UNIVERSIDADE FEDERAL DE PERNAMBUCO

CURSO DE GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO

Governança da Segurança da Informação – Uma proposta de uso combinado do CobiT e da ISO 27002 para sua implementação

Trabalho de Conclusão de Curso elaborado por:

Gustavo Maia

Professora Orientadora: Ana Paula Cabral

Recife, Junho / 2009

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CURSO DE GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO

Governança da Segurança da Informação – Uma proposta de uso combinado do CobiT e da ISO 27002 para sua implementação

Trabalho de Conclusão de Curso apresentado na Universidade Federal de Pernambuco – UFPE – como requisito parcial para obtenção do Grau em Engenharia de Produção.

Recife, Junho / 2009

M217g **Maia, Gustavo.**
Governança da Segurança da Informação: uma proposta de uso combinado do CobiT e da ISO 27002 para sua implementação / Gustavo Maia. – Recife: O Autor, 2009.
viii, 46 folhas, il : grafs., tabs.

TCC (Graduação) – Universidade Federal de Pernambuco. CTG. Curso de Graduação em Engenharia de Produção, 2009.

Inclui Referências Bibliográficas.

1. Engenharia de Produção. 2. Segurança da informação. 3. Governança da Segurança da Informação (GSI). 4. Norma ISO/IEC 27002:2005. 5. *framework* CobiT. I. Título.

UFPE

658.5 **CDD (22. ed.)** **BCTG/2009-117**

AGRADECIMENTO

Meus agradecimentos vão para todos aqueles que de alguma forma contribuíram no meu desenvolvimento acadêmico e na elaboração deste Trabalho de Conclusão de Curso. Gostaria de agradecer, portanto:

- Aos meus pais, pelas oportunidades que me deram;
- Ao meu irmão, pelos grandes ensinamentos;
- A Deus, por me dar forças a todo instante;
- Aos professores do DEP, pelas exposições enriquecedoras ao longo desses anos, e em especial, a Profª. Ana Paula, por todas as sugestões e orientações dadas para a elaboração deste trabalho.
- Aos amigos das turmas de 2004, 2003 e 2005, pelo companheirismo e pelo auxílio prestado durante todo o curso;
- A todos os que se mostraram prestativos e que contribuíram diretamente na elaboração deste trabalho, em especial a: Carolina Siqueira, Mariana Baltar e André Wanderley.

RESUMO

Atualmente, a informação possui um papel crucial no suporte aos processos e às operações de negócio das empresas. A gestão organizacional tem, portanto, dentre outras responsabilidades, a de proteger a informação de forma adequada, garantindo suas características de integridade, disponibilidade e confiabilidade, de maneira a permitir que ela cumpra fielmente sua finalidade. Entretanto, esta tarefa tem se tornado um desafio cada vez maior, visto que no ambiente altamente interconectado de hoje, a informação está sujeita a uma grande e crescente variedade de ameaças e vulnerabilidades. Apesar de ter grande importância para a continuidade dos negócios das organizações, a segurança da informação, muitas vezes, ainda é considerada como uma questão técnica e relegada ao departamento de TI. Uma abordagem ampla da segurança da informação defende a visão de que ela deve tratar a informação como um recurso crítico, que precisa ser levado tão a sério como qualquer outro de igual importância, representando mais um desafio à governança corporativa. Portanto, para se atingir segurança eficaz, executivos precisam estar envolvidos nos processos de avaliação de ameaças e estabelecimento de seus controles. Este trabalho terá, então, como tema a Governança da Segurança da Informação (GSI), esclarecendo seus conceitos e mostrando sua importância atual para as organizações. Ele também versará sobre princípios e melhores práticas que possibilitam sua implementação, estabelecendo, ainda, um comparação entre duas das mais conhecidas, o *framework* do CobiT e a norma ISO/IEC 27002:2005. Por fim, com base nas comparações estabelecidas e nas vantagens e desvantagens de se utilizar cada prática, será proposta uma alternativa de uso combinado de ambas para servir como base para a implementação da GSI nas organizações, a fim de se obter uma melhor utilização de recursos e um maior desempenho organizacional, bem como de se reduzir os riscos e os custos do negócio.

Palavras Chaves: Segurança da Informação, Governança da Segurança da Informação (GSI), Norma ISO/IEC 27002:2005, *framework* CobiT.

SUMÁRIO

1 INTRODUÇÃO 1

1.1 Relevância do Tema 2

1.2 Objetivos 2

1.2.1 Objetivo Geral 2

1.2.2 Objetivos Específicos 2

1.3 Metodologia 3

1.4 Estrutura do Trabalho 3

2 GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO 4

2.1 Informação 4

2.2 Segurança da Informação 5

2.3 Governança da Segurança da Informação 6

2.4 Importância da Segurança da Informação e GSI 10

2.5 Resultados da *Global Information Security Survey 2008* 11

3 PRÁTICAS PARA GOVERNANÇA DA GSI 18

3.1 Princípios gerais para o estabelecimento da GSI 18

3.2 CobiT 20

3.2.1 Visão geral 20

3.2.2 Características do framework 20

3.2.3 Questões de Segurança da Informação e GSI 27

3.3 ISO 27002:2005 29

3.3.1 Visão Geral 29

3.3.2 Estrutura da norma 30

3.3.3 Gestão dos Riscos de Segurança 32

3.4 Comparação entre o *framework* CobiT e a norma ISO 27002 34

3.5 Proposta de uma alternativa de uso do CobiT e da ISO 27002 40

4 CONSIDERAÇÕES FINAIS 43

4.1 Conclusão 43

4.2 Recomendações para trabalhos futuros..... 44

REFERÊNCIAS BIBLIOGRÁFICAS..... 45

LISTA DE FIGURAS

Figura 2.1 – Conseqüências de incidentes com segurança da informação. *12*
Figura 2.2 – Investimentos em segurança da informação. *13*
Figura 2.3 – Padrões de segurança da informação. *14*
Figura 2.4 – Padrões ou frameworks de segurança da informação mais utilizados. *15*
Figura 2.5 – Estratégia da segurança da informação *15*
Figura 2.6 – Nível de dificuldade das iniciativas de segurança da informação. *16*
Figura 3.1 – Princípio básico do framework CobiT. *20*
Figura 3.2 – Definindo os objetivos e a arquitetura de TI. *22*
Figura 3.3 – Visão geral do framework CobiT. *28*
Figura 3.4 – Estrutura do framework CobiT vs. Estrutura da ISO 27002. ..... *40*

LISTA DE TABELAS

Tabela 3.1 – Pertinência (P-Primária ou S-Secundária) das atividades desenvolvidas pelo CobiT e pela ISO 27002 com relação ao público-alvo..... 36
Tabela 3.2 – Mapeamento de Alto Nível da ISO/IEC 27002:2005 no CobiT..... 37
Tabela 3.3 – Pertinência (P-Primária ou S-Secundária) das atividades desenvolvidas pelo uso combinado do CobiT e da ISO 27002 com relação ao público-alvo..... 42

1 INTRODUÇÃO

Os grandes avanços tecnológicos e a globalização da economia no mundo ocorridos, nas últimas décadas, permitiram uma grande integração dos mercados e, conseqüentemente, um aumento significativo da concorrência empresarial, nunca antes vivenciado pelas organizações. A alta concorrência existente na conquista dos mercados força as empresas a buscar, cada vez mais, formas de otimizar o uso de seus recursos para conduzir melhor seus negócios e satisfazer às necessidades de seus clientes, de forma a manter ou ampliar seu espaço no mercado. Se racionalmente utilizada, a informação pode contribuir para a criação de um diferencial competitivo a essas empresas.

A essa realidade, acrescentam-se ainda mudanças globais em termos de governança que afetam diretamente as práticas de gestão organizacional, dentre as quais, estão as de gestão da informação. Devido a um número significativo de falhas graves por parte de grandes organizações ocorridas na última década, autoridades reguladoras têm elaborado um conjunto complexo de novas leis e normas com intuito de forçar a melhoria da governança, segurança, controle e transparência organizacionais (ITGI, 2006).

Além disso, a grande abertura e acessibilidade que estimulou a adoção e o crescimento das redes privadas e da Internet também ameaçam a privacidade dos indivíduos, a confidencialidade das informações de negócio e a integridade das transações. As maiores preocupações são os riscos com roubo, alteração, interceptação e disseminação de dados confidenciais, como também fraude, perda de reputação e perdas econômicas. Essas ameaças podem provir tanto do ambiente externo (concorrentes, *hackers*...), como do ambiente interno (empregados descontentes, subcontratados curiosos...). Independentemente de onde elas provenham, a conjunção de todas têm se tornado um problema crítico e de difícil gerenciamento para garantir a proteção das informações das empresas (Entrust, 2004).

Dado que a segurança da informação é vista muitas vezes somente sob uma perspectiva técnica, ela parece não ter a atenção devida da diretoria e alta administração das organizações. Em um relatório do *Corporate Governance Task Force* é proposto que, para proteger melhor a infraestrutura de TIC, as organizações deveriam incorporar as questões de segurança computacional em suas ações de governança corporativa (CGTFR, 2004).

Neste novo cenário, surge a necessidade de uma abordagem de governança para a gestão da informação. Seja por motivos mercadológicos, regulamentares (relativos às leis sobre privacidade e retenção da informação, por exemplo), ou tecnológicos (relativos às significativas ameaças as quais estão sujeitos os sistemas de informação), faz-se necessária, então, a proteção do maior ativo existente nas organizações – sua informação.

1.1 Relevância do Tema

Este tema possui grande relevância para toda e qualquer organização, independentemente de seu tamanho ou tipo de negócio, visto que na atual Era da Informação e do Conhecimento, as empresas se vêem cada vez mais dependentes da informação para boa gestão de seus negócios, como já notava Peter Drucker (1993), a mais de duas décadas atrás: *"A difusão da tecnologia e da comodidade da informação transformam o papel da informação em um recurso de igual importância aos importantes recursos tradicionais de terra, labor e capital"*.

Deve ser ressaltado o interesse que o trabalho pode vir a gerar devido ao seu conteúdo que enfatizará a aplicação prática dos conceitos reunidos nele à realidade das empresas.

1.2 Objetivos

1.2.1 Objetivo Geral

O objetivo geral deste trabalho é estabelecer uma comparação entre o *framework* do CobiT (*Control Objectives for Information and Related Technology*) e a norma ISO/IEC 27002:2005 (Código de Prática para a Gestão da Segurança da Informação), e propor uma alternativa que utiliza ambas as práticas para a implementação de uma eficaz Governança da Segurança da Informação (GSI).

1.2.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- Apresentar os conceitos de Segurança da Informação e de GSI;
- Mostrar a importância destes temas para as organizações atuais;
- Apresentar como estão estruturados o *framework* do CobiT e a norma ISO/IEC 27002:2005 e como estes abordam às questões de Segurança da Informação e GSI;
- Estabelecer uma comparação entre o *framework* CobiT e a norma ISO/IEC 27002:2005;
- Propor uma alternativa de uso de ambas as práticas para a implementação da GSI.

1.3 Metodologia

Quanto à natureza, esta poderá ser classificada como pesquisa aplicada, já que visa à geração de conhecimentos para aplicação prática, podendo auxiliar na solução de problemas enfrentados no ambiente organizacional pelas empresas.

Uma das técnicas de pesquisa a ser utilizada será a de documentação indireta, mais especificamente, a pesquisa bibliográfica. Esta técnica foi escolhida porque é a que melhor se adequa à execução de levantamento de dados pertinentes para a elaboração do trabalho. Ela consiste, basicamente, na identificação, seleção e compilação de informações relevantes e de confiável procedência. A partir dela, será possível estabelecer uma base teórica rica o suficiente para a elaboração de um trabalho que poderá ampliar o conhecimento existente sobre o assunto estudado.

1.4 Estrutura do Trabalho

Além do capítulo introdutório, este trabalho está dividido em outros 3 capítulos, que serão brevemente apresentados a seguir.

No capítulo 2 serão apresentados os conceitos de informação, segurança da informação e governança da informação, inseridos no contexto atual de negócios vivido pelas organizações. Além disso, será também mostrada a importância desses temas para a normalidade e continuidade dos negócios das organizações. Por fim, serão apresentados os resultados mais relevantes de uma pesquisa de âmbito mundial recentemente realizada sobre Segurança da Informação.

No capítulo 3 será apresentada, inicialmente, uma visão geral sobre os princípios gerais para o estabelecimento da GSI. Posteriormente, serão apresentadas as estruturas e os principais aspectos relacionados às questões de Segurança da Informação e GSI de duas das principais práticas internacionalmente aceitas: o *framework* do CobiT e a norma ISO/IEC 27002:2005. Por fim, será proposta uma alternativa de uso combinado dessas práticas para a implementação da GSI.

Por último, no capítulo 4, serão apresentadas as conclusões deste trabalho, bem como as sugestões para trabalhos futuros.

2 GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

Neste capítulo serão apresentados os conceitos de informação, segurança da informação e governança da informação, inseridos no contexto atual de negócios vivido pelas organizações. Além disso, será também mostrada a importância desses temas para a normalidade e continuidade dos negócios das organizações. Por fim, serão apresentados os resultados mais relevantes de uma pesquisa de âmbito mundial recentemente realizada sobre Segurança da Informação.

