sempre todas elas realmente se conhecem.

Em muitas organizações de TI acontecem, todos os dias, mudanças sem coordenação e não documentadas e um controle das mudanças inadequado acaba consumindo muito dinheiro e recursos, porque as coisas têm que ser refeitas.

Um outro problema é a abrangência de poucos ANS - Acordo de Nível de Serviços - acarretarão em problemas no alcance dos objetivos e na melhoria da qualidade dos serviços da corporação.

Desta forma os problemas podem ser divididos em três áreas principais:

- Atendimento aos Clientes:
    - Falta de um mecanismo estruturado de suporte ao cliente;
    - Baixa confiança e pouca percepção do cliente com relação a TI;
    - Falta de foco nas necessidades dos clientes.
- Gerenciamento:
    - Suporte sob uma estrutura com pouca gerência e falta de recursos;
    - Problemas sendo resolvidos repetidamente ao invés de eliminados;
    - Qualidade inconsistente no atendimento e nos tempos de resposta;
    - Falta de coordenação e de registro das mudanças.
- Informações gerenciais não disponíveis para tomadas de decisão.

3.3. COSO - Control Objectives for Sarbanes-Oxley

3.3.1. Definições [7]

O ato de Sarbanes-Oxley de 2002 foi criado para restaurar confiança de investidores dos mercados públicos dos Estados Unidos, devastados por escândalos e lapsos nos negócio envolvendo governanças corporativa. Embora reescrevessem literalmente as regras de contabilização corporativa, bem como a sua divulgação, as páginas inumeráveis do ato da sustentação legal seguem uma premissa simples: a governança corporativa e as práticas éticas de negócio já não são mais opcionais em IT, mas são leis.

O ato Sarbanes-Oxley representa a parte a mais significativa de uma legislação sobre os negócios, desde a última metade do século, pois evidencia a contabilização corporativa. Entretanto, é importante enfatizar que a seção 404 não requer apenas que as

empresas estabeleçam e mantenham uma estrutura interna adequada à controle, mas avaliar também sua eficácia anualmente, ou seja, para aquelas organizações que começaram o processo de conformidade e que a TI exerce um papel vital suportando os componentes de sistemas, de dados e de infraestrutura e que são críticos no processo de relatório financeiro.

Em 2003 o PCAOB emitiu um padrão propondo que fosse discutida a importância da TI no contexto de controles internos. A natureza e as características de uma empresa de TI que faz uso de seu sistema de informação afeta o controle interno da mesma sobre relatórios de desempenhos financeiros.

3.3.2. Elementos [7]

Exemplificando melhor os papéis e responsabilidades dos executivos das empresas e qual a atuação sobre as seções 302 e 404, abaixo segue uma pequena tabela da composição do COSO:

Tabela 2 – Seções 302 e 404 da Lei Sarbanes Oxley

Requerimentos da Lei Sarbanes-Oxley		
Lei →	**Seção 302**	**Seção 404**
Responsáveis	CMO, CEO e CFO	CMO, CEO e CFO
O quê	→ Avaliar a eficácia de controles de divulgação (com foco no tamanho das mudanças e na avaliação mais recente); → Avaliar mudanças no controle interno sobre relatórios financeiros; → Divulgar todas as deficiências e fraquezas sabidas do controle; → divulgar atos de fraudes.	→ avaliar o projeto e a eficácia dos controle interno sobre o relatórios financeiros; → divulgar todos os controles sabidos, deficiências significativas e fraquezas materiais; → divulgar atos de fraudes.
Quando	Em vigor desde jul/2002	Em vigor desde jun/2004
Periodicidade	Trimestral pelos executivos	Anualmente pelos executivos e por auditores independentes

É importante demonstrar também como os componentes de COSO controlam e sustentam sua estrutura. COSO identifica cinco componentes essenciais de controle interno eficaz. A figura 4 mostra que os 5 componentes do COSO incidem sobre os componentes do COBIT.

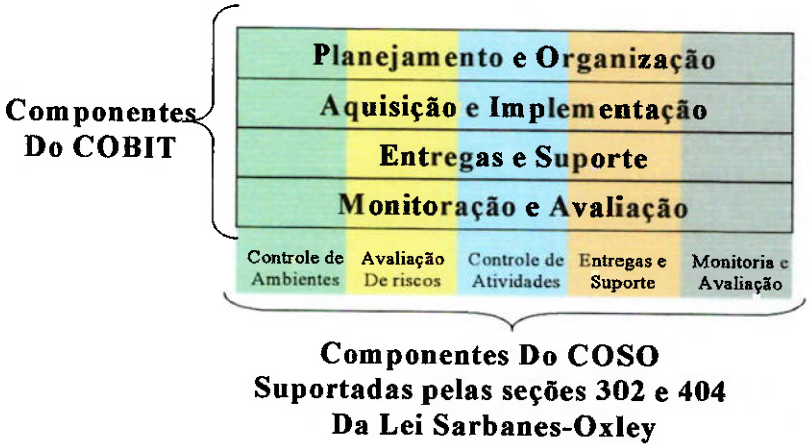

figura 4 - Processos de auditoria e controle do COSO sobre os Processos do COBIT

Controle de ambiente

Este componente cria a fundação para um controle interno eficaz, e representa o topo da estrutura da governança corporativa e este controle de ambiente aplica-se para toda a organização.

Avaliação de risco

Envolve a identificação e a análise pela gerência de riscos relevantes para alcançar os objetivos predeterminados, que dão forma à base para determinar atividades do controle. A avaliação de risco pode ocorrer no nível da companhia (para a organização total) ou no nível de atividade (para uma unidade específica do processo ou de negócio).

Controles de atividades

Os controles de atividades são políticas, procedimentos e as práticas que são publicados para se assegurar de que os objetivos de negócio estejam sendo seguidos e as estratégias de riscos mitigados. O controle de atividades são desenvolvidos para dirigir-se especificamente a cada objetivo de controle para mitigar os riscos identificados.

Informação e comunicação

COSO indica que a informação é necessária em todos os níveis de uma organização para suportar o negócio e para que se tenha um controle dos objetivos da empresa. Entretanto, a identificação, a gestão e a comunicação da informação relevante representam um desafio crescente ao departamento de TI.

A determinação do tipo de informação que é requerida para conseguir objetivos de controle, e a comunicação desta informação num modelo e no tempo correto é o que permitirá aos executivos realizem suas avaliações.

Monitoração

Monitorar cobre todo o controle interno da gerência de TI com os processos contínuos e da avaliação periódica. Este processo de monitoria está tornando-se cada vez mais importante para gerência de TI. Atualmente existem dois tipos de monitoração de atividades: a contínua e a separada por avaliações.

