Faculdade de Tecnologia de Americana

Curso Segurança de Informação

AS BOAS PRÁTICAS DA METODOLOGIA COBIT UTILIZADA NA GOVERNANÇA DE TI

MIRIAN ENMEAN KOON WU MON

Americana, SP

2014

Faculdade de Tecnologia de Americana

Curso Segurança de Informação

AS BOAS PRÁTICAS DA METODOLOGIA COBIT UTILIZADA NA GOVERNANÇA DE TI

MIRIAN ENMEAN KOON WU MON

mirianekwm@gmail.com

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança de Informação, sob a orientação do Prof. Esp. Edson Roberto Gaseta.

Área: Segurança de Informação.

Americana, SP

2014

BANCA EXAMINADORA

Prof. Esp. Edson Roberto Gaseta (Orientador)

Prof. Mestre Marcus Vinícius Lahr Giraldi

Prof.ª Esp. Daniele Junqueira Frosoni

AGRADECIMENTOS

Sempre a Deus, razão de toda minha existência.

Aos meus queridos familiares, especialmente minha mãe, mulher de fibra, de amor poderoso e abundante que vem do Senhor.

Ao Prof. Esp. Edson Roberto Gaseta, orientador, pelo apoio, comprometimento e amor em lecionar, compartilhando seu conhecimento e experiência do assunto abordado.

Aos mestres e educadores, que colaboram constantemente na formação como ser humano.

A todos os funcionários, que carinhosamente tive o privilégio, a convivência nesses anos de vida acadêmica.

A todos que de alguma maneira faz parte de minha história, agradeço e desejo tudo o que há de bom, nessa busca incessante pela razão, emoção e futuro melhor, muito obrigada!

DEDICATÓRIA

A meu marido Antônio e a meu filho Filipe, pela cumplicidade, paciência e amor.

RESUMO

O presente trabalho conceitua a necessidade cada vez maior das organizações interagirem a Governança Corporativa com a Governança de TI (Tecnologia da Informação), como forma de gerir os sistemas de informações, objetivando maior transparência aos atos, garantindo não só a segurança de informações como também todo o conhecimento do ambiente de TI que suporta o mundo corporativo das organizações. A Governança de TI, por meio da utilização de melhores práticas, como *CobiT* ***(****Control objectives for information and related Technology****)*, sendo exemplo a ser abordado neste trabalho de conclusão de curso, aborda os processos que venham a assegurar que as informações sejam confidenciais, integras e disponíveis, sendo forma de viabilizar operações e transações das organizações, proporcionando o retorno financeiro dos investimentos em TI, gerenciando os riscos, harmonizando e alinhando com as decisões sobre a gestão dos negócios proporcionados pelo mercado competitivo e uma sociedade dinâmica, inovadora, que compartilha e socializa informações de maneira instantânea e globalizada, em um cenário de preocupações crescentes decorrente de fraudes, espionagem e roubo de informações entendidas como valores na Governança Corporativa, levam as organizações a gerenciar o Sistema de Informações da Governança de TI.

Palavras Chave: Segurança de Informação; Governança de TI; Ferramentas de Gerenciamento de TI; Melhores práticas em TI; Gerenciamento de Riscos.

ABSTRACT

This paper defines the increasing need for organizations to interact the Corporate Governance with the IT (Information Technology) Governance in order to manage their information systems, aiming at a greater transparency of their actions, and ensuring not only information safety as well as the safety of all IT knowledge which supports the organization corporate world. IT Governance, through the use of best practices, such as the COBIT (Control objectives for information and related Technology), an example covered in this course conclusion paper, reviews the processes that ensure that the information remains confidential, complete and available, in order to enable the organization's operations and transactions, ensure the financial return on IT investment, manage risk, harmonize and align decisions on management of businesses generated by a competitive market as well as by an innovative and dynamic society, which shares and integrates information in an instantaneous and globalized way, in a scenario of increasing concerns related to fraud, espionage and theft of information considered an asset by Corporate Governance which lead organizations to manage the IT Governance Information System.

Keywords : *Information Security , IT Governance , IT Management Tools , Best Practices in IT , Risk Management* .

LISTA DE ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
CobiT	Control Objectives for Information and Related Technology
ITGI	Information Technology Governance Institute
ISACA	Information Systems Audit and Control Association
NBR	Norma Brasileira aprovada pela ABNT
TI	Tecnologia da Informação

Sarbanes-Oxley, SOX Lei de 30 de julho de 2002, criada pelo senador Paul Sarbanes (Democrata de Maryland) e pelo deputado Michael Oxley (Republicano de Ohio). Motivada por escândalos financeiros corporativos, essa lei foi redigida com o objetivo de evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores causada pela aparente insegurança a respeito da governança adequada das empresas.