2.1 Informação

Vários são os conceitos encontrados sobre informação na literatura. Segundo a definição do dicionário Michaelis, a palavra informação pode significar, dentre outros: 1) Ato ou efeito de informar; 2) Transmissão de notícias; 3) Comunicação; 4) Ação de informar-se; 5) Instrução, ensinamento; 6) Transmissão de conhecimentos.

Segundo Almeida et al (2002), a informação é um produto obtido de um sistema de produção que utiliza dados como matéria-prima. Estes, por sua vez, correspondem a um conjunto de letras, números ou dígitos, que se tomados isoladamente, não transmitem nenhum conhecimento (REZENDE, 2005).

A informação pode existir em várias formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida por carta ou por meio eletrônico, mostrada em filmes ou comunicada numa conversa. Qualquer que seja sua forma, ou meio usado para seu armazenamento ou compartilhamento, ela deve sempre ser protegida adequadamente (ISO/IEC 27002:2005).

No ambiente organizacional, informação pode ser considerada como um “ativo” que, como outros importantes ativos, é essencial para os negócios da organização e, consequentemente, precisa ser protegido. Esse fato torna-se ainda mais importante no atual cenário de negócios, onde eles estão cada vez mais interconectados. Como resultado desse crescimento em interconectividade, a informação está exposta a um número cada vez maior e a uma variedade cada vez mais ampla de ameaças e vulnerabilidades (ISO/IEC 27002:2005).

Atualmente, a informação possui um papel crucial no suporte às operações de negócio das empresas. Durante cada ciclo da operação, a informação entra em contato com pessoas, processos e tecnologia. Cada um desses elementos possui o potencial de apresentar um risco real contra os “ativos” de informação da empresa. Dessa forma, para assegurar que as informações de negócio

continuem a prover suporte às operações, várias características chaves precisam ser preservadas. (BS 7799, 1999).

A primeira dessas características é a confidencialidade. Segundo Humphreys *et al (apud* SHAUN, 2004), assegurar a confidencialidade envolve "proteger informação sensível contra revelação ou interceptação não autorizada". Em outras palavras, para manter a confidencialidade da informação, ela precisa estar sob sigilo e bem guardada, não podendo estar livremente disponível a qualquer um que queira acessá-la (SHAUN, 2004).

A segunda característica a ser preservada é a integridade. Preservar a integridade da informação envolve manter sua exatidão e compreensão intactas no tempo. (HUMPHREYS et al, 1998 *apud* SHAUN, 2004). Se a informação não estiver correta ou completa, poderá levar a uma decisão inapropriada por parte dos gestores. Como conseqüência, tais decisões levariam a situações indesejadas na organização, que poderiam ter sido prevenidas. Falhas de integridade podem surgir como resultado de uma modificação intencional, ou não, quando do armazenamento, processamento ou transmissão da informação (SHAUN, 2004).

A terceira característica a ser preservada é a disponibilidade. Para prover disponibilidade, a organização deve assegurar que os recursos de informação estão acessíveis ao uso, pelas partes apropriadas, no momento certo. Sem acesso às informações a tempo, as organizações seriam incapazes de continuar com normalidade suas operações. (GERBER et al, 2001 *apud* SHAUN, 2004).

A prioridade e significância relativa da confidencialidade, disponibilidade e integridade variam de acordo com dada informação dentro do sistema de informação e o contexto de negócio em que ela é usada. Por exemplo, a integridade pode ser especialmente importante para as informações gerenciais, devido ao impacto que ela tem nas decisões críticas de estratégia. Por outro lado, a confidencialidade é sem dúvida um ponto crítico quando a informação tem caráter pessoal, financeiro ou está associada a segredos comerciais e outras formas de propriedade intelectual (ITGI, 2006).

2.2 Segurança da Informação

Segundo a norma ISO/IEC 27002:2005, segurança da informação é a proteção da informação de uma ampla variedade de ameaças, de forma a assegurar a continuidade dos negócios, minimizar riscos e maximizar retornos sobre investimentos e oportunidades de negócios.

Diferentemente da segurança da tecnologia da informação, que está preocupada com a segurança da informação limitada ao âmbito da tecnologia de infraestrutura das redes, a segurança da informação lida com todas as formas de informação discutidas anteriormente (escrita, impressa, falada, etc) e com todas as fases de seu ciclo de vida (criação, visualização, transporte, armazenamento ou destruição) (ITGI, 2006).

A informação confidencial revelada numa conversa de elevador ou enviada por *email*, por exemplo, estaria fora do escopo da segurança da tecnologia da informação. Entretanto, do ponto de vista da segurança da informação, a natureza ou meio de transmissão da informação não são tão importantes quanto o fato de que a segurança foi violada; essa é a preocupação principal (ITGI, 2006).

A segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, quando necessário, para assegurar que a segurança necessária e os objetivos dos negócios sejam atingidos. Isso deve ser feito conjuntamente com outros processos de gerenciamento de negócios (ISO/IEC 27002:2005).

2.3 Governança da Segurança da Informação

Até recentemente, o foco da segurança da informação tinha sido dado à proteção dos sistemas de Tecnologia da Informação (TI), que processam e armazenam uma vasta quantidade de informação, em vez de ser dada à informação propriamente dita. Entretanto, essa abordagem é muito limitada para alcançar o nível de integração, a confiabilidade processual e a proteção geral, que se fazem necessários agora. (ITGI, 2006).

Para alcançar eficácia e sustentabilidade num mundo complexo e interconectado, como é o de hoje, a segurança da informação precisa ser tratada nos níveis mais altos da organização, e não considerada como uma especificidade técnica delegada ao departamento de TI (ITGI, 2006).

Uma abordagem ampla da segurança da informação incorpora a visão de que a informação da organização deve ser protegida adequadamente, visto que ela permeia um universo de riscos, benefícios e processos, da mesma forma que os demais recursos organizacionais. Assim, a segurança da informação deve tratá-la como um recurso crítico, que precisa ser levado a sério, representando mais um desafio à governança corporativa e envolvendo questões importantes,

como o gerenciamento de riscos. Segurança eficaz requer o envolvimento de executivos para avaliar ameaças emergentes e o poder da organização em responder a elas (ITGI, 2006).

Segundo o *IT Governance Institute* (2006), governança corporativa pode ser definida como: "conjunto de responsabilidades e práticas exercidas pelos diretores e pelo conselho administrativo com o propósito de prover direcionamento estratégico, de forma a assegurar que os objetivos sejam atingidos, que os riscos sejam gerenciados apropriadamente e que os recursos sejam usados racionalmente".

Atualmente, os sistemas e os serviços de tecnologia da informação desempenham um papel vital na coleta, análise, produção e distribuição da informação indispensável à execução do negócio das organizações. Dessa forma, tornou-se essencial o reconhecimento de que a TI é crucial, estratégica e um importante recurso que precisa de investimento e gerenciamento apropriados. Esse cenário motivou o surgimento do conceito de governança da tecnologia da informação e comunicação, do termo inglês *IT Governance*, através da qual se procura o alinhamento da TI com os objetivos da organização (BERNARDES e MOREIRA, 2005).

Segundo ITGI (2006), a Governança da Tecnologia da Informação e Comunicação pode ser definida como "uma estrutura de relacionamentos entre processos para direcionar e controlar uma empresa de modo a atingir seus objetivos corporativos, através da agregação de valor e controle dos riscos pelo uso da TI e seus processos". Para Van Grembergen (2003), *apud* Bernardes e Moreira (2005), ela é definida como a "capacidade organizacional exercida pelo conselho diretor, gerente executivo e o gerente de TI de controlar o planejamento e implementação das estratégias de TI e dessa forma, permitir a fusão de TI ao negócio".

A Governança da Segurança da Informação (GSI), por sua vez, deve ser parte transparente e integral da governança corporativa e estar alinhada com o *framework* de governança de TI. Os executivos seniores têm a responsabilidade de considerar e responder às preocupações e interesses gerados pela segurança da informação, enquanto diretores serão cobrados a fazer da segurança da informação parte intrínseca da governança, integrada aos processos já existentes (ITGI, 2006).

A governança da segurança da informação, então, pode ser entendida como um subconjunto da governança corporativa que provê direcionamento estratégico, assegura que objetivos sejam alcançados, gerencia riscos apropriadamente, usa recursos organizacionais responsavelmente e monitora o sucesso ou fracasso do programa de segurança da organização (ITGI, 2006).

Para se colocar em prática uma eficaz governança corporativa e da segurança da informação, diretores e executivos seniores precisam ter um entendimento claro do que esperar de seu programa de segurança da informação. Eles precisam saber como conduzir a implementação de um programa de segurança da informação, saber como avaliar seus próprios cargos com respeito a este programa e saber como definir sua estratégia e seus objetivos, de forma a torná-lo eficaz (ITGI, 2006).

A GSI consiste de liderança, estruturas organizacionais e processos que protegem a informação. Um ponto crítico para o sucesso dessas estruturas e processos é a comunicação eficaz entre as partes interessadas baseada em relacionamentos construtivos, de linguagem comum e comprometimento mútuo para tratar dos problemas. E o que se pode esperar como resultado da GSI? Basicamente, pode-se esperar (ITGI, 2006):

1. Alinhamento estratégico da segurança da informação com as estratégias de negócio de forma a suportar o alcance dos objetivos organizacionais;
2. Gerenciamento de riscos através da execução apropriada de avaliações para sua identificação, mitigação e redução de seus potenciais impactos nos recursos de informação a um nível aceitável;
3. Gestão de recursos através da utilização eficiente e eficaz do conhecimento da segurança da informação e da infraestrutura;
4. Avaliação de *performance* através da medição, monitoramento e comunicação de indicadores de GSI para assegurar que objetivos organizacionais são atingidos;
5. Valor agregado através da otimização dos investimentos com segurança da informação no suporte ao alcance de objetivos organizacionais.

A Associação Americana de Diretores Corporativos (NACD), organização líder nos EUA de associados conselheiros e diretores, reconhece a importância da segurança da informação. Ela recomenda quatro práticas essenciais para o conselho administrativo, como também várias práticas específicas para cada ponto, quais sejam:

- Colocar a segurança da informação na pauta do conselho;
- Identificar líderes, torná-los responsáveis pela segurança da informação e suportá-los no que for preciso;
- Assegurar a eficácia da política corporativa de segurança da informação através de revisões e aprovações;

- Designar a segurança da informação a um comitê chave e assegurar suporte a esse comitê.

Segundo Allen (2005), "governar a segurança corporativa significa visualizar uma segurança adequada como um requisito não-negociável no mundo dos negócios. Se a gestão da organização – incluindo seus conselheiros, diretores e gerentes – não estabelecerem e enfatizarem a necessidade nos negócios de se ter uma eficaz segurança corporativa, então, o estágio de segurança desejado pela organização não será articulado, atingido ou mantido. Para obter uma capacidade sustentável, as organizações precisam fazer da segurança uma responsabilidade dos líderes no nível de governança, e não daqueles com pouca autoridade, autonomia e recursos para agir e cumprir requisitos regulamentares".

Alguns dos benefícios relevantes gerados pela GSI incluem (ITGI, 2006):

- Incremento de seu valor de mercado para organizações que fazem uso de boas práticas de governança;
- Aumento da previsibilidade das operações de negócio através da redução da probabilidade de ocorrência (a níveis aceitáveis) dos riscos associados à segurança da informação;
- Proteção contra possíveis ônus de responsabilidade legal ou civil como resultado de falta de informação ou ausência de cuidado devido;
- Sistema e estrutura para otimizar a alocação de recursos limitados de segurança;
- Garantia de uma política de segurança da informação eficaz e de conformidade com regulamentações;
- Uma base firme para prover um eficiente e eficaz gerenciamento de riscos, melhoria de processos e rápido poder de resposta aos incidentes relacionados com a segurança da informação;
- Maior garantia de que a tomada de decisões críticas não será feita com base em informações falhas;
- Capacidade de "prestação de contas" durante atividades e momentos críticos, como fusões e aquisições, processo de recuperação de negócios e respostas às fiscalizações/regulamentações.

Esses benefícios adicionam significativo valor às organizações ao (ITGI, 2006):

1. Aumentar a confiança nas relações com clientes;
2. Proteger sua reputação;
3. Reduzir a probabilidade de violações de privacidade;

4. Prover maior segurança nas interações com parceiros comerciais;
5. Possibilitar novas e melhores formas de processar transações eletrônicas;
6. Reduzir custos operacionais por prover resultados previsíveis – mitigando fatores de risco que possam interferir neste processo.

Para assegurar que todos os elementos relevantes de segurança sejam tratados na estratégia de segurança da organização, várias práticas (padrões, *frameworks*, documentos orientativos, etc) sobre segurança têm sido desenvolvidas para servir de guia e garantir clareza de entendimento a essa questão. As mais comuns usadas atualmente pelas organizações são: ISO 27002:2005, CobiT (*Control Objectives for Information and related Technology)* e ITIL (*Information Technology Infraestructure Library*).

2.4 Importância da Segurança da Informação e GSI

Como dito anteriormente, os dados são a matéria-prima da informação. Se tomados de forma isolada são inúteis, até que sejam organizados e manipulados de uma forma que produzam informação. A informação, por sua vez, é a base para o conhecimento. Ao se juntar e cruzar informações, de forma que ela possa ser usada para realizar algo útil, se cria conhecimento. A informação e o conhecimento proveniente dela têm se tornado ativos cada vez mais importantes, isto é, críticos para os negócios das organizações, sem os quais muitas delas cessariam simplesmente suas operações (ITGI, 2006). Nada mais lógico, portanto, que proteger o maior ativo existente nas organizações.