3.3.3. Benefícios [8]

O trabalho requerido para atender as exigências do ato de Sarbanes-Oxley não deve ser considerado apenas como um processo de conformidade com a Lei, mas como uma oportunidade de estabelecer modelos fortes de governança projetados para assegurar as expectativas e objetivos dos acionistas e investidores bem como as exigências do negócio. Construir um programa de controle interno forte dentro de TI tem como benefícios:

- Fortalece a compreensão dos executivos em TI;
- Melhorias nas tomadas de decisões de negócio devido a melhor e mais precisa informação sobre TI;
- Alinha iniciativas do projeto com as exigências do negócio;
- Impede a perda de recursos intelectuais e a possibilidade de ruptura do sistema como um todo;
- Contribui à conformidade de outras exigências regulamentadoras, tais como a privacidade de Vantagem do competidor, do ganho com operações mais eficientes e mais eficazes;

- Otimização de operações com uma maior exatidão integrada à segurança;
- Disponibilidade e integridade de processamento de informações;
- Reforça a competência da gerência de risco e priorizações de iniciativas.

3.3.4. Diretrizes [7]

Com o contexto dos mercados de capitais em suas respectivas economias, houve a necessidade de se ligar a Governança Corporativa sadia com os controles interno e eficaz dos executivos que estão à frente destas empresas.

Os profissionais de TI, especialmente os executivos, verificaram que tanto na teoria quanto na prática, os controles internos encontram-se com as exigências do ato da Lei Sarbanes-Oxley e que os CIO tem agora como desafio:

- Realçar seu conhecimento sobre os controles internos que a empresa possui;
- Identificar os controles de processos de negócios da empresa que estão em conformidade com a Lei Sarbanes-Oxley;
- Planejamento do aumento do nível de controles sobre TI, integrando-a na planta total de conformidades da Lei Sarbanes-Oxley.

O objetivo desta publicação é oferecer a seguinte orientação àqueles responsáveis para empresas:

- Avaliar o estado atual do que se controla no ambiente;
- Projetar as melhorias de controles necessários de acordo com as diretrizes da seção 404 da Lei Sarbanes-Oxley;
- Unir estes dois pontos respaldados sobre as seções 302 e 404 de Sarbanes-Oxley.

4. O FRAMEWORK

Neste capítulo será detalhada a composição do framework que esta monografia se propõe a sugerir bem como uma sugestão de mudança na hierarquia organizacional que possa suportar os controles dos processos operacionais.

4.1. Definições

A composição do Framework aplicará os componentes do COBIT, ITIL e COSO na criação de processos operacionais capazes de:

- Contribuir para os controles necessários para a visão de negócios;
- Contribuir na Gestão de Serviços e Suporte de TI para sustentar os negócios;
- Permitir monitoramento e auditoria sobre os processos de negócios.

A visão de Negócios possui os processos do COBIT e estão divididos por níveis de maturidade (de 1 a 5) a serem implementados. Assim como o COBIT, o ITIL também possui um nível de maturidade (de 1 a 5) que as empresas seguirão para implementar as visões voltadas para Entrega de Serviços e Suporte a Serviços de TI. Já o COSO possui sua incidência sobre os processos do COBIT, onde cada um dos seus componentes intervem sobre as 4 visões do COBIT.

Os pontos de convergência ou que possuem o mesmo foco de gestão, estarão sob responsabilidade de uma área de infraestrutura fazendo uso das diretrizes do framework voltados para "Serviços e Suporte", porém esta gestão deverá ser feita de forma transparente para as unidades de negócios e para o corpo executivo da organização sobre as seguintes informações consolidadas:

- Do cumprimento dos ANS´s;
- Da gestão de mudanças;
- Dos problemas e incidentes ocasionados;
- Da Garantia da disponibilidade e Continuidade dos negócios (testes de "catástrofes e desastres", ativações de CPD´s (Central de Processamento de Dados) fisicamente localizados em outra região;
- Dos níveis de serviços da área de atendimento a clientes.

Não basta apenas efetuar a leitura e o entendimento dos componentes do Framework e tentar implementar na organização processos de controles, sem avaliar também se há uma estrutura organizacional que permita efetuar a gestão de negócios e de TI bem como saber a forma de comunicação que a organização faz uso para divulgações de informações entre as diversas hierarquias que possuem internamente.

Os passos para se implantar os processos do Framework são:

- Fazer o Reconhecimento da Empresa:
    - Conhecer os níveis hierárquicos;
    - Conhecer o Modelo Operacional da empresa – de forma setorial ou departamental:
        - Identificar os tipos de controles que existem nestes modelos;
        - Identificar a dependência entre os setores ou departamentos para se concluir uma tarefa ou mesmo atividade operacional.
- Conhecer o sistema de informação da empresa:
    - Identificar os processos de Negócios da Empresa;
    - Identificar o veículo de comunicação da empresa – como é utilizado;
    - Identificar a forma de armazenamento e extrações de informações bem como sua divulgação – sistema de BI (Business Inteligence);
    - Identificar a existência de alguma ferramenta capaz de ter processos de "workflow" de documentos associados aos modelos operacionais da empresa.
    - Identificar qual o percentual ou freqüência com que os colaboradores utilizam-se destes "workflows";
- Mapear no Framework os processos existentes na empresa, ou mesmo, adequações aos processos atuais obtendo-se aderência ao COBIT. Com espe mapeamento será avaliado o nível de maturidade dos processos;
- Junto a este nível, é sugerido um organograma hierárquico para a empresa: este organograma poderá modificar os papéis e responsabilidades de colaboradores ou mesmo de setores inteiros, ou então uma mudança organizacional que criará novos cargos e/ou setores;

- Avaliar o nível de maturidade com que a empresa trabalha atualmente com o controle dos seus processos;
- Avaliação dos resultados obtidos com a implantação deste 1° nível de Governança;
- Após esta avaliação e à medida em que os resultados forem apresentando melhoras com uma performance e uma boa aceitação sobre todos os envolvidos, será o momento de criarmos novos mecanismos capazes de elevar o nível de maturidade de todos os processos implantados;
- Sendo assim, um novo ciclo de reconhecimento da empresa deverá ser realizado e um novo estudo sobre o que deverá ser implantado se iniciará.

4.2. Estratégia de Criação do Framework

A criação do Framework se deu através da necessidade de se ter processos de controles de negócios e processos de controles voltados para prestação de serviços (entrega e suporte a serviços) capazes de englobarem dentro de TI as áreas que suportam os negócios da empresa e na garantia dos serviços prestados.

4.3. Elementos

4.3.1. Os Componentes Voltados para Negócios

Para que se possa efetivar a implantação dos componentes de processos operacionais voltados para o negócio da organização, em primeiro lugar deverão ser levantados o domínio e o grau de utilização dos processos operacionais atuais. Este mapeamento é independente da tecnologia atualmente utilizada ou mesmo a que será implementada, ou seja, é necessário primeiramente conhecer os processos operacionais internos da organização, verificar o quanto são "dominados" e o seu grau de utilização.