LISTA DE FIGURAS E DE TABELAS

Figura 01 - Relação entre Governança Corporativa e a Governança de TI

Figura 02 - Sistema de Governança Corporativa

Figura 03 – Modelo relacional dos Ativos da Empresa e de TI

Figura 04 – Ativos de Informação e TI , baseado na estrutura do CobiT

Figura 05 - Áreas de Foco na Governança de TI

Figura 06 – Gerenciamento dos Recursos de TI para entregar os objetivos de TI

Figura 07 – Domínios do CobiT Inter-relacionados

Sumário

1 INTRODUÇÃO 13

2 TIPOS DE GOVERNANÇAS 15

2.1 Governança Corporativa 15

2.1.1 Ativos de uma Organização 17

2.1.2 Ativos de Informação e de TI 19

2.2 Governança de TI 21

2.2.1 Objetivos da Governança de TI 21

3 MODELO CobiT 4.1 22

3.1 Os Domínios do CobiT 4.1 24

3.1.1 Domínio: Planejar e Organizar - PO 24

3.1.2 Domínio: Aquisição e Implantação - AI 26

3.1.3 Domínio: Entregar e Suportar - DS 27

3.1.4 Domínio: Monitoração e Avaliação - ME 30

3.2 Objetivos de controle de TI: 31

3.3 Objetivos de controle em relação a TI 32

3.3.1 Detalhamento dos Processos Pertinentes à Segurança da Informação 32

4 CONSIDERAÇÕES FINAIS 35

5 REFERÊNCIAS BIBLIOGRÁFICAS 36

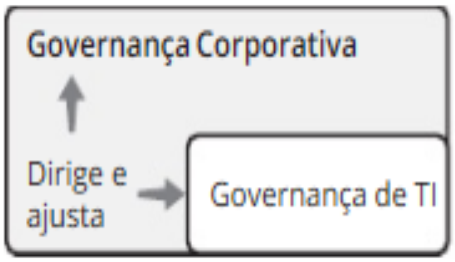
1 INTRODUÇÃO

É de conhecimento de muitos as constantes transformações e inovações tecnológicas ocorridas na sociedade, devido à globalização, compartilhamento e socialização de informações, como por exemplo, banda larga, comércio eletrônico, rede sem fio, computação em nuvem, mensagens instantâneas, telefonia via Internet, redes sociais, dispositivos de armazenamento de dados que exigem espaços físicos cada vez menores, nanotecnologias, entre outras, que ocorreram em pouco menos duas décadas. Neste cenário tecnológico, as empresas estruturadas de médio a grande porte, já inseridas no cenário econômico, político e social, procuram cada vez mais interagir com a tecnologia de informação para atingir seus objetivos de lucro, crescimento e inovação, para serem cada vez mais competitivas, e o papel dos trabalhadores no geral, cada vez mais qualificados a produzir ideias, resolver problemas e criar soluções (Cavalcante et all, 2012). Diversas abordagens para alcançar esses objetivos são utilizadas e, entre elas, a politica de Governança Corporativa, que tomou maiores proporções devido a escândalos corporativos, como por exemplo, os ocorridos nas empresas americanas como *Enron*, *Wordcom*, ocorridos em meados de 2.002, que derrubaram as ações na Bolsa de Valores Americana com ênfase em tecnologia, a *NASDAQ*, cerca de 36% (Well; Ross 2006, p. 4), a Lei Sarbanes Oxley , SOX de 30 de julho de 2002, surgiu objetivando evitar o esvaziamento dos investimentos financeiros e fuga de investidores, visa a criação de mecanismo de auditoria e segurança confiáveis nas organizações.

A estrutura da Governança Corporativa, sistema de gestão voltado à alta administração, tem com objetivo dar transparência de seus atos, gerando segurança ao mercado e em especial aos *stakeholders* (partes interessadas), ou seja, aos acionistas, às instituições financeiras, aos fornecedores, aos clientes, aos funcionários, a comunidade e aos próprios sócios proprietários. Em um cenário de preocupações crescentes decorrente de fraudes nas empresas, a necessidade da avaliação do valor da tecnologia da informação, o gerenciamento dos riscos e as crescentes necessidades de controle das informações entendidas como valores na Governança Corporativa, levam as empresas a gerenciar os Sistemas de Informação, por meio da Governança de Tecnologia da Informação (TI) que é parte

integrante da Governança Corporativa, conforme demonstrado na figura abaixo, figura 01, com processos estruturados que tornam as operações de negócios mais seguras, resultando assim em um melhor retorno financeiro dos investimentos e na redução de riscos, alinhando a TI com áreas de negócios. As boas práticas de Governança de TI harmonizam decisões sobre a gestão e a utilização de TI com encaminhamentos produtivos e objetivos ao negócio, ampliando os retornos e segurança dos investimentos nesta área. A Governança de TI é de responsabilidade da alta direção, diretores, executivos, consistindo em conduzir diretrizes aos processos e estruturas organizacionais, garantindo que a TI da empresa apoie a expansão das estratégias e objetivos da organização.

Figura 01 Relação entre Governança Corporativa e a Governança de TI



Fonte: (GASETA, 2012).

Justifica-se este trabalho, tendo em vista que em um cenário mundial cada vez mais competitivo, com investimentos mais dispendiosos, inclusive os investimentos tecnológicos, há a necessidade das organizações estruturarem melhor a área de TI, adotar mecanismos que permitam o estabelecimento de objetivos, avaliação de resultados e de mensurar de forma concreta as metas alcançadas, pois organizações que se apoiam nas tecnologias constantemente inovadoras, exigem modelos de gerenciamento ágeis e flexíveis.

O objetivo geral do trabalho é fazer um estudo sobre Governança Corporativa e ferramentas de apoio. Os objetivos específicos visa mostrar a necessidade cada vez maior das organizações interagirem a Governança Corporativa com a Governança de TI, como forma de gerir os sistemas de informações, objetivando maior transparência aos atos, garantindo não só a segurança de informações como também todo o conhecimento do ambiente de TI

que suporta o mundo corporativo das organizações, unificar os aspectos de TI com uma ferramenta de apoio, o Cobit, à gestão dos recursos da organização.

O procedimento metodológico adotado englobou as seguintes etapas: Levantamento bibliográfico e estudo de Governança Corporativa; Governança de TI. Em seguida foi feito o levantamento sobre a metodologia do CobiT, mostrando a adequação da ferramenta à Governança de TI, no sentido de assegurar o alinhamento de TI ao negócio da organização, bem como mostrar os processos associados a segurança da informação que estão inseridos na Governança de TI.

2 TIPOS DE GOVERNANÇAS

2.1 Governança Corporativa

Governança Corporativa, segundo IBGC - Instituto Brasileiro de Governança Corporativa é:

> ...sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo as práticas e os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade.

O IBGC é uma organização nacional, sem fins lucrativos, fundada em 1995, focada no desenvolvimento da governança corporativa, contribuindo na difusão de melhores práticas, seguindo os princípios que a regem de:

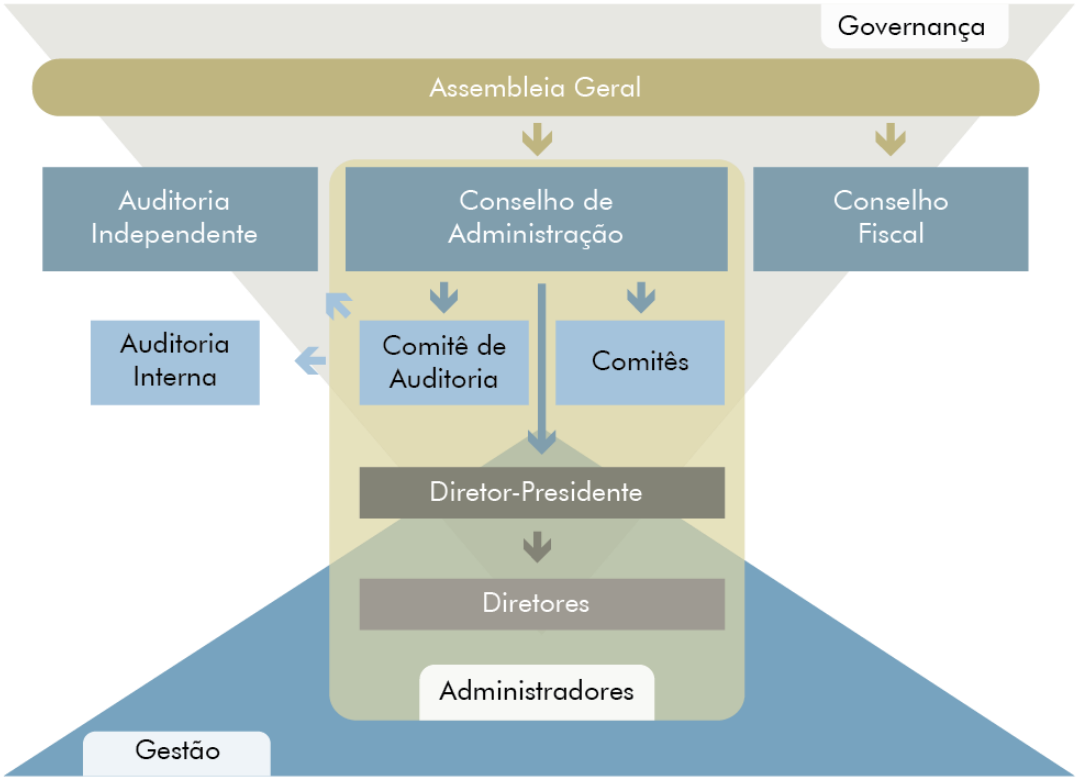
- Transparência: Disponibilização das informações das partes interessadas (proprietários, acionistas, fornecedores, entre outros), além das impostas por dispositivos de lei, adequadas a transparência de informação, incluindo as econômicas-financeiras, a fim de criar um clima de confiança nas ações de gestão que agregam valor ao negócio;