Além disso, as organizações, seus sistemas de informação e suas redes têm se deparado com ameaças provenientes de uma ampla variedade de fontes, como fraudes, espionagens, sabotagens, vandalismos, incêndios ou inundações. Outras ameaças ainda incluem: códigos maliciosos, ataques de *hackers* e de negação de serviço (*denial of service*), cada vez mais comuns, pretensiosos e sofisticados. Agravando ainda mais esse quadro, muitos sistemas de informação não foram projetados para serem seguros (ISO/IEC 27002:2005).

Inúmeros são os casos reais de ameaças que se materializaram e geraram prejuízos, por vezes difíceis de mensurar, às organizações que não souberam se proteger adequadamente. Muitos deles ocorridos, inclusive, em organizações que, sem sombras de dúvida, investem significativamente em segurança da informação.

Para citar um exemplo, recentemente, um grupo de *hackers* invadiu os sistemas de computação do Departamento de Defesa dos Estados Unidos e copiou informações sobre a construção do caça

F-35 Lightning II, o mais caro projeto já conduzido pelo Pentágono. De acordo com o "*Wall Street Journal*", os piratas copiaram informações que, em teoria, poderiam ensinar militares de outros países a se defender do avião, também conhecido como *Joint Strike Fighter*, cujo projeto está orçado em US$ 300 bilhões (Site da Globo.com, 2009).

Considerando-se a realidade brasileira, segundo a reportagem de capa da Revista VEJA (2009), o país é o quarto mais contaminado por vírus e programas capazes de furtar informações, alterar ou destruir dados dos computadores, o que mostra pouca familiarização com o uso do computador e da internet por parte dos brasileiros. Esta falta de familiaridade, em realidade, não exclusiva dos usuários de computador do país, torna-se mais um fator, dentre vários, a ser considerado na definição das medidas de segurança da informação das organizações, já que estes mesmos usuários serão os que vão operar seus sistemas de informação.

Em face a esses desafios, a segurança da informação buscará ajudar as organizações a mitigar os vários riscos associados a ela, através da aplicação de um conjunto adequado de controles de segurança, sejam eles físicos, técnicos e/ou operacionais. Exemplos de controles desta natureza seriam: fechaduras em portas, senhas de acesso a usuário ou políticas e procedimentos de segurança. A segurança da informação, portanto, auxilia as organizações a compartilhar suas informações de negócio de forma confiável, construindo e mantendo relacionamentos confiáveis com seus clientes, fornecedores e outros parceiros de negócio. Por sua vez, esses relacionamentos contribuem para aumentar o fluxo de caixa e a rentabilidade dos negócios (BS 7799, 1999).

Além deste aumento em fluxo de caixa, há também aumento no valor de mercado das organizações quando investidores tomam conhecimento de que elas possuem boas práticas de governança corporativa e de GSI, como sugere o estudo feito pela McKinsey (2003), conjuntamente com a *Institutional Investors Inc.* Segundo tal estudo, pode-se concluir que grandes investidores internacionais estão propensos a pagar até 10% a mais pelas ações de uma organização reconhecida por suas boas práticas de governança.

2.5 Resultados da *Global Information Security Survey 2008*

A seguir serão apresentados resultados e conclusões de uma pesquisa de segurança da informação de grande prestígio internacional, que revelam o atual estado e as preocupações principais dos executivos com respeito aos temas da área. Essa pesquisa (*Global Information Security Survey 2008*) foi coordenada e realizada pela empresa *Ernst & Young*, entre Junho e

Agosto de 2008, e contou com a colaboração de aproximadamente 1.400 executivos de organizações das principais indústrias e setores de 50 países.

Dentre as maiores descobertas da pesquisa, destacam-se:

1. **A proteção da reputação e da marca tornou-se um *driver* significante para a segurança da informação.** Quando perguntados sobre qual seria o nível de significância das conseqüências sobre perdas, indisponibilidade ou comprometimento da informação, 85% dos participantes responderam que dano a reputação e a marca seriam as mais significativas. As perdas de confiança pelos *stakeholders* (77%), de receitas (72%) e de clientes (71%), também foram conseqüências identificadas como significativas de incidentes com segurança da informação.

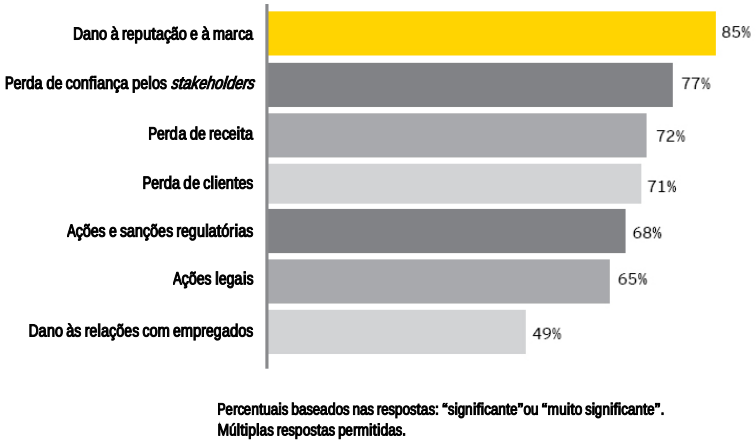


Figura 2.1 – Conseqüências de incidentes com segurança da informação.
Fonte: Ernst & Young (2008).

A preservação da reputação e da marca foi citada por 78% dos participantes como importante *driver* para a segurança da informação. Também foram considerados importantes *drivers* o alcance de conformidade com as políticas corporativas (77%) e com as regulamentações (79%).

De posse dessa informação, a pesquisa conclui, então, que a necessidade de proteger reputação e marca fez com que muitas empresas fossem além dos requerimentos de conformidade com regulamentações para tentar alcançar uma função mais integrada da segurança da informação.

2. **Apesar das pressões econômicas, as organizações continuam investindo em segurança da informação.** Quando perguntados sobre qual assertiva melhor descreveria o investimento anual da organização com segurança da informação, apenas 5% dos

participantes responderam que reduziriam seus gastos anuais e 50% responderam que planejam aumentar os investimentos com segurança da informação considerando-se seu percentual sobre os gastos totais.

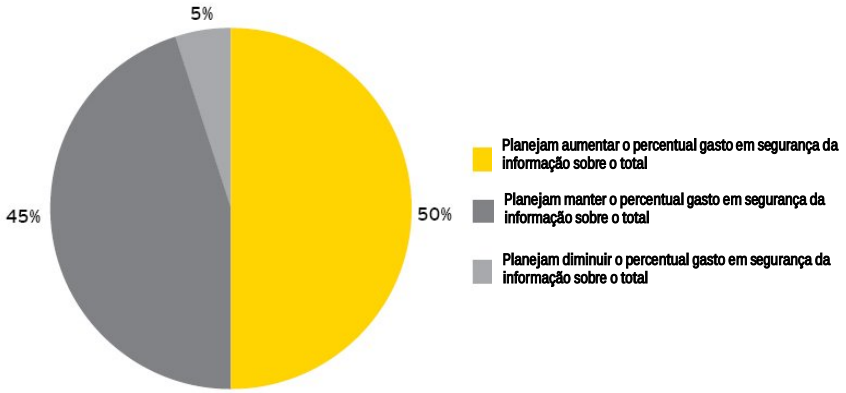


Figura 2.2 – Investimentos em segurança da informação.
Fonte: Ernst & Young (2008).

De posse dessa informação, a pesquisa conclui, então, que as organizações deverão continuar investindo em segurança da informação por duas razões em particular: a primeira é a de que reduzir os investimentos com segurança da informação causará um impacto negativo na percepção dos stakeholders mais importantes, e a segunda é a de que a variabilidade das ameaças e vulnerabilidades, bem como a freqüência de ataques, não param de crescer.

3. **Padrões internacionais de segurança da informação estão ganhando maior aceitação e adoção.** Segundo os pesquisadores, o uso de padrões internacionalmente aceitos de segurança da informação irá prover àqueles que os adotarem cedo uma vantagem competitiva. Da mesma forma que normas de gestão da qualidade, como as da família ISO 9000, se tornaram um requisito para fazer negócios em certas indústrias, padrões internacionais de segurança da informação continuarão a ganhar aceitação e eventualmente se tornarão uma necessidade para muitas organizações. Padrões e certificações proporcionam um nível de segurança para clientes e parceiros que é difícil de ser obtido com qualquer outro meio.

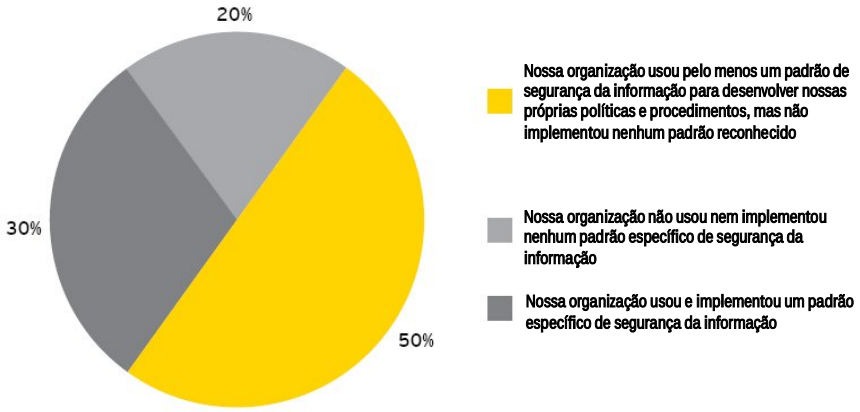


Figura 2.3 – Padrões de segurança da informação.
Fonte: Ernst & Young (2008).

De 2007 a 2008, houve um aumento de 8% no número de participantes da pesquisa que declararam haver incorporado algum padrão de segurança da informação (80%). Especificamente ao se comparar a adoção da norma ISO/IEC 27002:2005, de 2007 para 2008, nota-se um incremento de 9%.

A figura 2.4 ressalta os padrões de segurança da informação e *frameworks* de TI mais utilizados pelas empresas pesquisadas. Como poderá ser observado, os três mais usados são: os *frameworks* ITIL e CobiT e a norma ISO 27002. Segundo o *Office of Governance Commerce* (OGC, 2000), *apud* BERNARDES e MOREIRA (2005), o *framework* ITIL foi desenvolvido pelo governo britânico no final da década de 1980 e tem como foco principal a operação e a gestão da infraestrutura de TI na organização, incluindo todos os pontos importantes no fornecimento e manutenção dos serviços de TI (OGC, 2000). Apesar de ser amplamente utilizado, o ITIL não trata as questões de segurança da informação de forma tão direta e explícita, através de objetivos de controle e controles bem definidos, como fazem o *framework* CobiT e a norma ISO 27002, e por este motivo, não foi considerado alvo de estudo deste trabalho.

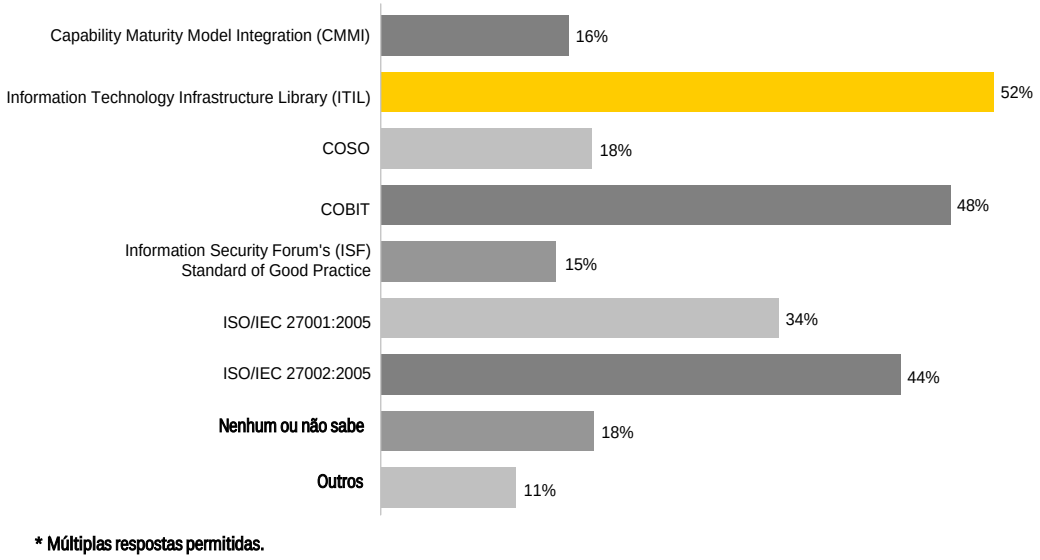


Figura 2.4 – Padrões ou frameworks de segurança da informação mais utilizados.
Fonte: Ernst & Young (2008).

4. **Muitas organizações ainda lutam para conseguir uma visão estratégia da segurança da informação.** Quando perguntados se a organização para a qual trabalhavam possuía uma estratégia de segurança da informação documentada para os próximos três anos, 29% dos participantes responderam que não, 20% responderam que a organização tinha desenvolvido uma estratégia específica para a segurança da informação, 33% responderam que a estratégia de segurança da informação estava integrada com a estratégia de TI e 18% responderam que a segurança da informação estava integrada à estratégia de negócio da organização.