Assim como o CMMI, o Framework possui uma pontuação de maturidade sobre os processos voltados para o negócio e que permite as empresas avaliarem o nível em que estão e como evoluir para melhorar seus processos operacionais. Este resultado é obtido através de auditorias externas e independentes.

O Framework apresentado está sub-dividido nas fases de maturidade, e que a partir do nível 1 (inicial) pode-se ter uma diretriz da empresa em fazer avaliações com auditorias externas, para se medir a maturidade do nível em que se encontra e até obter uma evolução sobre estes níveis.

A seguir foram classificados os processos operacionais do COBIT em uma necessidade inicial e respeitando-se os níveis seguintes de maturidade. Este nível representa os processos que inicialmente necessitarão ser implantados pela corporação. A partir deste nível será necessário avaliar e auditar a abrangência com que estes processos são utilizados pela corporação e como será possível subir um nível buscando-se a excelência na gestão de TI.

Tabela 3 – Componentes de COBIT que compõe o Framework

Planejamento e Organização	**Mat.**	**Entrega e Suporte**	**Mat.**
Define o plano estratégico de TI	1,2	Define e mantém acordos de níveis serviços (ANS)	1,2
Define a arquitetura da informação	4	Gerencia os serviços de terceiros	4
Define a direção tecnológica	3	Gerencia a performance e capacidade do ambiente	1,2
Define a organização de TI e seus relacionamentos	4	Assegura a continuidade dos serviços	1,2
Gerencia os investimentos de TI	1,2	Assegura a segurança dos serviços	3
Gerencia a comunicação das direções de TI	4	Identifica e aloca custos	1,2
Gerencia os recursos humanos	3	Treina os usuários	4
Assegura o alinhamento de TI com os requer. externos	5	Assiste e aconselha os usuários	5
Avalia os riscos	1,2	Gerencia a configuração	4
Gerencia Projetos	1,2	Gerencia os problemas e incidentes	1,2
Gerencia Qualidade	3	Gerencia os dados	4
Aquisições e Implantação	**Mat.**	Gerencia as operações	1,2
Identifica as soluções de automação	5	**Monitoração**	**Mat.**
Adquire e mantém os softwares	1,2	Monitora os processos	1,2
Adquire e mantém a infra-estrutura	1,2	Analisa a adequação dos controles	4

tecnológica		internos	
Desenvolve e mantém os procedimentos	3	Prove auditorias independentes	1,2
Instala e certifica softwares	5	Prove segurança independente	4
Gerencia as mudanças	1,2		

Neste framework pode-se constatar que o nível inicial (1) e o repetitivo (2) possuem 15 componentes do COBIT de um total de 34 processos. Estes 15 processos são essenciais e abrangem as 4 visões do COBIT.

O nível 3 (processos definidos) são acrescidos mais 5 componentes, pois este nível de maturidade identifica que a empresa possui conhecimento de seus processos, tendo-os bem definidos e disseminados.

O nível 4 (Processos gerenciáveis e medidos) são acrescidos mais 9 componentes do COBIT, pois este nível demonstra que a empresa além de ter seus processos bem definidos e disseminados, ela já é capaz de gerenciá-los e medi-los de forma que demonstre sua capacidade de avaliações, através de métricas, e ter o poder de decisão bem mais apurados e afinados.

O nível 5 fecha a quantidade total de 34 processos implementados na organização, onde demonstra que a organização possui pleno controle dos processos, o poder de avaliação sobre métricas geradas para tomadas de decisões e uma automatização destas informações.

A seguir teremos a representação dos processos do Framework que abrangem as visões do COBIT.

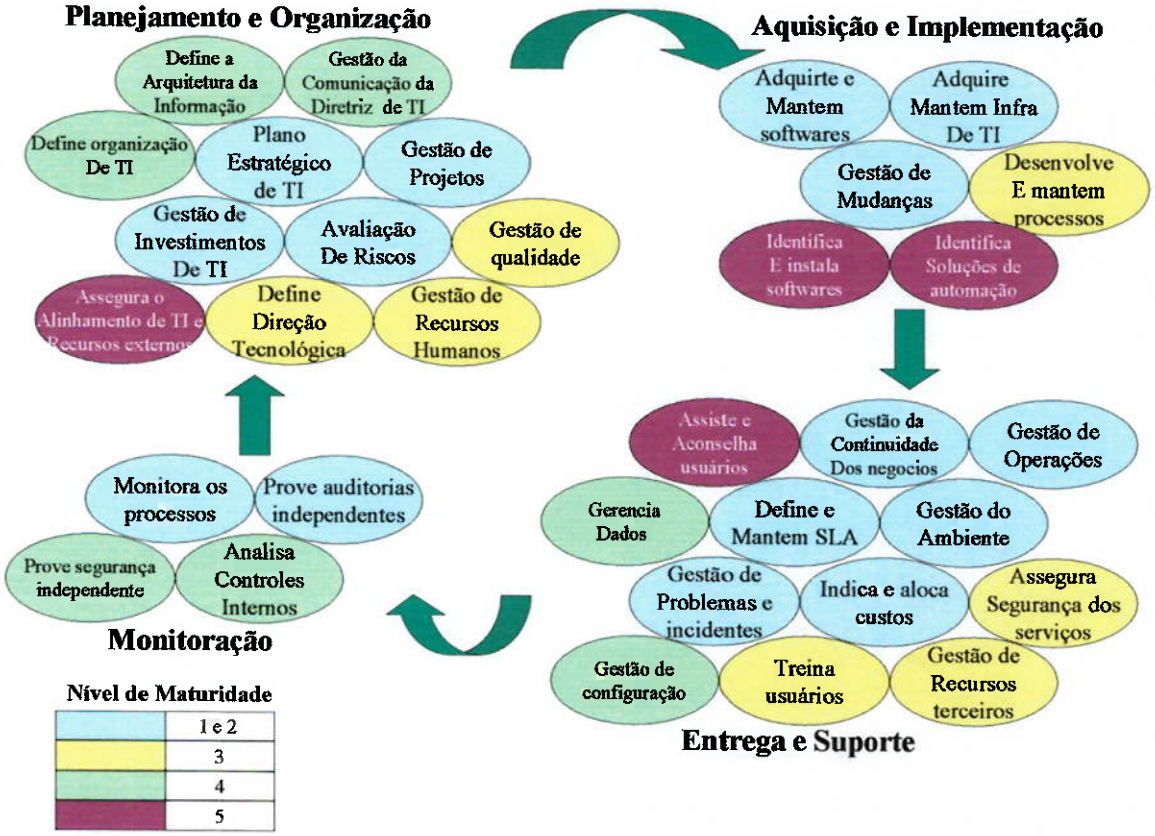

Figura 5 - Componentes de COBIT que compõe o Framework

Os processos apresentados em azul no workflow acima representa exatamente os níveis 1 e 2 do framework (para as visões do COBIT), onde temos processos iniciais ou mesmo repetitivos. A medida em que vamos subindo o nível de maturidade aparecem os processos em amarelo que representam o conhecimento dos processos organizacionais e sua aplicabilidade sobre o direcionamento dado pelo corpo executivo da empresa nos planejamentos estratégicos e incluindo-se também um planejamento evolutivo e inovador do "core" da empresa (nível 3).