- Equidade: Tratar de forma justa aos sócios e demais partes interessadas;

- Prestação de contas: Trata-se dos agentes de Governança prestar contas de sua atuação, assumindo integralmente as consequências de seus atos e omissões.

- Responsabilidade Corporativa: Os agentes de Governança devem zelar pela sustentabilidade e longevidade das organizações. (IBGC 2014)

Figura 02 - Sistema de Governança Corporativa



Fonte: (IBGC 2014).

A estrutura da Governança Corporativa, demonstrada na figura 02, é gerida pela alta administração, objetiva agregar valor ao negócio, dar transparência de seus atos, gerando segurança ao mercado e em especial aos *stakeholders*, como acionistas, as instituições financeiras, fornecedores, clientes, funcionários, a comunidade e aos próprios sócios proprietários em um cenário de crescentes preocupações crescentes decorrente de riscos e fraudes nas empresas.

Segundo Fernandes e Abreu (2012), o ambiente de negócio, no Brasil tem sido caracterizado por intensa competição, incluindo concorrentes globalizados e novas ameaças devido a essa internalização econômica.

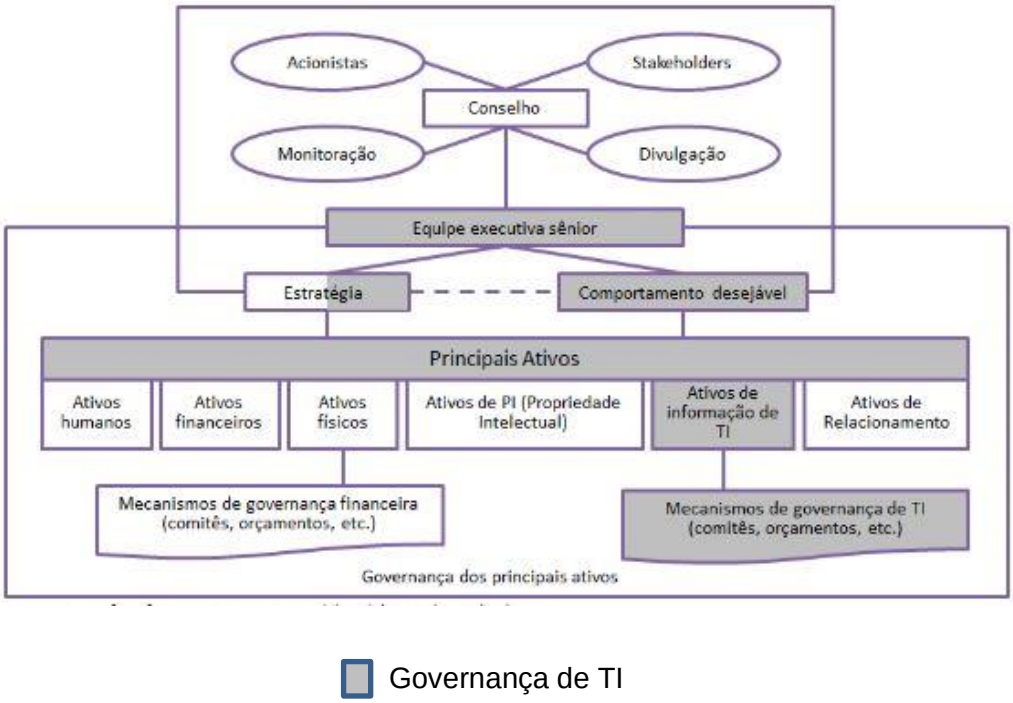
As constantes transformações e inovações tecnológicas ocorridas na sociedade, devido a globalização, caracterizam uma dependência cada vez maior dos objetivos de negócio em relação a TI e a necessidade de conter no planejamento estratégico de sua governança Corporativa a governança de TI.

Em junho de 2006, com a publicação da Resolução 3380 do Banco Central do Brasil, no que tange a TI, a resolução refere-se à falhas, riscos de atividades como interrupção de atividades, danos a ativos, determina que as instituições devam ser avaliadas, monitoradas, controladas e mitigadas os riscos que possam a ter a organização. A maioria das instituições, em atendimento a resolução 3380, utilizaram como ponto de partida, a avalição de riscos baseados na metodologia de processos "*Control Objetives for Information and related Technology" (*CobiT) (FERNANDES e ABREU, 2012, p. 37).

2.1.1 Ativos de uma Organização

Weill e Ross (2006) sugeriram um modelo, para associar a Governança Corporativa com a Governança de TI, pois, conforme citam os autores, a Organização para Cooperação e o Desenvolvimento Econômico (OCDE), afirma que não há um único modelo de boa governança corporativa. (WEILL, ROSS, 2006, p.5).

Figura 03 – Modelo relacional dos Ativos da Empresa e de TI



Fonte: (Weill; Ross 2006, p. 6).

Segundo Weill e Ross (2006), a Figura 03, apresenta os ativos nos quais uma organização agrega valores ao negócio e concretizam suas estratégias são:

a) Ativos Humanos: Pessoas, treinamentos, planos de carreira, e outros;
b) Ativos Financeiros: Dinheiro, investimentos, fluxo de caixa e outros;
c) .Ativos Físicos: Prédios, fábricas, equipamentos, além de outros;
d) Ativos de PI: Propriedade Intelectual, inclusive o *kwow–how* de produtos e serviços, devidamente patenteado, registrado;
e) Ativos de relacionamento: Relacionamentos, marca a reputação junto a clientes, fornecedores;
f) Ativos de informação e TI: Dados digitalizados, informações, conhecimento sobre os clientes, desempenho de processos, finanças, sistema de informação, e assim por diante.