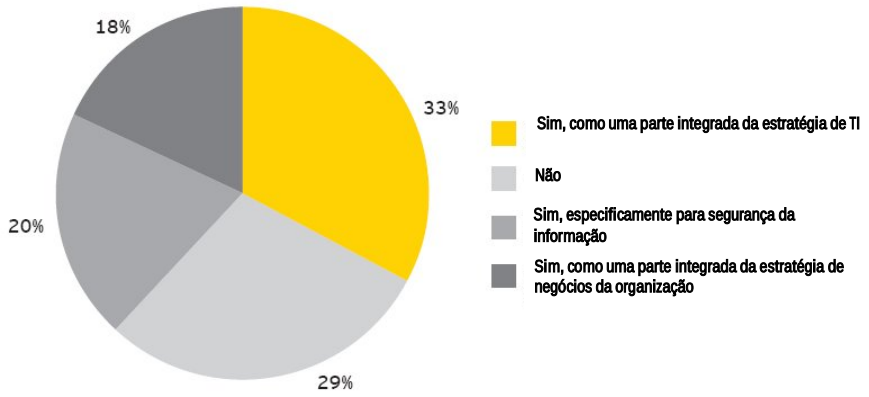


Figura 2.5 – Estratégia da segurança da informação.
Fonte: Ernst & Young (2008).

Segundo os pesquisadores, o desafio para muitas organizações é de como integrar completamente a segurança da informação e fazê-la parte do negócio. De forma simplificada, isso poderia ser feito em um processo de dois passos. Primeiro, as organizações devem querer trazer a segurança da informação para as discussões estratégicas como valiosa parceira. Segundo, os responsáveis pela segurança da informação devem ter uma visão mais focada em negócios, envolvendo-se em discussões sobre a mudança na cultura organizacional, estabelecendo processos confiáveis e desenvolvendo treinamentos e programas de conscientização de sua importância aos empregados.

5. **As pessoas ainda são o "ponto fraco" da segurança da informação**. Quando perguntados sobre qual seria o nível de dificuldade em conseguir que certas iniciativas de segurança da informação sejam eficazes, 50% dos participantes responderam que a conscientização organizacional é a que representa o maior desafio, mais do que a disponibilidade de recursos (48%), o orçamento adequado (33%) e o tratamento de novas ameaças e vulnerabilidades (33%).

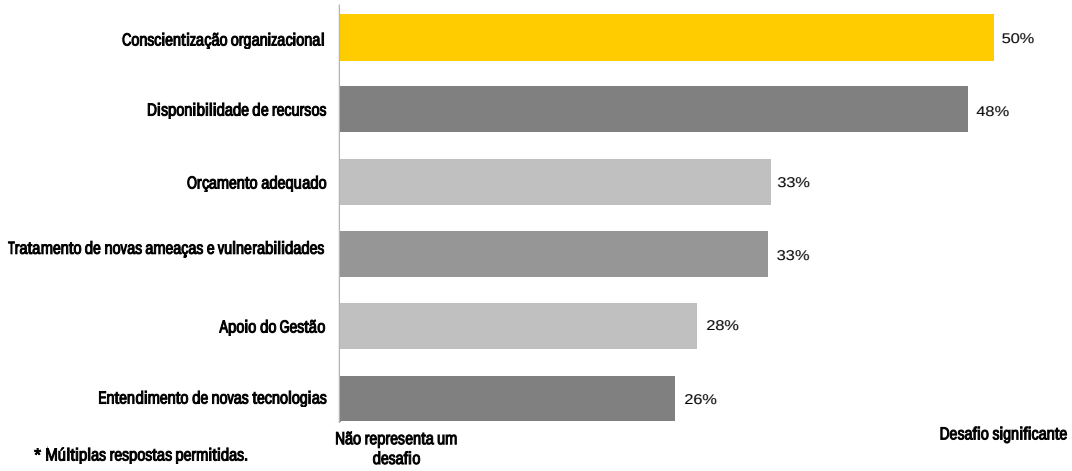


Figura 2.6 – Nível de dificuldade das iniciativas de segurança da informação.
Fonte: Ernst & Young (2008).

Segundo os pesquisadores, a tecnologia tem um papel essencial na segurança da informação, mas deve haver também foco em treinamentos e em programas de conscientização para a segurança da informação operar eficazmente. As organizações devem ver as pessoas tão críticas quanto qualquer outro componente da segurança da

informação – para que elas possam ajudar a prevenir e a responder adequadamente aos incidentes de forma eficaz e oportuna.

3 PRÁTICAS PARA GOVERNANÇA DA GSI

No capítulo 3 será apresentada, inicialmente, uma visão geral sobre os princípios gerais para o estabelecimento da GSI. Posteriormente, serão apresentadas as estruturas e os principais aspectos relacionados às questões de Segurança da Informação e GSI de duas das principais práticas internacionalmente aceitas: o *framework* do CobiT e a norma ISO/IEC 27002:2005. Por fim, será proposta uma alternativa de uso combinado dessas práticas para a implementação da GSI.

3.1 Princípios gerais para o estabelecimento da GSI

Segundo relatório do *Corporate Governance Task Force* (2009), as organizações possuem necessidades distintas e, por conta disso, variam na abordagem dada à segurança da informação. Desta forma, foram identificados nesse relatório um conjunto de princípios gerais para ajudá-las na orientação dos esforços à implementação da GSI. Ao considerar tais princípios, as organizações poderão desenvolver um programa de segurança da informação mais adequado para suas necessidades, quais sejam:

1. Os *Chief Executive Officers* (CEO) devem conduzir uma avaliação anual da segurança da informação, analisar os resultados com as equipes e comunicá-los para o conselho administrativo;
2. As organizações devem conduzir periodicamente uma avaliação de riscos relacionados às suas informações como parte do seu programa de gerenciamento de riscos;
3. As organizações devem implementar políticas e procedimentos baseados em análises de riscos para garantir a segurança da informação;
4. As organizações devem estabelecer uma estrutura de gerenciamento da segurança da informação para que seja possível definir papéis e responsabilidades para cada indivíduo;
5. As organizações devem desenvolver um planejamento estratégico e tomar medidas para prover a segurança da informação em suas redes de comunicação, instalações e sistemas;
6. As organizações devem tratar a segurança da informação como parte integral do ciclo de vida dos sistemas;
7. As organizações devem divulgar as informações sobre segurança da informação e promover treinamentos aos indivíduos;
8. As organizações devem conduzir periodicamente testes e avaliações sobre a eficácia das políticas e procedimentos relacionados à segurança da informação;

9. As organizações devem criar e executar um plano de remediação das deficiências que comprometam a segurança da informação;
10. As organizações devem desenvolver e implementar procedimentos de resposta aos incidentes com segurança da informação;
11. As organizações devem estabelecer planos, procedimentos e testes para prover continuidade das operações;
12. As organizações devem fazer uso das melhores práticas existentes, para medir a *performance* da segurança da informação e melhorar continuamente sua governança.

Nesse processo de estabelecimento da GSI, as organizações tem se dado conta de que é preferível ter como referência práticas reconhecidas internacionalmente para a implementação da GSI, em vez de tratá-la de forma não planejada e "caseira" (SOLMS, 2005).

Corroborando com o que acaba de ser exposto, existe uma série de razões convincentes para a adoção desses padrões, dentre os quais, estão (SPAFFORD, 2003):

1. A roda foi inventada – Nos dias de hoje, tempo é um valioso recurso. Por que então desprender esforços e gastar tempo para desenvolver um *framework* baseado em experiências restritas quando padrões desenvolvidos internacionalmente já existem?
2. Melhores práticas – Os padrões têm sido desenvolvidos e reavaliados ao longo do tempo por centenas de pessoas e organizações ao redor do mundo. A experiência acumulada em anos refletida nesses modelos é muito mais rica do que aquela obtida por uma ou poucas organizações que buscam desenvolver modelos próprios.
3. Conhecimento compartilhado – Ao seguir padrões, pessoas podem compartilhar idéias entre organizações, grupos de discussão, fóruns, revistas, livros, etc. Defensores de abordagens *ad hoc* não têm essa condição.
4. Possibilidade de serem auditadas – Sem padrões, os controles se tornam muito mais difíceis de serem avaliados, especialmente por auditores externos.

Atualmente, existe uma verdadeira profusão dessas práticas, com focos por vezes diferentes, mas proveitosos na orientação da implementação da GSI, e por este motivo, é prudente que as organizações façam uma avaliação prévia de algumas delas, antes de tomar a decisão de escolher aquela(s) mais apropriada(s) e adaptável(veis) às suas necessidades. A seguir serão apresentadas duas dessas práticas, escolhidas, principalmente, pelo fato de serem cada vez mais conhecidas, aceitas e adotadas internacionalmente.

3.2 CobiT

3.2.1 Visão geral

Desenvolvido e promovido pelo *IT Governance Institute* (ITGI), estabelecido em 1998 para contribuir no avanço das idéias e padrões internacionais sobre a direção e o controle da TI nas organizações, *Control Objectives for Information and related Technology* (CobiT), cuja tradução em português é "Objetivos de Controle para Informação e Tecnologias relacionadas", parte da premissa que a TI precisa entregar a informação que a organização necessita para alcançar seus objetivos (ITGI, 2006).

Segundo o ITGI (2007), a missão do CobiT é a de pesquisar, desenvolver, publicar e promover um atualizado e internacionalmente aceito *framework* para o controle corporativo de TI, que seja adotado pelas empresas e utilizado no dia-a-dia por gerentes de negócios e auditores de TI. O CobiT foi elaborado para servir de ferramenta para a governança da TI, e, portanto, não é exclusividade da Segurança da Informação – apenas faz referências a esta, dentre outras questões (SOLMS, 2005).

O CobiT provê boas práticas para a gestão de questões importantes da tecnologia da informação, através de um *framework* composto de domínios e processos, e apresenta, ainda, atividades numa estrutura lógica e gerenciável. Ele representa o consenso de *experts* e suas práticas estão focadas mais em controles do que em execução. Essas práticas irão ajudar a otimizar os investimentos de TI, a garantir a entrega dos serviços e a prover medidas que poderão ser utilizadas para analisar e julgar o porquê de certas coisas terem dado errado (ITGI, 2007).

3.2.2 Características do *framework*

Em resposta a algumas necessidades levantadas em tópicos anteriores, o *framework* CobiT foi criado com as seguintes principais características (ITGI, 2007):

1) Focado no negócio – O *framework* CobiT foi desenvolvido não somente para ser usado por prestadores de serviços de TI, usuários e auditores, mas também, e principalmente, para servir como um guia para a gestão e para os "donos" dos processos de negócio.

Ele é baseado no princípio de que: "para fornecer a informação necessária para alcançar seus objetivos, a organização precisa investir, gerenciar e controlar os recursos de TI, que são utilizados em um conjunto estruturado de processos que fornecem os serviços que entregam a informação requerida", como pode ser observado na Figura 3.1.

Figura 3.1 – Princípio básico do framework CobiT.
Fonte: ITGI (2007).

Para atender aos objetivos de negócio, considerados pelo CobiT como requerimentos de negócio para a informação, a informação precisa estar em conformidade com certos critérios de controle, quais sejam: eficácia, eficiência, disponibilidade, integridade, confidencialidade, confiabilidade e conformidade.

Enquanto os critérios de controle para informação fornecem um método genérico para a definição dos requerimentos de negócio, a definição de um conjunto genérico de objetivos de negócio e de TI fornece uma base mais refinada e relacionada aos negócios para o estabelecimento dos requerimentos de negócio e o desenvolvimento de indicadores para monitorar a *performance* com relação a esses objetivos. Toda organização usa a TI para permitir iniciativas de negócio, e essas podem ser representadas como objetivos de TI.

Se a TI pretende entregar serviços com sucesso para suportar a estratégia da organização, então deverá haver claro entendimento dos requerimentos de negócio (usuário/cliente) e claro entendimento do que ela precisa entregar e como (fornecedor).

A Figura 3.2 mostra como a estratégia da organização deve ser traduzida pelos negócios em objetivos relacionados às iniciativas possibilitadas pela TI (os objetivos de negócio para TI). Esses objetivos devem conduzir a uma definição clara dos próprios objetivos de TI que, por sua vez, definirão quais devem ser seus recursos e suas capacidades (arquitetura de TI) necessários para executar com sucesso sua parte dentro estratégia organizacional.

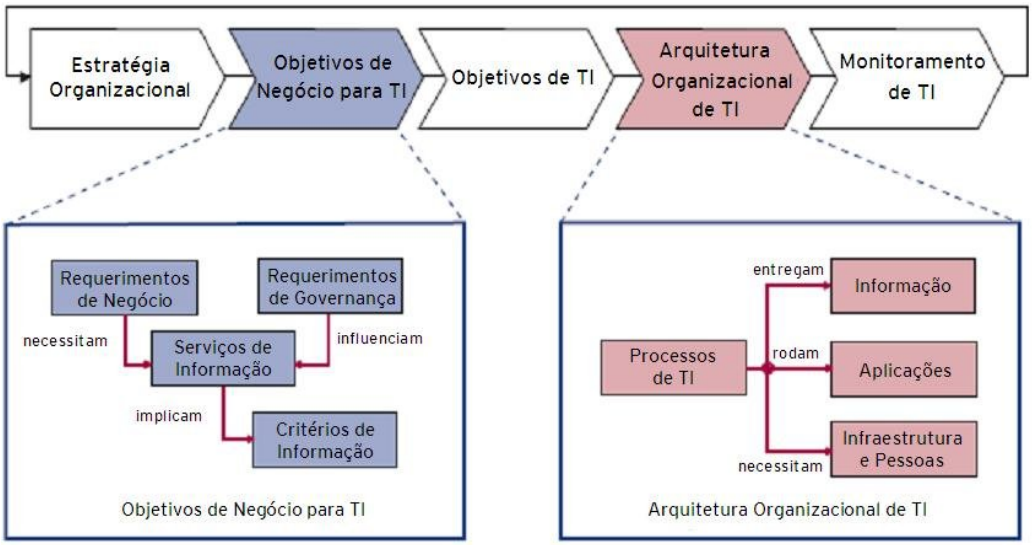


Figura 3.2 – Definindo os objetivos e a arquitetura de TI.
Fonte: ITGI (2007).