Os processos em verde representam que o nível de maturidade da empresa é tão alto que já se tem medições e avaliações dos serviços prestados ou mesmo das entregas demandas pelo comitê executivo e/ou de tecnologia, seja para atender ao planejamento estratégico ou então dos planejamentos de tecnologia (segurança, crescimento, continuidade dos negócios – nível 4).

Para o nível 5, tem-se tal maturidade que permitirá à empresa manter em suas áreas um processo de solicitações de atendimento, serviços controlados por demandas entre departamentos.

4.3.2. Os Componentes Voltados para Serviços e Suporte

Estes componentes voltados para atender a serviços e suporte tem como foco principal a operação e a gestão de infraestrutura de TI dentro da organização e possui os seguintes princípios para este fim:

- Serviços de TI são considerados um conjunto de recursos de TI necessários para se atender uma demanda solicitada;
- Serviços de Suporte: auxiliam no atendimento de uma ou mais necessidades do cliente, apoiando-o em seus objetivos de negócios;
- Fornecimento de qualidade em serviços com custos justificáveis, relacionando os custos dos serviços de tecnologia e como estes trazem valores estratégicos ao negócio.

É muito importante para área de infraestrutura de TI a utilização de componentes voltados à serviços e suporte, pois com metodologias padronizadas de gerenciamento de TI pode-se ter uma relação adequada de custos e níveis de serviços.

Os processos de Gerenciamento de Mudanças, de Configuração, de Versões, de Incidentes, de Problemas, de pessoas, de processos, de produtos bem como o "serviço de atendimento" compõe a visão de suporte à serviços do framework enquanto os processos de definição dos novos serviços para Disponibilidade, Continuidade dos negócios, da Capacidade de TI, dos Níveis de Serviço e de Finanças compõe a visão de entrega de serviços do framework.

Igual a separação feita nos processos operacionais voltados a negócios com níveis de maturidade, abaixo estão os processos operacionais voltados à serviços e à suporte do framework de forma a facilitar a implementação destes processos.

Tabela 4 - Componentes de ITIL que compõe o Framework

Suporte a Serviços	Mat.	Entrega de Serviços	Mat.
Gerenciamento de Mudanças	1,2	Gerenciamento de Disponibilidade do Ambiente	1,2
Gerenciamento de Configuração	4	Gerenciamento da Continuidade dos Negócios	1,2
Gerenciamento de Versões	3	Gerenciamento da Capacidade de TI	1,2
Gerenciamento de Incidentes	3	Gerenciamento dos Níveis de Serviços	1,2
Gerenciamento de Problemas	1,2	Gerenciamento de Finanças	3
Serviço de Atendimento	1,2		

Há apenas uma diferença entre os processos com relação a sua implementação: para os processos que atenderão demandas através de serviços e de suporte, deverão ser implementados já nos níveis 1 e 2 de maturidade 7 dos 11 processos. Isto se dá pelo fato de estarmos com o mesmo sentido de raciocínio com relação às dependências dos processos.

Primeiro deverão ser implementados processos que são considerados como um nº mínimo imprescindível para atender aos níveis 1 e 2 de maturidade (representados em azul na figura 6), dos processos voltados a serviços e de suporte que podem impactar diretamente nos negócios da corporação. Estes processos são:

- Para o Suporte a Serviços:
    - Gestão de Mudanças.: Este processo se faz necessário para que se tenha uma visão e um controle das implantações feitas pela área de TI;
    - Gestão de Problemas.: Associado a monitoria das implantações efetuadas – este processo é importante na detecção de ocorrências devido as implantações efetuadas pela área de TI;
    - Serviço de Atendimento.: Canal de comunicação da corporação para realização de diversas solicitações – no nível 1 e 2 de maturidade, este

atendimento poderá ser restrito a dúvidas sobre serviços, suporte à área de TI com relação a implantações ou mesmo procedimentos. A medida em que este processo estiver amadurecido para os papéis e responsabilidades dadas nos primeiros níveis de maturidade, o setor envolvido será recapacitado e estará utilizando o processo de treinamento do COBIT para aperfeiçoamento sobre as atividades de atendimento;

- Para a Entrega de Serviços:
    - Gerenciamento da Disponibilidade do Ambiente.: Esta gestão se faz necessária, pois este processo efetua uma avaliação sobre os recursos de infraestrutura atuais e frente as demandas de negócios o quanto será necessário crescer o "parque tecnológico" para manter a disponibilidade dos negócios;
    - Gerenciamento da Continuidade dos Negócios.: Outra questão importante, pois em caso de indisponibilidade do "parque tecnológico atual" onde fisicamente seria possível de ativar um "segundo parque tecnológico" para que não sejam impactados os processos de negócios da corporação.
    - Criar processos que façam a gestão de ANS´s para com seus clientes;
    - Criar processos que tenham por objetivo avaliar a capacidade de TI e que de forma antecipada seja possível fazer "prospecções" de necessidades futuras.

Para o nível 3 de maturidade (representado em amarelo na figura 6), temos então um entendimento dos processos de negócios suportados pelos processos operacionais voltados à serviços e à suporte, e que o domínio e o grau de utilização destes processos pela corporação já está ao ponto de se ter um aumento sobre as responsabilidades da corporação:

- Para o Suporte a Serviços:
    - Passar a ter um processo que faça a gestão de incidentes, de forma separada da gestão de problemas, porque: a gestão de problemas tem seu foco sobre projetos implantados pela área de TI enquanto que a gestão de

incidentes tem seu foco voltado para ocorrências sem uma implantação de TI, ou seja, ocorrências externas a corporação (exemplo: falta de energia, manutenção feita por empresas terceiras, cabeamento de telecomunicação com falhas, entre outros aspectos);

- Passar a ter um processo operacional que controle o versionamento de softwares, principalmente, implementados pela área de TI (sejam softwares de mercado ou mesmo desenvolvidos internamente na corporação);

- Para a Entrega de Serviços:
  - Passar a ter uma gestão sobre os investimentos e fazer com que esta gestão informe o quanto deverá ser agregado ao negócio.

O nível 4 (representado em verde na figura 6) será o último a ser implementado com a gestão de configuração do ambiente de infraestrutura. Este processos fará a gestão de recursos físicos necessários do "parque tecnológico" da empresa.

O nível 5 de maturidade somente representará o quanto de domínio e de utilização dos processos implementados do ITIL são realizados pela corporação em conjunto com os processos implementados do COBIT.