2.1.2 Ativos de Informação e de TI

Os Ativos de TI, na qual suportam os objetivos de negócio da organização, devem atender os critérios de controles segundo o CobiT (2007, p. 12):

a) De Qualidade:

- Eficácia – Informação relevante e pertinente aos processos de negócio, como também entregue de maneira correta, consistente e utilizável;
- Eficiência – Melhor uso do recurso (produtiva e econômica);

b) De Segurança:

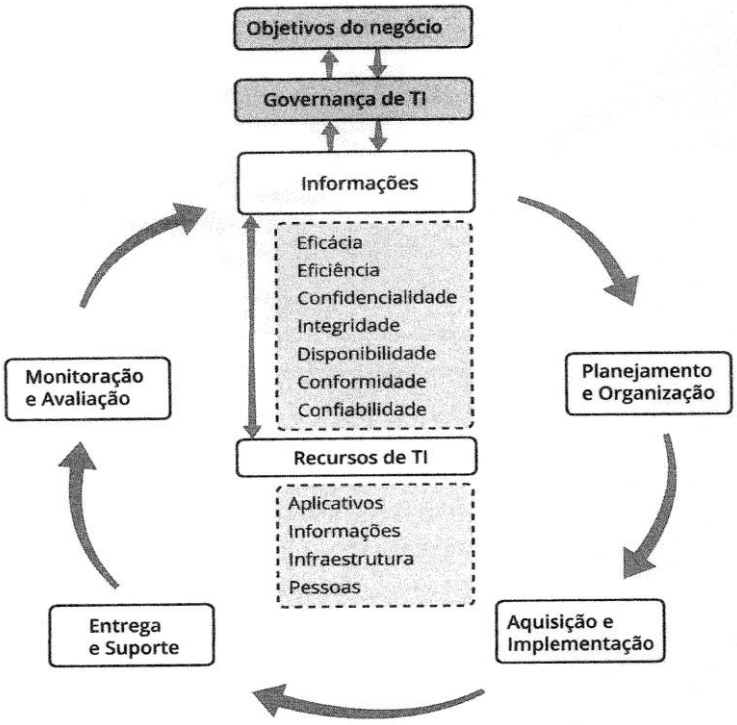
- Confidencialidade: Proteção de informações confidenciais, a acessos indevidos;
- Integridade: A informação deve estar íntegra, precisa e completa, bem como sua validade de acordo aos valores e expectativas de negócio;
- Disponibilidade: A informação tem que estar disponível, quando requerida ao processo de negócio.

c) Fiduciário:

- Conformidade: A informação deve estar em conformidade com as leis, normas, regulamentos e contratos com os quais os processos de negócios estão associados;
- Confiabilidade: relativo que a informação seja entregue de forma apropriada para os executivos exercer e administrar a organização de maneira a ser responsabilizados fiduciários e de governança. Os recursos de TI das Organizações, que devem atender aos objetivos de negócios, segundo o Cobit (2007, p. 14), e também demonstrado na figura 04 (Gaseta, 2012, p. 38), é composto de:

- Aplicativos: Sistemas de informação, utilizados pelos usuários da organização;
- Informações: Todos os dados utilizados no sistema de informação e pelos processos de negócios;
- Infraestrutura: Refere-se à tecnologia empregada e utilizada, ou seja, hardware, softwares, sistema de gerenciamento de redes, mídia e, também, relacionados aos ambientes que abrigam e dão suporte a eles;
- Pessoas: São os colaboradores requeridos para planejar e organizar, adquirir e implementar, entregar e suportar, monitorar e avaliar o sistema de informação e serviços. Eles podem ser internos, contratados ou terceirizados, conforme a necessidade.

Figura 04 – Ativos de Informação e de TI, baseado na estrutura do CobiT



Fonte: (Gaseta, 2012, p. 38)

2.2 Governança de TI

De acordo com IT Governance Institute – ITGI (2007):

> A Governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e entenda as estratégias e objetivos da organização.

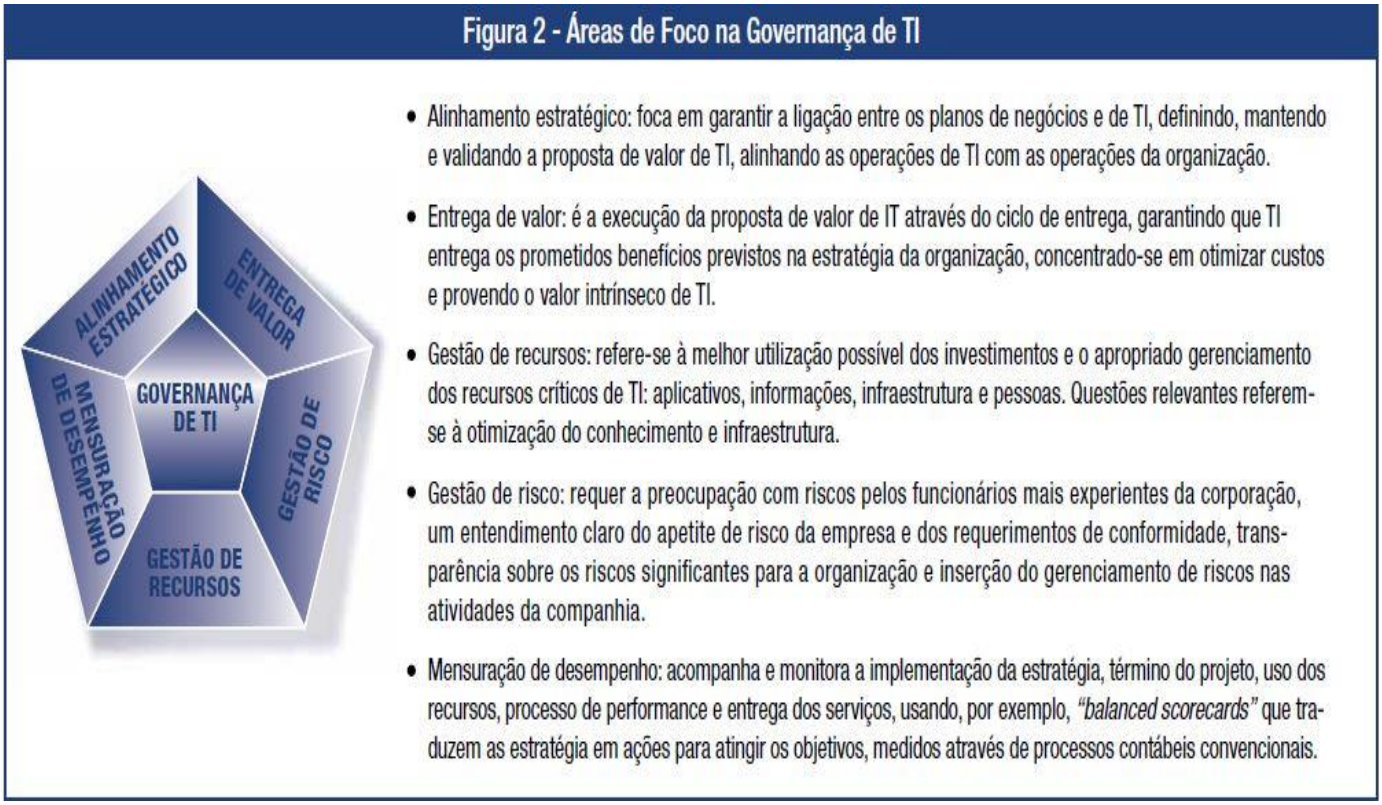
A Governança TI, integra e institucionaliza boas práticas para garantir que a área de TI da organização, suporte e direcione os objetivos de negócios, ou seja, para atingir esses objetivos, precisam ser gerenciados e monitorados por uma série de processos naturalmente agrupados (ITGI, 2007).