Uma vez definidos objetivos alinhados, eles precisam ser monitorados para garantir que as entregas reais atendem às expectativas, o que pode ser feito através do uso de indicadores derivados desses objetivos. Para os usuários/clientes entenderem os objetivos de TI, todos os seus indicadores devem ser expressos em termos significativos de negócio. Em conjunto com uma hierarquia de objetivos alinhados, isso irá garantir uma boa probabilidade de que a TI irá suportar os objetivos da organização.

Os objetivos de TI são atendidos através de um conjunto bem definido de processos que utiliza as habilidades das pessoas e infraestrutura tecnológica para executar aplicações automatizadas e processar informações de negócio. Esses recursos, juntamente com os processos, constituem a arquitetura da organização para a TI, como mostrado na Figura 3.2. Para atender aos requerimentos de negócio para a TI, a organização precisa investir nos recursos necessários para gerar a capacidade técnica adequada (por exemplo, sistemas ERP) para suportar as capacidades de negócio (por exemplo, implementar uma cadeia de suprimentos), resultando em resultados desejados (por exemplo, aumento das vendas).

Os recursos de TI identificados pelo CobiT são os seguintes:

- Aplicações – sistemas de usuários automatizados e os procedimentos manuais que processam as informações.
- Informação – dados de entrada, transformados, ou de saída, em qualquer uma de suas formas, processados nos sistemas de informação e utilizados pelos negócios.

- Infraestrutura – tecnologia e instalações (por exemplo, *hardware*, sistemas operacionais, sistemas de gerenciamento de banco de dados, redes, *multimedia* e o ambiente físico que os abrigam) que permitem a execução das aplicações.
- Pessoas – pessoal necessário para planejar, organizar, adquirir, implementar, entregar, dar suporte, monitorar e avaliar os sistemas de informação e serviços. Pode ser interno, terceirizado ou contratado temporariamente conforme seja necessário.

2) Orientado para processos

O foco no processo do CobiT é ilustrado por um modelo de processo que subdivide a TI em 34 processos, alinhados com funções de planejamento, implementação, execução e monitoramento, proporcionando uma visão de início a fim da TI, não necessariamente aplicáveis em todas as organizações, que pertencem a quatro domínios (ITGI, 2007):

1) **Planejamento e Organização (PO)** – Este domínio aborda estratégias e táticas e se preocupa em identificar a forma como a TI irá melhor contribuir para o alcance dos objetivos de negócio. A implantação de uma visão estratégica precisa ser planejada, comunicada e gerenciada segundo diferentes perspectivas. Para isto, organização e infraestrutura tecnológica devem se fazer presentes. Este domínio, tipicamente, lida com questões como:

- A TI está alinhada à estratégia do negócio?
- A organização está otimizando o uso de seus recursos?
- Todos na organização entendem os objetivos de TI?
- Os riscos de TI são conhecidos e estão sendo mapeados?
- A qualidade dos sistemas de TI é apropriada para a necessidade do negócio?

2) **Aquisição e Implementação (AI)** – Para implementar a estratégia de TI, soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, bem como implementadas e integradas aos processos de negócio. Além disso, as questões relativas às mudanças e à manutenção dos sistemas existentes são cobertas por este domínio para se garantir que as soluções continuem a atender aos objetivos de negócio. Este domínio, constantemente, lida com questões como:

- Os novos projetos irão fornecer soluções que atendam as necessidades do negócio?

- Os novos projetos serão finalizados nos prazos corretos e dentro do orçamento?
- Os novos sistemas irão funcionar adequadamente quando implementados?
- As mudanças ocorrerão sem afetar a normalidade das operações de negócio atuais?

3) **Entrega e Suporte (DS)** – Este domínio se preocupa com as entregas efetivamente feitas dos serviços requisitados, abrangendo entrega de serviço, gerenciamento da segurança e da continuidade, suporte a usuários, e gerenciamento de dados e de instalações operacionais. Este domínio costuma lidar com questões como:

- Os serviços de TI estão sendo entregues de acordo com as prioridades de negócio?
- Os custos de TI estão otimizados?
- Os usuários são capazes de utilizar os sistemas de TI com produtividade e de forma segura?
- A confidencialidade, a integridade e a disponibilidade da informação estão sendo bem gerenciadas?

4) **Monitoramento e Avaliação (ME)** – Todos os processos de TI precisam ser regularmente avaliados ao longo do tempo com relação à qualidade de seus requisitos de controle e a conformidade destes. Este domínio, tipicamente, trata de questões como:

- A *performance* da TI é medida para detectar problemas antes que seja tarde demais?
- A gestão garante que os controles internos são eficazes e eficientes?
- A *performance* de TI está realmente conectada às metas do negócio?
- Existem controles adequados de segurança da informação para a confidencialidade, integridade e disponibilidade da informação?

Para cada processo, um objetivo de controle de alto nível é definido (ITGI, 2006):

- Identificando-se quais critérios da informação são mais importantes para tal processo
- Listando-se quais recursos serão necessários
- Fazendo-se considerações sobre o que é importante para controlar tal processo

Além disso, para cada um desses processos, é feita uma ligação entre os objetivos de negócio e os de TI. Também são fornecidas informações sobre como os objetivos podem ser alcançados, quais são as atividades-chave e principais entregas, e quem é responsável por elas (ITGI, 2007).

3) Baseado em controles

O CobiT define objetivos de controle para todos os seus 34 processos.

Controles podem ser entendidos como as políticas, procedimentos, práticas e estruturas organizacionais desenhadas para prover garantia de que objetivos de negócio serão alcançados e eventos indesejáveis serão prevenidos ou detectados e corrigidos. Os objetivos de controle de TI provêem um conjunto completo de requerimentos de alto nível que devem ser considerados pela gestão para o controle eficaz de cada processo de TI. A gestão precisa, contudo, tomar algumas decisões relacionadas a esses objetivos de controle, tais como (ITGI, 2007):

- Selecionar aqueles que são aplicáveis;
- Decidir quais deles serão implementados;
- Escolher como eles serão implementados (freqüência, período, automação, etc);
- Aceitar o risco de não implementar aqueles que são aplicáveis.

A gestão operacional usa processos para organizar e gerenciar as atividades de TI. O CobiT fornece um modelo de processo genérico que representa todos os processos normalmente encontrados sob domínio das funções de TI e é compreensível para os gerentes de negócio e da operação de TI. Para alcançar uma governança eficaz, controles precisam ser implementados pelos gerentes operacionais através de um *framework* de controle bem definido para todos os processos de TI. Como os objetivos de controle de TI do CobiT estão organizados por processos de TI, seu *framework* provê *links* entre os requerimentos de governança, processos e controles de TI. Cada processo de TI do CobiT possui uma descrição e uma série de objetivos de controle, que em geral, provêem as características de um processo bem gerenciado (ITGI, 2007).

Entender os papéis e responsabilidades de cada processo é crucial para uma governança eficaz. O CobiT define uma tabela RACI para cada processo, que indica quem são as pessoas que "fazem acontecer" (*Responsible),* provêem direção e autorizam uma atividade (*Accountable),* precisam estar envolvidas e suportar o processo (*Consulted* e *Informed)* (ITGI, 2007).

4) Motivado por medidas

Toda organização precisa entender o *status* do seu próprio sistema de TI e decidir que nível de gestão e controle será estabelecido. Para tomar a decisão mais acertada, a gestão precisa perguntar a si mesmo: quão longe devemos ir e o custo justifica o benefício? (ITGI, 2007).

Conseguir uma visão objetiva do seu próprio nível de *performance* não é uma tarefa fácil para as organizações, pois nem sempre está claro o que deve ser medido e como. Elas precisam medir o que conseguiram estabelecer e onde melhorias são requeridas, implementando ainda ferramentas que sejam capazes de monitorá-las (ITGI, 2007).

O CobiT lida com essas questões ao prover:

- Modelos de maturidade que permitem a identificação de melhorias de capacidade necessárias através de *benchmarking*;
- Objetivos e métricas de *performance* para os processos de TI, demonstrando como os processos atendem aos objetivos de negócio e de TI e como eles são usados para medir *performance* interna;
- Metas para as atividades que garantam uma *perfomance* eficaz dos processos.

A avaliação da capacidade do processo baseada nos modelos de maturidade CobiT é uma parte crucial na implementação da governança de TI. Depois de identificar os processos e controles críticos de TI, a modelagem da maturidade torna os *gaps* em capacidade identificáveis e demonstráveis à gestão. Planos de ação podem, então, ser desenvolvidos para levar esses processos aos níveis de capacidade desejados (ITGI, 2007).

O modelo do CMM (*Capability Maturity Model for Software*) estabelece os seguintes níveis de maturidade (PAULK et al, 1993 *apud* BERNARDES e MOREIRA, 2005):

- Nível 0 - Inexistente: Significa que o processo de gerenciamento não foi implementado;
- Nível 1 - Inicial: O processo é realizado sem organização, de modo não planejado;
- Nível 2 - Repetível: O processo é repetido de modo intuitivo, isto é, depende mais das pessoas do que de um método estabelecido;
- Nível 3 - Definido: O processo é realizado, documentado e comunicado na organização;
- Nível 4 - Gerenciado: Existem indicadores de desempenho das atividades, o processo é monitorado e constantemente avaliado;

- Nível 5 - Otimizado: As melhores práticas de mercado e automação são utilizadas para a melhoria contínua dos processos.

Com o uso dos modelos de maturidade em cada um dos processos do CobiT, a gestão poderá identificar:

- *Performance* real da organização – Onde a organização está hoje
- O estado atual da indústria – A comparação
- A meta da organização para melhorias – Aonde a organização quer chegar
- O caminho de crescimento necessário entre "onde ela está" e "onde ela quer estar"

O uso dos modelos de maturidade do *framework* CobiT para a avaliação do nível de maturidade dos processos ajuda a área de TI a identificar seu grau atual e em como evoluir para melhorar os processos da organização, permitindo a evolução desses (BERNARDES e MOREIRA, 2005).

A figura 3.3 mostra os principais elementos do *framework* CobiT e o relacionamento existente entre eles, ilustrando de forma sintética sua estrutura processual.

3.2.3 Questões de Segurança da Informação e GSI

Diante do exposto, fica claro que o CobiT não é um *framework* específico para tratar das questões de segurança da informação. Entretanto, ele lida com questões preocupantes sobre a segurança da informação em mais de 20 processos, dos quais quatro estão mais diretamente relacionados com a segurança da informação, quais sejam (ITGI, 2006):

- PO6 – Comunique o direcionamento e os objetivos da gestão
- PO9 – Avalie e gerencie riscos de TI
- DS4 – Garanta a continuidade dos serviços
- DS5 – Garanta a segurança dos sistemas

Uma das vantagens de se usar o CobiT como *framework* de GSI é a de que a segurança da informação estará integrada numa estrutura maior e mais ampla de governança da TI, proporcionada pelos outros 30 processos. Mesmo quando utilizado somente para a GSI, ele ainda proporcionará a base necessária para que a organização futuramente, se assim desejar, implemente a governança de TI. O *framework* já existente para a GSI estará perfeitamente acomodado no *framework* mais amplo do CobiT (SOLMS, 2005).