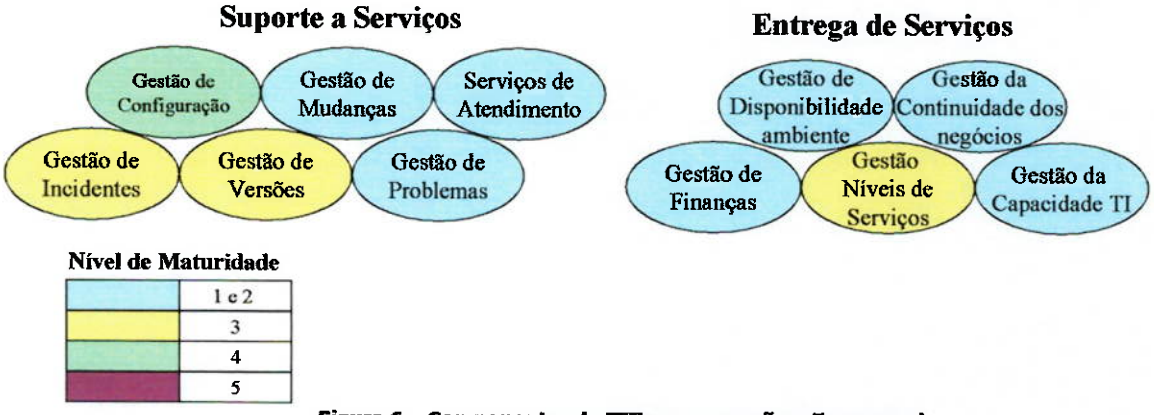

Figura 6 - Componentes de ITIL que compõe o Framework

4.3.3. Os Componentes de Auditoria

Os componentes de auditoria estão voltados para validar e auditar os processos implementados no âmbito de negócios (COBIT). Desta forma os processos de auditoria implantados terão dois objetivos:

- Permitir aos executivos da corporação que efetuem as pré-auditorias, com uma periodicidade mínima: trimestral. Com estas pré-auditorias será possível efetuar os ajustes necessários sobre distorções que forem identificadas durante o ano;
- Permitir às auditorias independentes um trabalho de avaliação e auditamento sobre os processos do COBIT.

A figura 7 demonstra os pontos de auditoria em que os componentes do COSO abrangerão os processos do COBIT implantados com o framework. As 5 visões do COSO estão diferenciadas em por cores para facilitar no entendimento onde cada visão atual sobre os processos de COBIT.

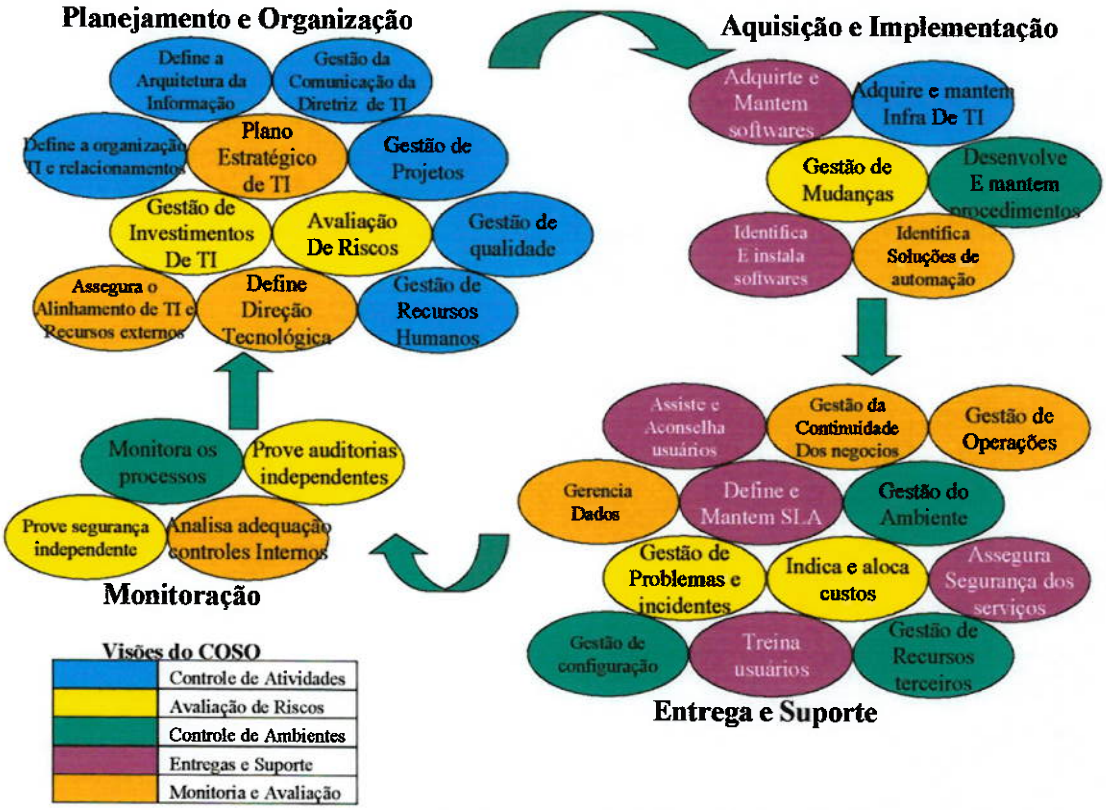

Figura 7 – Componentes do COBIT auditados pelos Processos do COSO

4.4. Diretrizes

Para suportar os processos operacionais do framework há a necessidade de se ter uma estrutura organizacional capaz de centralizar os esforços e direcionamentos com relação:

- a visão estratégica do mercado e como posicionar a organização no contexto em que vive garantindo seu sucesso e sobrevivência;
- Como garantir a renovação e inovação tecnológica no mundo de TI;
- Fazer a gestão de projetos estratégicos, táticos de cunho tecnológico e de segurança;
- Avaliações de planejamentos, de riscos e de controle de fraudes.