A Governança de TI ganha força em um cenário mundial cada vez mais competitivo, em que há a necessidade da área de TI adotar mecanismos que permitam o estabelecimento de objetivos, avaliação de resultados e de mensurar de forma concreta as metas alcançadas, pois organizações que se apoiam nas tecnologias constantemente inovadas, exigem modelos de gerenciamento ágeis e flexíveis (GASETA, 2012, p. 2).

2.2.1 Objetivos da Governança de TI

O principal objetivo é alinhar a TI aos requisitos de negócio. O CobiT é uma ferramenta fundamental da implantação da Governança de TI, promove um método para assegurar que a TI, esteja alinhada com os negócios, que habilite o negócio e maximize os benefícios, que os recursos sejam usados responsavelmente, e os riscos mitigados e gerenciados apropriadamente.

Figura 05 - Áreas de Foco na Governança de TI



Fonte: (ITGI, 2007)

O foco da Governança de TI descreve tópicos que o executivo da área de tecnologia deve atentar para direcionar os processos da área de TI. CobiT, é um modelo, no o qual todos os componentes, processos, requerimentos de Governança de TI e controle de TI são inter-relacionados (ITGI, 2007) conforme pode ser observado na figura 05.

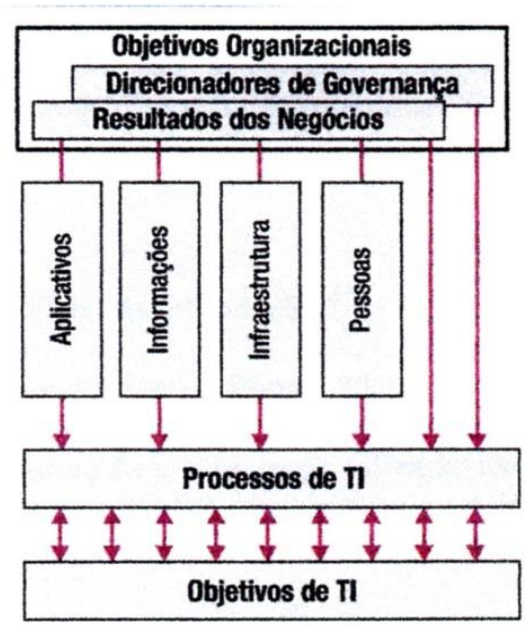
3 MODELO CobiT 4.1

O Cobit 4.1 (embora exista a versão Cobit 5, optou-se pela versão acima citada por ser mais conhecido e ter maior embasamento literário), é um modelo, uma metodologia de TI criada com as principais características de ser focada em negócios, centrada em processos, baseada em controles e orientada a medições (ITGI, 2007, p. 12), visando o controle, o gerenciamento e a mensuração de cada processo. A busca pela utilização de boas práticas de Governança de TI, visa adequação da infraestrutura tecnológica para dar sustentabilidade aos objetivos de

negócio da organização, surgem no mercado, uma série de ferramentas de controle para auxiliar na Governança de TI, entre elas o CobiT 4.1, que auxilia nos requisitos de auditoria e de controle na área tecnológica (GASETA,2012, p. 35).

Os ativos de TI (aplicativos, informações, infraestrutura e pessoas), são direcionados pelos objetivos de negócios, demonstrado graficamente na figura 06, visto que necessitam serem gerenciados pelos processos de TI para a entrega dos objetivos de TI, conforme demonstrado na figura 06 abaixo:

Figura 06 – Gerenciamento dos Recursos de TI para entregar os objetivos de TI



Fonte: (ITGI, 2007, p.14)

O CobiT é composto por:

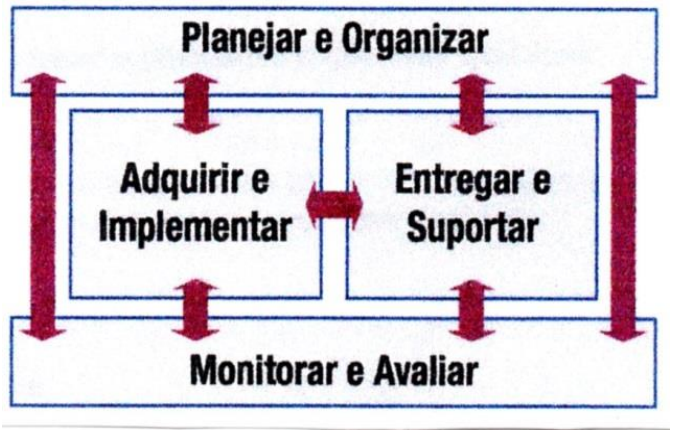
- 4 Domínios;
- 34 Processos;
- 34 Objetivos de controle de alto nível;

- 210 Objetivos de controle detalhados.

3.1 Os Domínios do CobiT 4.1

O CobiT, está dividido em quatro domínios, visando que a Governança de TI seja eficiente, é importante avaliar as atividades e os riscos de TI que precisam ser gerenciados, Eles são ordenados em domínios de responsabilidades de planejamento, construção , processamento e monitoramento, embora muitas organizações poderão identificar os mesmos processos chaves, poucas terão a mesma estrutura de processos ou aplicarão todos os 34 processos do CobiT (ITGI, 2007). No modelo CobiT, os domínios inter-relacionam conforme demonstrado na figura 07:

Figura 07 – Domínios do CobiT Inter-relacionados



Fonte: (ITGI, 2007, p.14)

3.1.1 Domínio: Planejar e Organizar - PO

São as estratégias e as táticas, preocupa-se em como a TI pode contribuir para atingir os objetivos de negócios. O sucesso da visão estratégica precisa ser planejado, comunicado e gerenciado por diferentes perspectivas. Nesse domínio, as questões que auxilia a serem respondidas relativas à Governança de TI são:

-As estratégias de TI e de negócio estão alinhadas?