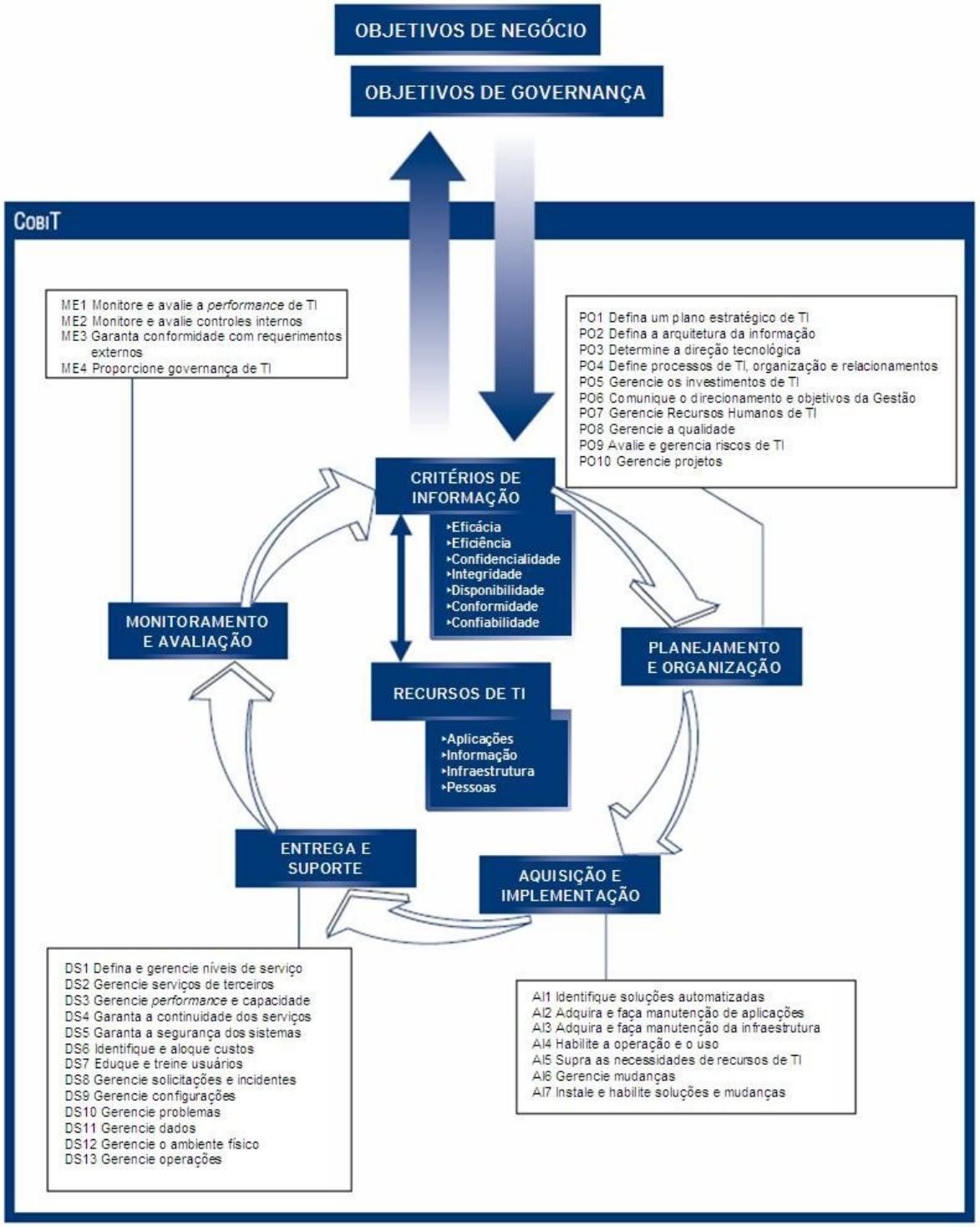


Figura 3.3 – Visão geral do framework CobiT.
Fonte: ITGI (2007).

Por outro lado, a desvantagem de se utilizar o CobiT para a GSI está no fato de que ele nem sempre é muito detalhado em termos de "como" se deve fazer certas coisas. Os objetivos de controle são mais focados em "o que" deve ser feito. Em muitos casos, uma orientação mais detalhada de "como" fazer as coisas será necessária (SOLMS, 2005).

3.3 ISO 27002:2005

3.3.1 Visão Geral

Para atender às necessidades das organizações, agências governamentais e instituições internacionais em relação ao estabelecimento de padrões e normas que refletisse as melhores práticas de mercado relacionadas à segurança dos sistemas e informações, o *British Standards Institute* (BSI) criou uma das primeiras normas sobre o assunto. Denominada BS 7799 - *Code of Practice for Information Security Management*, ela foi oficialmente apresentada em primeiro de dezembro de 2000, após um trabalho intenso de consulta pública e internacionalização. A BS 7799 foi aceita como padrão internacional pelos países membros da *International Organization for Standardization* (ISO), sendo então denominada ISO/IEC 17799:2000 (ISO, 2000 *apud* BERNARDES e MOREIRA, 2005).

A norma ISO/IEC 17799, Código de Prática para a Gestão da Segurança da Informação, tem a intenção de servir como ponto de referência para identificar a gama de controles necessários para grande parte das situações em que sistemas de informação são utilizados na indústria e comércio. Ela se adequa a organizações de qualquer tamanho e trata a informação como um ativo que, como os outros principais ativos de negócio, tem valor para a organização e, consequentemente, precisa ser protegido adequadamente (ITGI, 2006).

Em 15 de junho de 2005, foi publicada a segunda edição tecnicamente revisada da norma. A partir de 2007, a norma ISO/IEC 17799 passou a ser denominada ISO/IEC 27002, mudança essa realizada para que ela passasse a fazer parte de uma nova família de normas relacionadas aos temas de requerimentos de segurança para gerenciamento de sistemas, gerenciamento de riscos, indicadores e suas medições, e guias de implementação (ISO/IEC 27002:2005).

A norma ISO 27002 estabelece diretrizes e princípios gerais para o planejamento, implementação, manutenção e melhoria da gestão da segurança da informação nas organizações. Os objetivos contidos nessa norma fornecem orientações gerais para o estabelecimento das metas mais comumente aceitas de gerenciamento da segurança da informação (ISO/IEC 27002:2005).

A norma, portanto, refere-se exclusivamente às questões de segurança da informação. Um de seus pontos fortes na implementação da GSI é o maior nível de detalhe, quando comparado ao CobiT, provendo maior orientação sobre "como" as coisas precisam ser feitas. Ela fornece, por exemplo, orientações sobre o que a política de segurança da informação deve ter em termos de estrutura e conteúdo. Por conta de uma abordagem mais detalhada e técnica, a norma é usualmente escolhida como *framework* pelos gerentes de TI e de Segurança da Informação. Seu ponto fraco reside no fato de que ela é de certa forma independente, não integrada num *framework* mais amplo de governança de TI (SOLMS, 2005).

3.3.2 Estrutura da norma

A norma ISO 27002 contem 11 cláusulas de controle, as quais, conjuntamente, possuem 38 categorias principais de segurança, e uma cláusula introdutória sobre avaliações de riscos e tratamento. As cláusulas de controle, bem como suas principais categorias de segurança, são as seguintes:

1. Política de Segurança
    a. Política de Segurança da Informação
2. Organização da Segurança da Informação
    a. Organização Interna
    b. Organização Externa
3. Gestão dos Ativos
    a. Responsabilidade sobre Ativos
    b. Classificação da Informação
4. Questões de Segurança relacionadas aos Recursos Humanos
    a. Antes de empregar
    b. Durante o emprego
    c. Término ou mudança da relação empregatícia
5. Segurança Física e Ambiental
    a. Áreas Seguras
    b. Segurança dos Equipamentos
6. Gestão da Comunicação e Operação
    a. Procedimentos Operacionais e Responsabilidades
    b. Gestão da Entrega de Serviços por Terceiros

   c. Planejamento e Aceitação de Sistemas
   d. Proteção contra Códigos Maliciosos e Móveis
   e. Cópia de Segurança (*Back-Up*)
   f. Gestão da Segurança em Redes
   g. Manuseio de Mídias
   h. Trocas de Informações
   i. Serviços de Comércio Eletrônico
   j. Monitoramento
7. Controle de Acesso
   a. Requerimentos de Negócio para Controle de Acesso
   b. Gestão do Acesso a Usuário
   c. Responsabilidades do Usuário
   d. Controle de Acesso à Rede
   e. Controle de Acesso aos Sistemas Operacionais
   f. Controle de Acesso às Aplicações e Informações
   g. Computação Móvel e Trabalho à Distância
8. Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação
   a. Requerimentos de Segurança para Sistemas de Informação
   b. Processamento Correto de Dados em Aplicações
   c. Controles Criptográficos
   d. Segurança dos Arquivos de Sistema
   e. Segurança nos Processos de Desenvolvimento e Suporte
   f. Gestão da Vulnerabilidade Técnica
9. Gestão dos Incidentes de Segurança da Informação
   a. Comunicação dos Eventos e Fraquezas da Segurança da Informação
   b. Gestão dos Incidentes e Melhorias da Segurança da Informação
10. Gestão da Continuidade de Negócios
   a. Aspectos da Segurança da Informação na Gestão da Continuidade de Negócios
11. Conformidade
   a. Conformidade com Requerimentos Legais
   b. Conformidade com Políticas de Segurança e Padrões e Conformidade Técnica

c. Considerações sobre Auditoria de Sistemas de Informação

A ordem das cláusulas na norma não tem relação com sua importância. Dependendo, das circunstâncias, algumas cláusulas podem ser mais importantes que outras, e por isso, ao aplicar a norma, cada organização deve identificar aquelas que são aplicáveis, quão importante elas são e como se aplicam a cada um dos processos de negócio (ISO/IEC 27002:2005).

Cada categoria principal, relacionada acima, possui um objetivo de controle, que declara o que se pretender alcançar, e um ou mais controles que podem ser aplicados para alcançar tal objetivo. Por sua vez, cada controle possui uma estrutura que consta de (ISO/IEC 27002:2005):

- Definição – estabelece uma declaração específica do controle que satisfaz o objetivo de controle;
- Orientação para implementação – fornece informações mais detalhadas para auxiliar na implementação do controle e atendimento ao objetivo de controle. Algumas orientações talvez não sejam adequadas em todas as situações;
- Outras informações – fornecem aspectos adicionais que precisam ser considerados, como por exemplo, obrigações legais e referências a outros padrões.

3.3.3 Gestão dos Riscos de Segurança

Um dos pontos de destaque da norma refere-se à forma como as organizações devem gerenciar seus riscos para o adequado gerenciamento da segurança da informação, ou seja, como elas avaliam e tratam de seus riscos. Segundo a norma, as avaliações de riscos devem identificar, quantificar e priorizar riscos levando-se em consideração níveis de aceitação de riscos estabelecidos e objetivos relevantes das organizações. Os resultados das avaliações devem orientar e determinar ações apropriadas e prioridades para a gestão dos riscos de segurança da informação e para a implementação dos controles selecionados para mitigar tais riscos. Vale ressaltar que o processo de avaliação de riscos e de seleção de controles talvez precise ser realizado várias vezes para cobrir partes diferentes da organização ou sistemas de informação individuais (ISO/IEC 27002:2005).

A avaliação dos riscos deve incluir uma abordagem sistemática de estimação da magnitude dos riscos e um processo de comparação entre riscos estimados e certos critérios que permitam estabelecer sua significância (ISO/IEC 27002:2005).

Avaliações de riscos devem também ser realizadas periodicamente para atender às mudanças nos requerimentos de segurança e nas situações de riscos, ou seja, mudanças relativas a ativos,

ameaças, vulnerabilidades, impactos e aquelas consideradas significativas. Essas avaliações de riscos devem ser feitas de forma metódica, capaz de produzir resultados comparáveis e reprodutíveis (ISO/IEC 27002:2005).

A avaliação dos riscos de segurança da informação deve ter um escopo bem definido para que seja eficaz e deve possuir relações com avaliações de riscos de outras áreas, se apropriado. O escopo da avaliação pode ser definido para toda a organização, para partes dela, para um determinado sistema de informação, para componentes específicos de sistema, ou serviços para os quais ela seja prática, realística e útil (ISO/IEC 27002:2005).

Antes de partir para o tratamento dos riscos, a organização deve decidir critérios para determinar quando os riscos podem ser aceitáveis ou não. Riscos podem ser aceitáveis se, por exemplo, foi avaliado que o risco é baixo ou seu tratamento não possui uma boa relação custo-benefício. Tais decisões devem ser registradas (ISO/IEC 27002:2005).

Para cada um dos riscos identificados na avaliação de riscos, deve ser tomada uma decisão sobre seu tratamento, cujas opções básicas são (ISO/IEC 27002:2005):

1. Aplicar controles apropriados para reduzir riscos;
2. Aceitar, conscientemente e objetivamente, os riscos, de acordo com as políticas da organização e com os critérios para aceitação de riscos;
3. Evitar riscos, não dando margem para que suas causas se materializem;
4. Transferir os riscos para parceiros comerciais, como seguradoras ou fornecedores.

Quando da decisão de aplicação de controles apropriados para redução de riscos, estes devem ser selecionados e implementados para atender aos requerimentos identificados na sua avaliação. Esses controles devem assegurar também que os riscos são reduzidos para um nível aceitável levando-se em consideração (ISO/IEC 27002:2005):

- Requerimentos e restrições das legislações e regulamentações nacionais e internacionais;
- Objetivos organizacionais;
- Requerimentos e restrições operacionais;
- Custo-benefício da implementação e operacionalização desses controles;
- A necessidade de balancear o investimento em implementação e operacionalização dos controles e o possível dano resultante de falhas na segurança.

A norma ISO 27002 ressalta que é necessário reconhecer que alguns controles não são aplicáveis para todo sistema de informação ou ambiente, e que podem não ser praticáveis para todas as organizações (ISO/IEC 27002:2005).

Controles de Segurança da Informação devem ser considerados na especificação dos requerimentos dos projetos e sistemas e no estágio de desenho. Falhas nesta consideração podem resultar em custos adicionais e soluções menos eficazes e, talvez, no pior caso, falta de capacidade para alcançar segurança apropriada (ISO/IEC 27002:2005).

Além disso, não se deve esquecer o fato de que nenhum conjunto de controles pode alcançar a segurança completa, e que ações gerenciais adicionais devem ser realizadas para monitorar, avaliar e melhorar a eficiência e eficácia dos controles de segurança, a fim de dar suporte aos objetivos da organização (ISO/IEC 27002:2005).