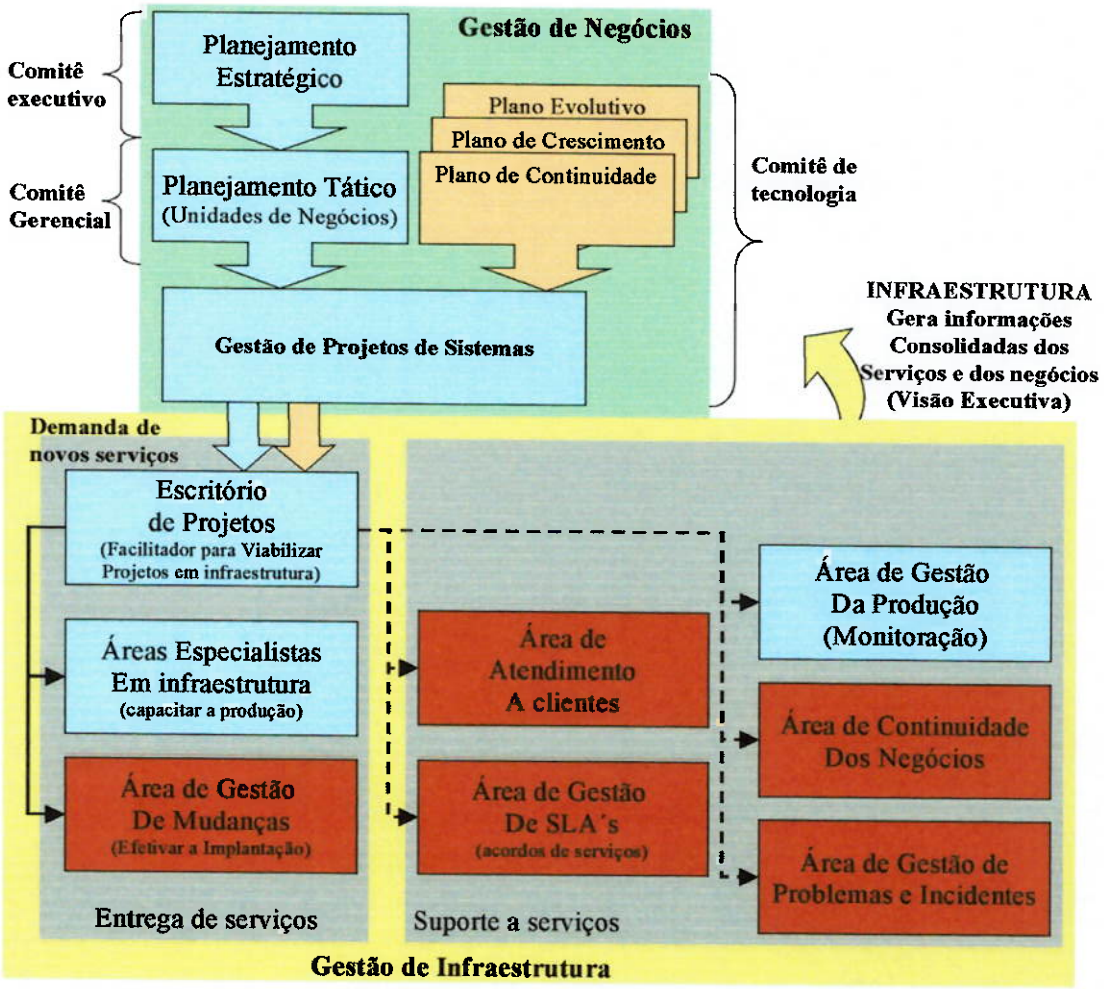

Figura 8 – Estrutura Organizacional para Suportar os Processos do Framework

Desta forma os requisitos organizacionais para suportar os processos operacionais do framework são:

- Comitê executivo: formado pelos altos executivos da organização que traçam o plano estratégico anual e as diretrizes da empresa;
- Comitê de tecnologia: formado pelos gerentes de tecnologia e, alinhados com o comitê executivo, tem a responsabilidade de estudar evoluções e inovações de tecnologia que possam trazer benefícios à organização;
- Comitê Gerencial: alinhado com o comitê executivo tem por responsabilidade viabilizar projetos voltados para atender as necessidades do plano estratégico e direciona-los para a área de gestão de projetos – que é composta também pelos integrantes do comitê de tecnologia;

- A área de escritório de projetos possui 2 responsabilidades fundamentais:
    - Ao receber as demandas feitas pelo comitê de tecnologia, estará alinhada com o plano estratégico e tático traçados (por assim também possuir um representante de infraestrutura nos comitês executivo e gerencial) e estará fazendo a gestão de recursos de TI para garantir a implantação de uma demanda (de um projeto);
    - Garantirá os processos criados:
        - para fluxos de projetos;
        - para fluxos de demandas sobre serviços;
        - para gerar informações consolidadas sobre implantações efetuadas;
- A área de gestão da produção possui por responsabilidade:
    - Monitoração operacional sobre todos os processos de negócios;
    - Geração de informações consolidadas sobre os componentes que envolvem o suporte a serviços:
        - ANS's;
        - Problemas e Incidentes;
        - Nível de atendimento a clientes;
        - Visão consolidada dos recursos de infraestrutura e de seu nível de disponibilidade;
        - Garantia da Continuidade de negócios (em off-sites físicos).

A gestão de projetos efetua um importante papel sobre a gestão de serviços e de suporte, direcionando para outras áreas as necessidades do cliente. Isto faz parte do planejamento e da execução dos novos serviços bem como a criação de novas demandas às áreas de suporte. Após a implantação dos processos voltados aos serviços entram em ação as áreas de suporte que farão a gestão e monitoria dos novos serviços implantados, informando para as áreas executivas da organização: níveis de acordos de serviços, os próprios ANS's alcançados, avaliação sobre a produção e relatar em caso de detecção de problemas ou incidentes encontrados.

Após implementados os processos operacionais baseados neste framework, há um fator importante que precisa ser mantido, principalmente com o respaldo do comitê executivo - a manutenção destes processos:

- ao implantar os processos de COBIT, os executivos necessitarão de pontos de controle que permitam trimestralmente avaliar o andamento dos mesmos, o que precisa ser revisto e melhorado e ainda avaliar a maturidade com que estão sendo utilizados. De certo anualmente estes processos serão auditados por profissionais do mercado embasados nas leis SOX (COSO);
- Ao se implantar os processos de ITIL, os executivos necessitarão também de acompanhamento, pois o objetivo final é obter a certificação de ITIL sobre os processos implementados.

4.5. Benefícios

Os principais benefícios sobre a implementação do Framework voltado a suportar a Governança em TI são:

- Existência de processos operacionais que atendam as necessidades das unidades de negócios, e que estes processos permitam aos níveis hierárquicos da corporação ter uma visão dos objetivos da corporação sendo atendidos, o direcionamento da corporação frente ao mercado competitivo bem como a evolução da corporação sobre controles internos e de seus processos corporativos;
- Existência de processos que permitam a corporação trabalhar numa visão de prestação de serviços e de suporte aos serviços prestados – esta visão é muito importante à área de infraestrutura com relação a controles de recursos computacionais da corporação para suportar as necessidades de negócios;
- Existência de processos de auditoria e de monitoração, capazes de mostrar ao alto escalão executivo, aos acionistas e investidores, que a corporação está aderente a Lei Sarbanes-Oxley.

Com estes benefícios trazidos será possível que o nível de confiabilidade e comprometimento da corporação com seus acionistas e investidores seja alto e sólido, garantindo assim a sobrevivência da corporação no mercado.