- A Organização está utilizando da melhor forma seus recursos?

- Todos conhecem os objetivos de TI na Organização?

Os riscos de TI são entendidos e estão sendo gerenciados?

- A qualidade dos sistemas de TI são adequadas à necessidades de negócio?

Os processos do domínio PO são:

• **PO1 Definir um Plano Estratégico de TI:** Alinhados com objetivos de negócio;

• **P02 Definir a Arquitetura da Informação:** Estabelecer um modelo de dados para assegurar a integridade e consistência de todos os dados;

• **PO3 Determinar o Direcionamento Tecnológico:** Define e implanta plano de infraestrutura tecnológica, arquitetura e padrões que reconheçam e alavanquem oportunidade de negócios;

• **PO4 Definir os Processos, Organização e os Relacionamentos de TI:** Definição de estruturas organizacionais de TI transparentes, flexíveis e responsáveis, definição e implementação de processos de TI, com regras e responsabilidades integradas aos processos de negócio;

• **PO5 Gerenciar o Investimento de TI:** Decisão de forma eficiente, efetiva e em conformidade sobre os investimentos de TI;

• **PO6 Comunicar as Diretrizes e Expectativas da Diretoria:** Comunicação de todas as ações e planos de TI, bem com relatórios da capacidade de TI para atender às necessidades do negócio;

• **PO7 Gerenciar os Recursos Humanos de TI:** Contratar, qualificar, treinar e motivar colaboradores competentes, pois a Governança TI, o ambiente de controle

de informação, elas são altamente dependentes da motivação e competência dessas pessoas.

• **PO8 Gerenciar a Qualidade:** Gestão de qualidade dos serviços de TI, atendendo às necessidades de negócios e requisitos de qualidade de serviços.

• **PO9 Avaliar e Gerenciar os Riscos de TI:** Desenvolver uma estrutura de gerenciamento de riscos de TI, que juntamente com a estrutura de riscos operacionais e de negócio, visam estratégias a mitigar os riscos, assim minimizando os riscos residuais a níveis de tolerância aceitáveis.

• **PO10 Gerenciar Projetos:** Definir estrutura de gestão de projetos aplicados a projetos de TI

3.1.2 Domínio: Aquisição e Implantação - AI

As soluções de TI, compreendidas na estratégia de TI, são identificadas desenvolvidas ou adquiridas, implementadas e integradas ao processo de negócio, comtemplando as manutenções, mudanças dos sistemas existentes garantindo a continuidade das soluções de TI de acordo com os objetivos de negócio da organização. Nesse domínio, as questões que auxilia a serem respondidas relativas à Governança de TI são:

- Novos projetos atenderão e fornecerão soluções às necessidades de negócios?

- Novos projetos serão entregues no prazo e no orçamento previsto?

- Novos sistemas funcionam corretamente após implantação?

- As alterações poderão ser ocorridas sem o comprometimento das operações de negócios atuais?

Os processos do domínio AI são:

- **AI1 - Identificar Soluções Automáticas:** Definição das necessidades, a revisão da viabilidade econômica e tecnológica, em um projeto eficaz e eficiente de soluções automatizadas.
- **AI2 – Adquirir e Manter Software Aplicativo:** Aquisição e manutenção de sistemas e aplicativos que atendam à necessidade de TI.
- **AI3 – Adquirir e Manter a Infraestrutura Tecnológica:** Adquirir e manter a infraestrutura tecnológica que atendam a necessidade de TI, padronizada e integrada.
- **AI4 – Habilitar as Operações em Uso:** Habilitar aos usuários e para TI, através de manuais, documentos, treinamentos para assegurar correto uso da infraestrutura e das aplicações.
- **AI5 – Obter Recursos de TI:** Obtenção de recursos de TI com melhor custo-benefício que atendam as necessidades de TI da organização.
- **AI6 – Gerenciar Mudanças:** Gerenciamento de maneira controlada de todas as mudanças na organização, incluindo manutenções e correções emergenciais, elas devem ser registradas, avaliadas e autorizadas antes da implementação e revisadas, assegurando a mitigação de riscos de impactos negativos ou na integralidade do ambiente de produção.
- **AI7 – Autorizar e Instalar Mudanças e Soluções:** Autorização e Colocação em operação de novos sistemas, que atendam a demanda de TI, revendo pós-implementação para assegurar a operabilidade eficaz dos novos sistemas.

3.1.3 Domínio: Entregar e Suportar - DS

Esse domínio refere-se a entrega de serviços solicitados, gerenciamento da segurança e continuidade, serviço de suporte de usuários e gerenciamento de dados e recursos operacionais. Nesse domínio, as questões que auxilia a serem respondidas relativas à Governança de TI são:

- Os serviços de TI, estão sendo entregues e alinhados conforme prioridade de negócio?

- Os custos de TI estão otimizados?

- Os colaboradores são capacitados para melhor utilização de maneira segura e produtiva dos sistemas de TI?

- A confidencialidade, integralidade e disponibilidade da informação, estão sendo adequadamente tratada pela organização?

Os processos do domínio DS são:

- **DS1 – Definir e Gerenciar Níveis de Serviço:** Define um modelo de gerenciamento de serviços, incluindo monitoração e relatórios dos níveis de serviços facilitando o alinhamento entre os serviços de TI e os respectivos requisitos do negócio.
- **DS2 – Gerenciar Serviços de Terceiros:** É o gerenciamento dos serviços terceirizados para satisfação dos requisitos de negócio, é a definição clara de responsabilidades, obrigações e gestão definidas em acordo, bem como a revisão e monitoramento quanto o efetivo e conforme serviço realizado, minimizando assim, os riscos de não cumprimento.
- **DS3 – Gerenciar Desempenho e Capacidade:** Processo faz análise critica periódica de desempenho e capacidade atuais dos recursos de TI , otimizando o desempenho da infraestrutura e a capacitação da TI em responder às necessidades do negócio.
- **DS4 – Assegurar Continuidade de Serviços:** Processo de Desenvolvimento, manutenção e teste de um plano de continuidade de TI para minimizar a probabilidade e o impacto de uma interrupção de serviços prioritários de TI.
- **DS5 - Garantir a Segurança de Sistemas:** Estabelecimento de políticas de segurança, padrões e procedimentos de

segurança de TI, monitoramento e resoluções de vulnerabilidade e incidentes relativas a segurança.