3.4 Comparação entre o *framework* CobiT e a norma ISO 27002

Apesar de não possuírem estruturas idênticas e mesma finalidade, a seguir serão feitas comparações entre ambas as práticas com relação a uma série de aspectos. Esta comparação não tem como objetivo indicar qual é a melhor prática, e sim, consolidar, de forma resumida, as diferenças ou sobreposições existentes em cada um dos aspectos a seguir:

- Com relação à taxonomia documental:

O CobiT representa uma coletânea de documentos que podem ser classificados como melhores práticas geralmente aceitas para a prática de governança de TI, controle e auditoria. Por sua vez, a ISO/IEC 27002:2005 é uma norma internacional composta pelas melhores práticas para o desenvolvimento e a manutenção de padrões de segurança e de gestão para a melhoria da confiabilidade da segurança da informação nos relacionamentos interorganizacionais. Desta forma, a natureza e a classificação dos documentos que suportam as práticas são distintas.

- Com relação aos objetivos:

O CobiT tem como missão pesquisar, desenvolver, publicar e promover um atualizado e internacionalmente aceito *framework* para o controle corporativo de TI, que seja adotado pelas empresas e utilizado no dia-a-dia por gerentes de negócios e auditores de TI. O objetivo da ISO 27002 é de prover diretrizes e princípios gerais que sejam adotados pelos responsáveis pela segurança da informação, quando do planejamento, implementação, manutenção e melhoria da gestão da segurança da informação nas organizações. Seus objetivos, portanto, assemelham-se, na

medida em que buscam definir princípios e orientações que sejam amplamente adotados no estabelecimento de controles para processos de TI.

- Com relação às motivações de negócio para sua implementação:

O CobiT é comumente recomendado e utilizado quando da aparição de um ou mais dos seguintes casos de negócio:

- Existe a necessidade de se implementar a governança de TI;
- Os serviços entregues por TI precisam ser alinhados com os objetivos de negócio;
- Processos de TI precisam ser padronizados/automatizados;
- Um *framework* para os processos gerais de TI se faz necessário;
- Processos de TI precisam ser unificados;
- Uma abordagem de auditoria estruturada precisa ser definida;
- São desejadas iniciativas de controle de custos para TI;
- Conformidade com requerimentos externos (reguladores, parceiros, clientes, etc) é uma preocupação;
- Mudanças importantes na organização, nos objetivos e processos de negócio afetam TI;

Os fatores motivadores para a adoção da ISO 27002, por sua vez, estão relacionados com necessidades de:

- Definição de um sistema de gerenciamento da segurança da informação, utilizando-se para tanto melhores práticas de gerenciamento da segurança baseadas em uma abordagem sistemática;
- Identificação dos ativos críticos de informação através do gerenciamento dos riscos de negócio;
- Intensificação do conhecimento e importância das questões relacionadas à segurança em nível gerencial;
- Definição de responsabilidades e estruturas organizacionais para a segurança da informação;
- Certificação para o sistema de gerenciamento da segurança da informação;
- Quebrar barreiras comerciais e firmar relacionamentos contratuais que prevêem requisitos e práticas contempladas na norma;

Diante do exposto, percebe-se que os fatores motivadores para a adoção do CobiT surgem das necessidades de melhorar a *performance* de TI, a fim de transformá-la em um facilitador para o alcance dos objetivos de negócio, diferentemente daqueles da norma ISO 27002, que surgem das necessidades de melhorar a gestão da segurança da informação, a fim de suportar a TI e a organização no cumprimento de seus objetivos.

- Com relação ao público-alvo:

Segundo o ITGI (2006), todo tipo de organização, seja pública ou privada, e profissionais de auditoria externa e de consultoria formam o público-alvo do CobiT. Ainda com relação a este *framework*, dentro das organizações, três níveis são atendidos: o de gestão, o de usuários e profissionais de TI e o de auditoria. Por outro lado, a norma ISO 27002 tem como alvo os profissionais com a responsabilidade de iniciar, implementar e manter a segurança da informação nas organizações. Com relação a este aspecto, pode-se dizer que as práticas são complementares, já que as atividades necessárias para a adoção de cada uma delas terão pertinência heterogênea para os cargos responsáveis pela governança da tecnologia da informação e pela GSI, como poderá ser constatado na Tabela 3.1.

Tabela 3.1 – Pertinência (P-Primária ou S-Secundária) das atividades desenvolvidas pelo CobiT e pela ISO 27002 com relação ao público-alvo.

Pertinência (Primária ou Secundária) das atividades em relação ao público-alvo											
Atividades/ Público-Alvo	Chief Executive Officer (CEO)	Chief Financial Officer (CFO)	Diretores	Chief Information Officer (CIO)	Dono do Processo de Negócio	Supervisor de Operações	Responsável pela Arquitetura	Supervisor de Desenvolvimento	Supervisor de Administração de TI	*Project Management Office* (PMO)	*Compliance*, Auditoria, Riscos e Segurança
CobiT	S	S	P	P	P	S	S	S	S	S	P
ISO/IEC 27002	S	-	S	P	S	S	P	P	P	-	P

Fonte: ITGI (2006).

- Com relação às oportunidades de certificação:

As oportunidades de certificação do CobiT são apenas para indivíduos e não para organizações. Por outro lado, a ISO 27002 é uma norma que concede certificação para aquelas organizações auditadas por entidades credenciadas que comprovaram possuir pelo menos o grau mínimo de conformidade exigido com ela. Dessa forma, há divergência no foco dado por cada prática para as questões de certificação.

- Sobreposição dos objetivos de controle:

O ITGI investigou cada objetivo e/ou sub-objetivo da norma e os mapeou nos objetivos de controle do CobiT, quando existentes, estabelecendo relações entre todos os seus pontos em comum. Pode-se dizer, portanto, que há relativa equivalência entre os objetivos de controle sobre segurança da informação de ambas as práticas. A Tabela 3.2 mostra o resultado do mapeamento de alto nível da ISO 27002 no CobiT (ITGI, 2006).

Tabela 3.2 – Mapeamento de Alto Nível da ISO/IEC 27002:2005 no CobiT.

Mapeamento de Alto nível da ISO/IEC 27002:2005 no CobiT													
Processos e Domínios do CobiT	1	2	3	4	5	6	7	8	9	10	11	12	13
Planejamento e Organização (PO)	-	o	o	+	-	+	+	-	+	-			
Aquisição e Implementação (AI)	o	o	o	-	-	o	o						
Entrega e Suporte (DS)	-	o	-	+	+	-	-	o	o	-	+	+	o
Monitoramento e Avaliação (ME)	-	+	+	-									

(+) Mapeamento significativo (mais de 30 requerimentos foram mapeados em um processo do CobiT);

(o) Mapeamento pouco significativo (entre 15 e 29 requerimentos de informação mapeados);

(-) Foco não relacionado (menos de 15 requerimentos foram mapeados);

(\) Processo CobiT inexistente;

Fonte: ITGI (2006).

- Abrangência e nível de detalhe:

O CobiT abrange um amplo espectro de deveres na gestão da TI, não se limitando às questões de segurança da informação, como faz a norma ISO 27002. Apesar de o primeiro não contemplar detalhes técnicos, as tarefas e atividades estabelecidas por ele para o alcance dos objetivos de controle são auto-explicativas (ITGI, 2006).

Diversos exemplos que ilustram bem o que acaba de ser dito podem ser encontrados no mapeamento detalhado entre objetivos de controle do CobiT e da ISO 27002, elaborado pelo *IT Governance Institute* em trabalho intitulado *Mapping of ISO/IEC 17799:2005 with CobiT 4.0* (ITGI, 2006).

De acordo com tal mapeamento é mostrado, por exemplo, que sob o objetivo de controle DS5.4 do CobiT (Gestão das Contas de Usuário) foram mapeados 15 controles da norma ISO 27002. Por um lado, o objetivo de controle do CobiT faz considerações sobre o "que" precisa ser feito, quais sejam:

a) Solicitações, definições, criações, suspensões, modificações e fechamento de contas e/ou privilégios de usuário devem ser conduzidos conforme procedimentos sobre a gestão de contas dos usuários;
b) Um procedimento de aprovação para o estabelecimento de acessos privilegiados deve existir;
c) Tais procedimentos devem ser aplicados a todos os usuários, incluindo administradores (usuários privilegiados) e usuários externos e internos, em casos normais e de emergência;
d) Contratos devem estabelecer os direitos e deveres relacionados ao acesso dos sistemas da organização para cada tipo de usuário;
e) Revisões periódicas devem ser realizadas sobre todas as contas e privilégios.

Por outro lado, cada um dos 15 controles da ISO 27002, listados abaixo, buscará alcançar o objetivo de controle correspondente através de uma orientação mais detalhada, indicando "como" ele deve ser estabelecido.

6.1.5 Acordos de confidencialidade
6.2.1 Identificação de riscos relacionados a terceiros
6.2.2 Conduzindo a segurança quando do contato com clientes
8.1.1 Papéis e responsabilidades
8.3.1 Responsabilidades ao término ou mudança do vínculo empregatício
8.3.3 Remoção de direitos de acesso
10.1.3 Segregação de funções
11.1.1 Política de controle de acesso
11.2.1 Registro de usuários
11.2.2 Gestão dos privilégios
11.2.4 Revisão dos direitos de acesso dos usuários
11.3.1 Uso de senhas
11.5.1 Procedimentos de *logon* seguro
11.5.3 Sistema de gestão de senhas
11.6.1 Restrição ao acesso de informação

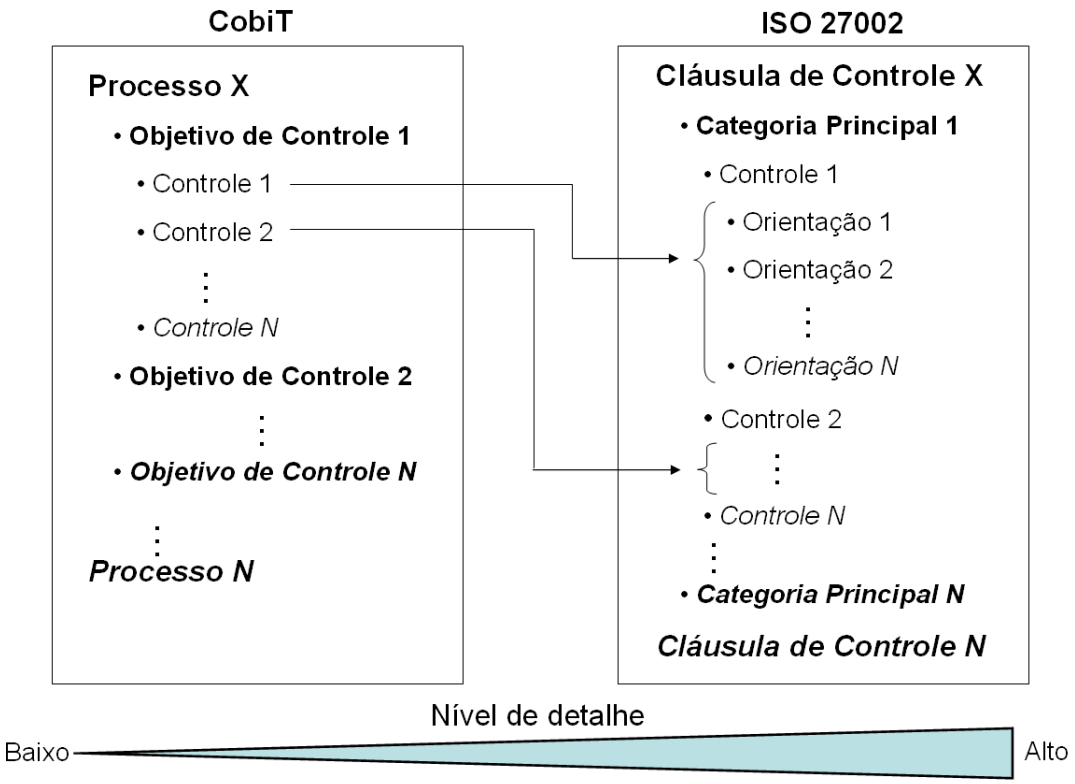
A título de exemplo, foram relacionadas abaixo apenas as orientações de implementação para o controle 11.2.4 Revisão dos direitos de acesso dos usuários. Este controle está diretamente relacionado ao controle estabelecido pelo item e) das considerações feitas pelo objetivo de controle DS5.4 do CobiT.

a) Direitos de acesso dos usuários devem ser revisados em intervalos regulares, por exemplo, de 6 em 6 meses, e depois de qualquer mudança decorrente de promoção ou término da relação empregatícia;
b) Direitos de acesso do usuário devem ser revisados e reconsiderados quando da realocação interna deste funcionário;
c) Autorizações para direitos de acesso privilegiado devem ser revisados em intervalos mais freqüentes, por exemplo, de 3 em 3 meses;
d) Alocações de privilégio devem ser verificadas em intervalos regulares para garantir que privilégios não autorizados não foram obtidos;
e) Mudanças em contas privilegiadas devem ser registradas para revisão periódica.

De forma semelhante, poderá ser constatado que os demais 14 controles da ISO 27002 provêem mais riqueza de detalhe no alcance dos objetivos de controle.

A figura 3.4 ilustra, de forma genérica, o que acaba de ser exposto através do exemplo. Nesta figura, as estruturas de cada prática foram colocadas lado a lado e o relacionamento existente, na maioria das vezes, entre os controles sobre segurança da informação estabelecidos no *framework* CobiT e as orientações dadas sobres os controles da ISO 27002 foi evidenciado. A figura também indica um nível de detalhe mais baixo para os controles *do framework* CobiT em comparação com o nível de detalhe dos controles da ISO 27002.