4.6. Problemas e Restrições

Cada vez mais, as mudanças que ocorrem no mercado obrigam as empresas a modificar sua estrutura ou seus processos. A mudança pode assumir muitas formas: desde a atuação da empresa num mercado de concorrência acirrada, das diretrizes executivas para atender processos de reengenharia, de downsizing até a diretriz sobre uma transformação cultural. As mudanças não devem ser tratadas de forma reativa, como a maioria dos colaboradores das empresas a enxergam, mas deve ser encarada como uma oportunidade de crescimento para todos que estão envolvidos na empresa, pois sua sobrevivência dependerá do próprio empenho de transformação e adequação sobre as exigências do mercado.

Desta forma é impossível ocorrer uma mudança importante sem que a alta gerência apóie estas diretrizes: para a implementação de processos operacionais que alterarão o modelo operacional de seus funcionários, temos que ter o comprometimento e o envolvimento do alto escalão da empresa, empenhados numa causa que trará benefícios corporativos à empresa.

Outro obstáculo é a falta de capacitação e recursos necessários para enfrentar cada um dos passos com eficácia. Também as estruturas formais e os sistemas de informação funcionam como obstáculos, pois qualquer transformação exige um prazo determinado, incluindo-se capacitações de colaboradores e não convém ficar na expectativa de que sejam acelerados.

Os valores compartilhados, que são menos visíveis, mas estão mais profundamente enraizados na cultura corporativa, são os mais difíceis de mudar do que as normas de comportamento. Existem dois fatores importantes na determinação do novo enfoque cultural de uma corporação: o primeiro é explicar às pessoas que determinados comportamentos e atitudes ajudam a melhorar o desempenho da empresa e o segundo é assegurar-se de que as gerações de gerentes seguintes mantenham este foco.

5. APLICABILIDADE DO FRAMEWORK

5.1. Mapeamento de Processos

Este trabalho de mapeamento necessitará de esforços das pessoas que estarão fazendo os questionamentos internamente na organização. O processo de mapeamento consiste:

- Na identificação de publicações e documentações de procedimentos operacionais feitos na organização, por qualquer que seja o meio de armazenamento destes – sejam através de ferramentas de mercado ou mesmo em repositórios de documentos mantidos por uma área de processos
- Na identificação de atividades e procedimentos que não são publicados corporativamente pelos setores ou departamentos que compõe a organização (isto se deve ao fato de que dependendo do tamanho da organização haverão departamentos ou setores que trabalham com procedimentos e processos próprios);
- No levantamento dos processos de negócios em que a organização atua, envolvendo clientes, fornecedores, colaboradores, prestadores de serviços;
- No levantamento dos processos internos sobre políticas financeiras (para aquisições de recursos tecnológicos), avaliações e aprovações de investimentos, plano de retorno sobre o investimento;
- Avaliar o nível de conhecimento e qual o grau de utilização sobre os processos existentes, com o objetivo de identificar a maturidade de uso e domínio dos mesmos de forma setorial, departamental ou na organização como um todo;

Este mapeamento deverá ser feito por uma área chamada PMO (Process Management Officer), e estará realizando ajustes e adequações sobre os processos existentes bem como implementar modificações para obter a aderência ao framework. Mas não basta apenas implementar os processos das metodologias de COBIT e ITIL sem que se tenham ferramentas de gestão: este trabalho deverá andar em paralelo com o estudo da área de PMO que além de definir os processos operacionais da organização,

estará avaliando o uso de ferramentas que possibilitem aos executivos das empresas terem as visões necessárias para uma boa Governança na área de TI.

Com o estudo concluído sobre "quanto se conhece do funcionamento da empresa internamente e quanto os processos são divulgados pela hierarquia organizacional", com a diretriz de mudanças a serem apresentadas pelo PMO e com o apoio do comitê executivo em estar efetuando uma mudança na organização, a escolha da ferramenta de gestão acaba sendo uma "conseqüência" de todo este trabalho, pois esta aquisição será estudada e validada com maior profundidade inclusive por um comitê de tecnologia, pois afeta diretamente o dia-a-dia operacional de técnicos, especialistas e colaboradores.

As empresas podem contar com pacotes de mercados voltados para gestão como por exemplo, ferramentas:

- de BI (Business Inteligence);
- de CRM (Customer Relationship Management);
- de ERP (Enterprise Resource Planning);
- de SCM (Supply Chain Management).

5.2. Aderência aos Componentes do Framework

A partir dos mapeamentos finalizados, a área de PMO iniciará o trabalho de adaptação dos processos existentes sobre o framework proposto:

- Identificando primeiramente se este trabalho será feito de forma setorial ou departamental e estendendo-se posteriormente para toda a organização;
- Criar ou alterar os workflows de processos existentes;
- Criar documentos e publicá-los como oficiais;
- Formalizar papéis e responsabilidades sobre setores / departamentos da organização e como deverá ser a dinâmica de comunicação no dia-a-dia das áreas envolvidas;
- Solicitar a criação de setores ou departamentos que por ventura necessitem (ex.: setor de controles internos – que garanta a segurança dos processos de negócios; setor de Acordos de Serviços – que garanta o tempo dos acordos sobre os serviços da empresa, entre outros).

5.3. Monitoração

Para prevenir a organização de perdas por causa de irregularidades e de manipulações deliberadas de dados, deve-se ter uma auditoria regular e ampla das atividades de TI. O comitê de tecnologia observa, por meio de metodologia específica, a relevância que o papel da auditoria tem para o comitê executivo da organização e como devem ser informados os resultados e as recomendações dos exames. O escopo, a freqüência e os resultados desses trabalhos são pontos de atenção.

Ao se fazer a implementação de processos de monitoração e auditoria do Framework, está se prevendo auditorias interna e externa como parte dos processos de controles internos da organização. Essa implementação estará voltada para atender a regulamentação da Lei SOX e inclui regras sobre independência de funções entre os processos. Os trabalhos devem ser planejados e organizados para se complementarem em escopo e qualidade, observadas as responsabilidades de cada um.

Espera-se que o atendimento dos requisitos de capacidade técnica e o conhecimento das atividades de TI estejam contidos nos padrões do COSO. É de extrema importância que as análises da auditoria devem cobrir aspectos abordados nas três grandes áreas em que se organizam as atividades de TI:

- Planejamento e organização;
- Desenvolvimento e Manutenção de sistemas; e
- Produção e suporte técnico.

Os exames consideram os seguintes procedimentos:

- Revisões em controles e procedimentos operacionais, com atenção para questões de segurança;
- Realização de testes e exames;
- Observação de sistemas antes de sua entrada em operação, para verificar a seu comportamento e os requisitos de segurança;
- Exame de documentos-fonte, cálculos e checagens para observar a correção das saídas de dados diante das entradas.

O monitoramento das atividades de TI deve considerar outros aspectos além dos exames de auditoria. São esperadas ações do comitê de tecnologia que assegurem meios e condições para as auto-avaliações de riscos e de controles, análises sobre desempenho, custos e qualidade dos serviços. Espera-se que indicadores supram a gerência com informações que auxiliem na previsão de riscos, indicando problemas no processo. Isso demanda seleção de indicadores e instalação de procedimentos de monitoramento.