- **DS6 - Identificar e Alocar Custos:** Identificação precisa, justa e razoável de custos, a alocar aos usuários dos serviços de TI.
- **DS7 – Educar e Treinar Usuários:** Processo compreende a definição, execução de uma estratégia, requer a identificação das necessidades de treinamento de cada grupo de usuário e educação efetiva de todos usuários do sistema de TI.
- **DS8 – Gerenciar Central de Serviços e Incidentes:** Processo de implantar de uma central de serviços de TI, para dar suporte às dúvidas e problemas dos usuários de TI e através de efetivos relatórios gerados, mitigar os problemas.
- **DS9 – Gerenciar Configuração:** Assegurar um repositório íntegro das configurações dos ativos de TI, facilitando a disponibilidade do sistema, minimizando questões de produção e solucionando problemas rapidamente.
- **DS10 - Gerenciar Problemas:** Processo de identificação, classificação e análise de problemas e solução de causa-raiz para os problemas de TI.
- **DS11 – Gerenciar Dados:** Manutenção da integridade, da exatidão de informações, o estabelecimento de controle de cópia de segurança, recuperação de dados, assegurando a qualidade , a rapidez e a disponibilidade de dados ao negócio.
- **DS12 – Gerenciar Ambiente Físico:** Manter, proteger um ambiente físico de TI, instalações adequadas, coibindo dano ou roubo de informações e equipamentos.
- **DS13 – Gerenciar Operações:** Definição de políticas e procedimentos de gerenciamento, manutenção, monitoramento da infraestrutura de TI.

3.1.4 Domínio: Monitoração e Avaliação - ME

Com o passar do tempo, todos os processos de TI necessitam ser avaliados para assegurar a qualidade atendendo os requisitos de controle. Este domínio é direcionado ao gerenciamento de performance, o monitoramento de controle interno e a conformidade regulatória da governança de TI. Nesse domínio, as questões que auxilia a serem respondidas relativas à Governança de TI são:

- Há a mensuração de performance para detecção de problemas preventivamente?

- Há gerenciamento efetivo e eficiente assegurando os controles internos da organização?

- O desempenho de TI pode ser associado aos objetivos de negócio?

- Há controles adequados que garantam a confidencialidade, integridade e disponibilidade da informação?

Os processos do domínio ME são:

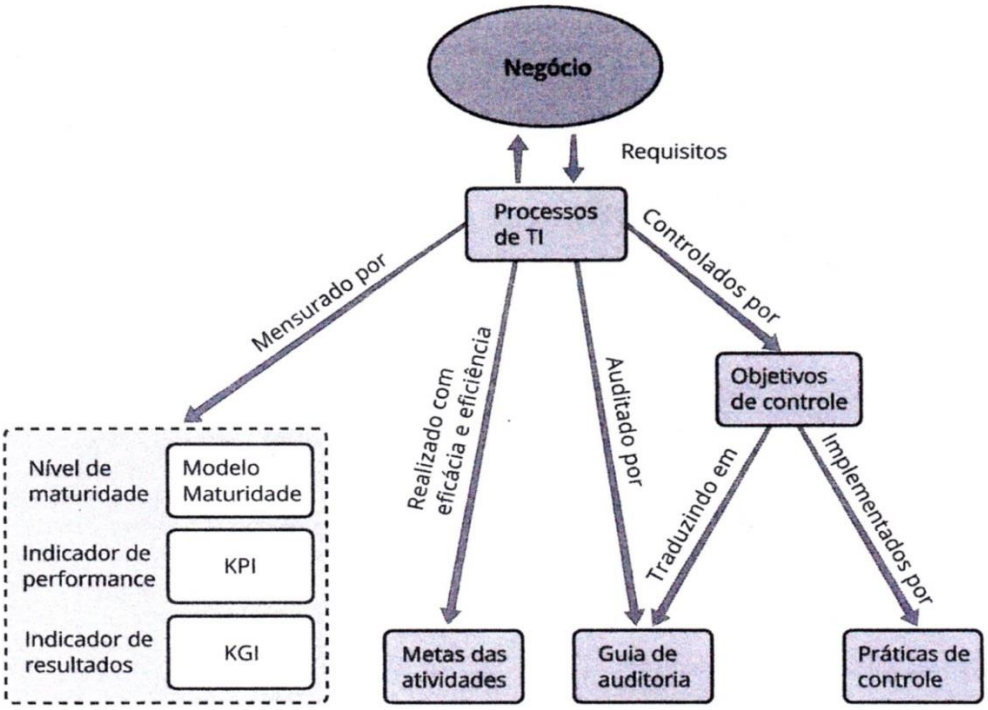
- **ME1 – Monitorar e Avaliar Desempenho de TI:** Procedimento que define os indicadores de desempenho relevantes, sistemáticos e oportunos em conformidade com os requisitos de Governança.
- **ME2 – Monitorar e Avaliar Controles Internos:** Processo de monitoramento bem definido, monitora e reporta as exceções de controle estabelecimento de um programa eficaz de controle interno de TI.
- **ME3 – Assegurar Regulamentação de Conformidade:** Processo que revisa, assegura a conformidade da legislação, regulamentações e requisitos contratuais.
- **ME4 – Prover a Governança de TI:** Processo que integra a Governança de TI às respectivas responsabilidades que assegurem os investimentos de TI esteja alinhada aos objetivos corporativos

entregue em conformidade à legislação e regulamentações contratuais.

3.2 Objetivos de controle de TI:

Conforme mostrado na Figura 08, os processos de TI, são controlados pelos **objetivos de controles para todos os 34 processos**, que traduzem em resultados que espera obter com a implementação de procedimento de controles em uma determinada atividade de TI. Os **objetivos de controle**, são implementados por **práticas de controle de TI**, como exemplo, aquisição de bens e serviços de tecnologia, traduzidos por um **guia de Auditoria**, no qual os processos de TI são **auditados.** Os processos de TI também são associados às **metas de atividades,** realizados com eficácia e eficiência, sendo que a mensuração são realizados pelos **modelos de maturidade, indicadores de performance e resultados.**

Figura 08 - Inter-relacionamentos dos componentes CobiT



Fonte: (Gaseta, 2012, p. 37).

O CobiT é uma ferramenta de suporte, direcionada aos gerentes, executivos e alta direção a resolver problemas relacionados aos requisitos de controle, questões técnicas e de riscos aos negócios.

3.3 Objetivos de controle em relação a TI

Segundo Gaseta (2012, p. 36), os objetivos de TI do CobiT, que são baseados em processos, contribui nos seguintes aspectos:

- Estabelece uma ligação entre a TI e os requisitos de negócios;

- Dentro de um modelo de processo, organiza as atividades de TI;

- Identifica os recursos de TI que suportam os negócios da organização;

- Define o gerenciamento dos objetivos de controle mais significativos para Governança de Ti.