Exames de controles internos e de segurança devem ser periodicamente realizados por meio de auto-avaliação ou auditoria independente, para se assegurar que estejam operando de acordo com os requisitos exigidos. Relatórios devem apontar riscos minimizados e sinalizar necessidades de adoção de ações por parte da alta administração.

O monitoramento e as avaliações de controles internos devem ser realizados por especialistas com competência técnica, que detenham procedimentos adequados para a realização de uma revisão efetiva e eficiente. Uma certificação independente deve ser requerida:

- Previamente à implantação de novos sistemas críticos (certificação sobre segurança e controles internos);
- Após a implantação de novos sistemas;
- Previamente à contratação e utilização dos serviços de provedores de serviços externos;
- de forma rotineira como meio de certificar a efetividade dos serviços de TI (próprios e desenvolvidos por provedores externos) e a observância de requisitos legais e regulamentares.

O comitê executivo deve se assegurar que um plano de auditoria regular e independente contemple aspectos sobre a efetividade e a eficiência dos procedimentos de controles internos e de segurança das atividades de TI.

A avaliação da habilidade gerencial no controle dessa área também deve estar prevista. Deve-se cuidar para que os planos de trabalho dos auditores para os sistemas de informação estabeleçam objetivos de exame em consonância com os padrões

profissionais aplicáveis e as análises devem assegurar e evidenciar o alcance desses objetivos.

Os relatórios devem trazer as conclusões, as recomendações cabíveis e as restrições sobre sua circulação. Um acompanhamento deve ser estabelecido para se verificar o atendimento dos apontamentos.

Porém a organização deverá se antecipar e efetuar auditorias internas com o objetivo de observar se os padrões esperados para a auditoria externa estão sendo devidamente direcionados. Espera-se que os auditores internos tenham conhecimentos e habilidades que permitam:

- Conduzir, planejar, programar e supervisionar atividades específicas de auditoria;
- Habilidade para investigação e documentação do trabalho; habilidade para comunicações oral e escrita;
- Habilidade para elaborar, sintetizar e relatar apontamentos críticos e construtivos;
- Visão geral de conceitos sobre concepção e projetos de sistemas.

Os manuais da auditoria interna devem definir o papel do departamento dentro da organização, descrevendo o escopo e os objetivos gerais de auditoria e refletir as necessidades da instituição e a filosofia do comitê de auditoria. Um manual é pré-requisito para um efetivo programa de auditoria interna que deve abordar políticas, padrões e procedimentos para o departamento.

5.4. Auditoria

O primeiro passo é definir qual o objetivo que vamos auditar. No caso de instituições financeiras os riscos já são pré-definidos, mas na maioria dos casos esta definição deve ser mais aprofundada. Os riscos definidos pressupõem uma atividade, com os respectivos objetivos pré-estabelecidos. Deve então levantar o maior número de informações sobre os seguintes pontos:

- Quais são as metas traçadas para o objetivo que vai ser auditado;

- Quais são os sistemas de informação e relatórios que permitirão o acompanhamento das metas traçadas;
- Quais as leis e normativos que regem o objetivo que vai ser auditado.

O passo seguinte é verificar se os riscos estão alinhados ao cumprimento de cada objetivo. Selecionar os riscos com maior probabilidade de ocorrência e que podem causar perdas, no caso de sua consumação. Listar os riscos para cada objetivo traçado.

Para cada risco listado, verificar quais são, as atividades de controle que, se conduzidas de maneira adequada, podem diminuir ou permitir o gerenciamento do risco. Para cada atividade de controle apontada, deverão ser verificadas quais já estão sendo cumpridas e definitivas (estão efetivamente permitindo a diminuição/gerenciamento do risco). Esta também é a ocasião para identificar as fontes de informações, métodos de comunicação e atividades de monitoramento.

Após a reunião das seguintes informações: riscos, objetivos da corporação traçados e identificação das atividades de controle, devidamente listados, deverá ser adicionado então a este relatório questionamentos como:

- Se há perdas ocorrendo;
- Se a probabilidade de ocorrerem riscos é grande;
- Se os gestores estão cientes destes riscos.

Estes tipos de questionamentos são importantes para avaliar se há ocorrências de riscos sobre as atividades da corporação, que possam acarretar em perdas e conseqüentemente não se alcançar os objetivos traçados.

Esta aplicação de auditoria não é apenas para identificar falhas nos processos de controle, mas para se antecipar às auditorias externas e principalmente executar soluções de contorno em caso de identificação de irregularidades.

6. CONCLUSÃO

A Governança em TI tem seu foco voltado para os mecanismos de controle que devem ser fornecidos à gerência superior. Este fornecimento de informações permitirá à alta gerencia avaliar controles importantes como: despesas de TI, satisfação do usuário, eficiência do desenvolvimento e operações, perícia da equipe de TI e possibilita efetuar comparações de medidas com estudos de mercado realizado. Isto evita que relatórios da alta administração utilizado em tomadas de decisões esteja restrito à informações técnicas.

A Governança em TI é parte fundamental da Governança corporativa e deve fornecer:

- A garantia que não há investimentos em projetos que não estejam alinhados com a diretriz estratégica da empresa;
- Mecanismos adequados de controles às estruturas organizacionais, permitindo a criação de valor para o negócio através de TI.

A Governança em TI não está vinculada apenas na utilização do COBIT ou ITIL, como muitas publicações existentes no mercado, mas a Governança em TI é um conjunto sistemático de processos de controles de como TI é dirigida e controlada dentro das empresas, e também pela comprovação de que TI gera valor agregado aos negócios das empresas.

Para análise dos processos definidos nestas metodologias, foi criado um framework capaz de se implementar os componentes de COBIT, ITIL e COSO nas corporações, tomando-se o cuidado de mostrar a importância de se conhecer internamente os processos das organizações para, em seguida, estudar mudanças sobre setores e departamentos das organizações.

LISTA DE REFERÊNCIAS

[1] Charan, Ram; "Governança Corporativa que produz resultados"; 2005 - Ed. Campus

[2] Weill, Peter e Ross, Jeanne W; "Governança de TI"; 2006 - Ed. M.Books do Brasil

[3] Botto, Renato; "Arquitetura Corporativa de TI"; 2004 - Ed. Brasport.

[4] Associados, GaleGale &; "COBIT - Framework" - 3ª Edição.

[5] Castro, Jorge - "Governança em TI na Organização" - 2005.

[6] Institute, IT Governance; "Marcos de Referência de COBIT"; - 2005.

[7] CISA - "The importance of IT in the design, implementation and substainability of internal control over disclosure and financial report" - 2004.

[8] CISA - "The importance of IT in the design, implementation and substainability of internal control over disclosure and financial report" - 2005.

[09] "Monitoramento e auditoria" - 2002 - material de palestra interna - Orbitall.

[10] www.itgovernance.org

[11] www.isaca.org