3.3.1 Detalhamento dos Processos Pertinentes à Segurança da Informação

O assunto segurança da informação é tratado pelo CobiT nos seguintes processos:

PO9 - Avaliar e Gerenciar os Riscos de TI: Desenvolver uma estrutura de gerenciamento de riscos de TI, que juntamente com a estrutura de riscos operacionais e de negócio, visam estratégias de mitigar os riscos, assim minimizando os riscos residuais a níveis de tolerância aceitáveis.

O objetivo de TI mais importante deste processo é analisar e comunicar os riscos de TI e seus possíveis impactos, sendo que seu foco está no desenvolvimento de uma estrutura de gerenciamento de riscos de TI integrada às estruturas corporativa, operacional, de riscos, mitigando os riscos, a níveis toleráveis.

Os Ativos de Informação e de TI, baseado na estrutura do CobiT, que são atingidos por esse processo são as aplicações, a informação, a infraestrutura e as pessoas (ITGI, 2007, p. 65).

AI6 – Gerenciar Mudanças: Gerenciamento de maneira controlada de todas as mudanças na organização, incluindo manutenções e correções emergenciais, que devem ser registradas, avaliadas e autorizadas antes da implementação e revisadas, assegurando a mitigação de riscos de impactos negativos ou na integralidade do ambiente de produção.

O objetivo de TI mais importante deste processo é gerenciar mudanças, que atendam aos requisitos de negócio, controlando a avaliação de impacto, autorizando e implementando todas as mudanças na infraestrutura, nas aplicações e nas soluções técnicas de TI.

Os Ativos de Informação e de TI, baseado na estrutura do CobiT, que são atingidos por esse processo são as aplicações, a informação, a infraestrutura e as pessoas (ITGI, 2007, p. 95).

DS4 – Assegurar Continuidade de Serviços: Processo de desenvolvimento, manutenção e teste de um plano de continuidade de TI para minimizar a probabilidade e o impacto de uma interrupção de serviços prioritários de TI.

O objetivo de TI mais importante deste processo é assegurar a continuidade de serviços, assegurando o mínimo de impactos e interrupções de serviços de TI, incorporando recuperações em soluções automatizadas, desenvolvendo, mantendo e testando planos de continuidade.

Os Ativos de Informação e de TI, baseado na estrutura do CobiT, que são atingidos por esse processo são as aplicações, a informação, a infraestrutura e as pessoas (ITGI, 2007, p. 115).

DS5 - Garantir a Segurança de Sistemas: Estabelecimento de políticas de segurança, padrões e procedimentos de segurança de TI, monitoramento e resoluções de vulnerabilidade e incidentes relativas a segurança.

O objetivo de TI mais importante deste processo é garantir a segurança dos sistemas, mantendo a integridade da infraestrutura de informação, e de

processamento, minimizando os impactos de vulnerabilidade e incidentes de segurança, definindo politicas de acesso e procedimentos de segurança, .

Os Ativos de Informação e de TI, baseado na estrutura do CobiT, que são atingidos por esse processo são as aplicações, a informação, a infraestrutura e as pessoas (ITGI, 2007, p. 119).

DS12 – Gerenciar Ambiente Físico: Manter, proteger um ambiente físico de TI, instalações adequadas, coibindo dano ou roubo de informações causadas a equipamento ou pessoas.

O objetivo de TI mais importante deste processo está em gerenciar o ambiente físico, mantendo adequado, protegendo os ativos de TI e informações, promovendo e mantendo um ambiente adequado e seguro fisicamente.

O Ativo de Informação e de TI, baseado na estrutura do CobiT, que é atingido por esse processo está relacionado a infraestrutura, segurança física promovida nas instalações (ITGI, 2007, p. 147).

4 CONSIDERAÇÕES FINAIS

Conforme proposta inicial, este trabalho visa ratificar que a Governança de TI, por meio de uma ferramenta de boas práticas como *CobiT* ***(****Control objectives for information and related Technology****)*****,*** aborda processos que venham a assegurar que as informações sejam confidenciais, integras e disponíveis como forma de viabilizar operações e transações das organizações, como também todo o conhecimento do ambiente de TI que suporta o mundo corporativo das organizações, unificar os aspectos de TI com esta ferramenta de apoio à gestão dos recursos da organização, proporcionando o retorno financeiro dos investimentos em TI, gerenciando os riscos, harmonizando e alinhando com as decisões sobre a gestão dos negócios, pois há a necessidade cada vez maior das organizações interagirem a Governança Corporativa com a Governança de TI, como forma de gerir os sistemas de informações, objetivando maior transparência aos atos, garantindo não só a segurança de informações, mas também todo o conhecimento do ambiente de TI que suporta o mundo corporativo das organizações.

O Cobit, é uma ferramenta focado no negócio, orientado a processos, baseado em controles e direcionados por métricas, ele recomenda a implementação de boas práticas em Governança de TI, que possibilita identificar e especificar os objetivos de controle, ajudando a organização a direcionar os recursos de TI, identificar os processos de TI impactante, que geram riscos para o negócio. O CobiT, segue a premissa que não se gerencia o que não é mensurado.

Organizações estruturadas, preocupadas em investimentos nos ativos e recursos de TI, em boa parte, previnem e asseguram seus bens que são a informação e seu patrimônio de modo geral, e nesse sentido, adotar processos que levam a estruturar a Governança de TI torna a empresa mais forte e segura.

5 REFERÊNCIAS BIBLIOGRÁFICAS

CAVALCANTE, R. G.; MELO, A. de; NOBREGA, P.: **Trabalho necessário:** INOVAÇÃO TECNOLÓGICA E PROJETO EDUCACIONAL DE EMPRESARIADO INDUSTRIAL BRASILEIRO: UMA ANÁSILE CRÍTICA. Ano10, nº 14, 2012. http://www.uff.br/trabalhonecessario/images/TN14RafaelAlessandroPaulo.pdf. Data da Pesquisa 17.03.2014.

http://www.ibgc.org.br . Data da pesquisa 17.03.2014.

ITGI: **CobiT 4.1 Modelo, Objetivos de controle, Diretrizes de Gerenciamento, Modelos de Maturidade.** 2007.200 p.

FERNANDES, A. A.; ABREU, W.F: **Implantando a Governança de TI da Estratégia à Gestão dos Processos e Serviços**. - 3ª ed. - Rio de Janeiro – Brasport, 2012.615 p.

GASETA, E. R.: **Governança de TI** – Rio de Janeiro. RNP/ESR, 2012.162 p.

WELL,P.; ROSS J.W.: **Governança de TI Tecnologia da Informação** – São Paulo – M. Books, 2006. 276p.