A partir desta análise, pode-se dizer que o *framework* do CobiT é classificado como sendo de relativo alto nível, buscando ser genericamente completo e não tão específico. Em contrapartida, a norma ISO 27002 estabelece orientações mais aprofundadas e técnicas para o alcance dos objetivos de controle propostos, sendo assim classificada como de relativo baixo nível.



3.5 Proposta de uma alternativa de uso do CobiT e da ISO 27002

Ao analisar a literatura, pode-se encontrar notável convergência existente entre os documentos que recomendam práticas relacionadas à segurança da informação. Existe amplo consenso entre os *experts* sobre quais as medidas e ações que devem ser tomadas pelas organizações. Entretanto, nenhum documento, de forma única, fornece o *framework* necessário para a segurança da informação. Os existentes atualmente são ou muito detalhados ou não tão práticos na sua abordagem *top-down* para as organizações (BSA, 2003).

Como mencionado anteriormente, a vantagem de se utilizar o *framework* do CobiT é que este posiciona a GSI dentro de um *framework* mais amplo de governança da TI, o que proporciona uma plataforma (arquitetura/estrutura) mais ampla para a governança de TI. Sua desvantagem, porém, reside no fato de que seu *framework* sobre a GSI provê boas orientações sobre "o que" deve ser feito, e não, "como" se deve fazer (SOLMS, 2005).

Por outro lado, a norma ISO 27002 é um padrão reconhecido internacionalmente e utilizado por diversas indústrias para definir eficácia na segurança da informação. Ela serve como referência para as pessoas e processos nos níveis operacionais e táticos e para a tecnologia nesses

mesmos níveis, além do estratégico. A norma é extremamente detalhada no nível operacional, ao mesmo tempo em que é vaga com respeito às responsabilidades da alta administração (BSA, 2003).

Desta forma, sua maior vantagem reside neste detalhamento técnico, provendo orientações mais diretas sobre "como" as coisas devem ser feitas. Sua desvantagem é que ela é independente e não provê uma plataforma mais ampla, como o faz o *framework* do CobiT (SOLMS, 2005).

Este trabalho propõe, portanto, o uso combinado de ambas as práticas, aproveitando as potencialidades isoladas de cada uma delas de maneira conjunta, como forma de se implementar uma GSI eficaz. Segundo Solms (2005), a sinergia proporcionada pela combinação desses *frameworks* pode ser substancial, já que, de certa forma, eles se complementam naturalmente.

Partindo dessa premissa, o CobiT deve ser usado como um *framework* de referência de alto nível, onde a GSI está bem posicionada e o "que" fazer está bem definido, enquanto que a norma ISO 27002 deve ser usada como diretriz de baixo nível específica para a Segurança da Informação, onde o "como" está mais detalhado (SOLMS, 2005). Desta forma, sob o ponto de vista processual, o nível estratégico será definido mais pelo CobiT, enquanto que o operacional pela ISO 27002.

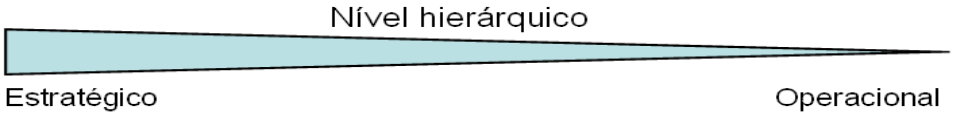
Por sua vez, sob o ponto de vista hierárquico, analisando-se os públicos-alvo de ambas as práticas e tomando por base o que está estabelecido na Tabela 3.1, pode-se supor o quão pertinente as atividades desenvolvidas pelo seu uso combinado serão para os colaboradores que compõem a GSI. O resultado desta suposição é mostrado na Tabela 3.3 e foi obtido através de uma operação lógica entre as pertinências das atividades de cada prática para cada cargo, a qual fez uso das seguintes premissas:

- Se a pertinência das atividades de uma das práticas for Secundária e a pertinência das atividades da outra prática for Secundária ou não existir, então a pertinência das atividades pelo seu uso combinado será Secundária para aquele cargo.
- Se a pertinência das atividades de uma das práticas for Primária, então a pertinência das atividades pelo seu uso combinado será Primária para aquele cargo.

Através desta tabela, pode ser observado que o uso combinado de ambas as práticas tornará as questões de segurança da informação mais presentes e disseminadas entre os níveis operacionais, táticos e estratégicos, precisamente, onde, no contexto atual, elas se fazem necessárias.

Tabela 3.3 – Pertinência (P-Primária ou S-Secundária) das atividades desenvolvidas pelo uso combinado do CobiT e da ISO 27002 com relação ao público-alvo.

Pertinência (Primária ou Secundária) das atividades em relação ao público-alvo											
Atividades/ Público-Alvo	Chief Executive Officer (CEO)	Chief Financial Officer (CFO)	Diretores	Chief Information Officer (CIO)	Dono do Processo de Negócio	Supervisor de Operações	Responsável pela Arquitetura	Supervisor de Desenvolvimento	Supervisor de Administração de TI	*Project Management Office* (PMO)	*Compliance*, Auditoria, Riscos e Segurança
Uso combinado	S	S	P	P	P	S	P	P	P	S	P



Fonte: ITGI (2006) e o Autor (2009).

Uma possível estratégia a ser adotada por uma organização para a implementação combinada de ambas as práticas, proposta por este trabalho, é a de, em um primeiro momento, considerar os objetivos de controle comuns a ambas as práticas, identificar os mais adequados para as necessidades e realidade da organização e partir para sua implantação. Para tal tarefa, pode ser bastante útil consultar o resultado do mapeamento detalhado entre ambas as práticas elaborado pelo ITGI. Posteriormente, a organização deverá considerar os objetivos de controle pertencentes a ISO 27002 e ao CobiT, de cada vez, não necessariamente nesta ordem.

Essa estratégia proverá às organizações uma sistemática para a implementação da GSI, que será estabelecida de forma gradual. Essa abordagem diminuirá a complexidade deste processo, ao não se optar por implementar ambas as práticas de uma só vez, aumentando sua probabilidade de êxito. Além disso, ela permitirá uma adoção mais imediata dos objetivos de controle, teoricamente, mais relevantes com respeito à segurança da informação, já que estes estão presentes em ambas as práticas, fato este que aumenta sua importância para as organizações, e serão os primeiros a serem implementados.

Diante do exposto, espera-se que com o uso combinado de ambas as práticas, as organizações sejam capazes de implementar uma GSI mais completa e eficaz, onde a estratégia da segurança da informação esteja alinhada com a estratégia de negócios, os riscos aos recursos de informação estejam sendo gerenciados e mitigados a níveis aceitáveis e os recursos de TI (aplicações, pessoas, informação e infraestrutura) estejam sendo bem gerenciados.

4 CONSIDERAÇÕES FINAIS

4.1 Conclusão

No atual ambiente de negócios, a informação possui um papel crucial no suporte às operações de negócio das empresas. Durante cada ciclo da operação, a informação entra em contato com elementos (pessoas, processos e tecnologia) que possuem o potencial de apresentar um risco contra suas próprias características. Desta forma, surge a necessidade de se gerir adequadamente este importante recurso organizacional, cabível em parte à segurança da informação.

O papel da segurança da informação será, portanto, o de auxiliar as organizações a compartilhar suas informações de negócio de forma segura, construindo e a mantendo relacionamentos confiáveis com seus clientes, fornecedores e outros parceiros de negócio. Por sua vez, esses relacionamentos contribuem para aumentar o fluxo de caixa e a rentabilidade dos negócios (BS 7799, 1999).

A partir de uma pesquisa sobre segurança da informação realizada em âmbito global, foi mostrado que muitas organizações ainda enfrentam dificuldades para integrar completamente a segurança da informação aos seus negócios e que padrões e práticas internacionais de segurança da informação seguirão a mesma tendência de normas como as da família ISO 9000, que se tornaram um requisito para fazer certos negócios.

Para que a segurança da informação, portanto, esteja mais integrada aos negócios, ela deve deixar de ser tratada como uma questão técnica restrita ao departamento de TI e passar a ser tratada como mais uma questão de governança corporativa, de forma a receber a atenção que merece.

No processo de integração da segurança da informação aos negócios e implementação da GSI, as organizações podem fazer uso das várias práticas disponíveis para estabelecer processos e controles exaustivamente testados e já consagrados mundialmente. O presente trabalho comparou duas das práticas cada vez mais conhecidas, aceitas e adotadas internacionalmente para tal tarefa.

A comparação estabelecida mostrou e consolidou as diferenças e pontos em comum existentes entre as práticas, contribuindo para a posterior formulação de uma proposta que utiliza as potencialidades de ambas de forma combinada. Tal proposta, por um lado, recomenda o uso do CobiT para abordar as questões de nível mais alto, já que o “que” deve ser feito está bem definido. Por outro lado, foi recomendado o uso da norma ISO 27002 nas questões de nível mais

baixo, servindo de guia no estabelecimento de “como” estabelecer controles para segurança da informação.

Espera-se que o uso combinado dessas práticas proporcione uma abordagem mais completa sobre a segurança da informação no estabelecimento da GSI, contribuindo incisivamente para o alinhamento das estratégias e objetivos de negócio das organizações com as estratégias e objetivos da segurança da informação, e para a gestão dos riscos associados a segurança da informação, de forma que melhor desempenho organizacional seja alcançado.

4.2 Recomendações para trabalhos futuros

O presente trabalho buscou discutir um tema relativamente recente e não completamente difundido na literatura e entre as empresas. Sem dúvida, uma das principais dificuldades enfrentadas foi a de encontrar material bibliográfico pertinente e de procedência confiável para seu desenvolvimento.

Em trabalhos futuros, a análise e identificação das potencialidades de outras práticas e padrões relacionados à segurança da informação podem ser bastante úteis para indicar lacunas e pontos de melhoria à proposta apresentada.

Por fim, espera-se que o conhecimento aqui consolidado contribua na diminuição de escassez de material sobre um tema tão importante, ao mesmo tempo em que fomenta seu desenvolvimento.

REFERÊNCIAS BIBLIOGRÁFICAS

Almeida, A. T. e Ramos, F. S. (org). **Gestão da Informação na competitividade das Organizações**. Recife: Ed. Universitária da UFPE. 2002.

Allen, Julia; **Governing for Enterprise Security**. Carnegie Mellon University. USA, 2005.

Bernardes, M. C. ; Moreira, E. S. **Um Modelo para Inclusão da Governança da Segurança da Informação no Escopo da Governança Organizacional**. In: Simpósio Segurança em Informática, São José dos Campos. 2005.

British Standards Institution. **BS 7799: Code of practice for information security management as a base for certification**; 1999.

Business Software Alliance (BSA). **Information Security Governance: Toward a Framework for Action.** Junho, 2003. Disponível em <http://www.bsa.org/country/Research%20and%20Statistics/~/media/BD05BC8FF0F04CBD9D76460B4BED0E67.ashx> Acessado em 25 de Maio de 2009.

Corporate Governance Task Force Report (CGTFR). **Information Security Governance: A Call to Action**. April, 2004. Disponível em: <http://www.cyberpartnership.org/InfoSecGov4_04.pdf>. Acessado em 25 de Abril 2009.

Drew, Mark. **Information risk management and compliance — expect the unexpected**. **BT Technology Journal**, Vol. 25, Núm. 1. Janeiro, 2007

Drucker, Peter. **Management Challenges for the 21st Century**. Harpers Business. 1993.

Entrust. **Information Security Governance (ISG): An Essential Element of Corporate Governance**. April 2004. Disponível em <http://itresearch.forbes.com/detail/RES/1082396487_702.html>. Acessado em 25 de Abril 2009.

Ernst & Young. **Global Information Security Survey 2008**. Disponível em: <http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/$file/TSRS_Global_Information_Security_Survey_2008.pdf> Acessado em 25 de Abril de 2009.

Humphreys EJ, Moses RH, Plate EA. **Guide to BS7799 risk assessment and management**. British Standards Institution. 1998.

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). **Information technology — Security techniques — Code of practice for information security management**. ISO/IEC 27002:2005.

IT Governance Institute (ITGI). **CobiT 4.1**. 2007.

IT Governance Institute (ITGI). **Mapping of ISO/IEC 17799:2005 with CobiT 4.0**. 2006.

IT Governance Institute (ITGI). **Information Security Governance: Guidance for Boards of Directors and Executive Management**. 2ª edição. 2006.

Site da Globo.com. **Matéria jornalística*: Hackers invadem site do Pentágono e roubam projeto de avião de US$ 300 bi.*** Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1092884-6174,00.html> Acessado em 25 de Abril 2009.

Gerber, M.; Solms, R. von. **From Risk Analysis to Security Requirements**. **Computers & Security**, 20, p.577-584. 2001.

McKinsey e Institutional Investors Inc.; **McKinsey/KIOD Survey on Corporate Governance**. Janeiro, 2003. Disponível em: <www.mckinsey.com/clientservice/organizationleadership/service/corpgovernance/pdf/cg_survey.pdf> Acessado em 26 de Abril de 2009.

Revista VEJA. **"Mouse ao Alto!"**. Edição 2.113, ano 42, nº. 20, pg 88. Editora Abril. 20 de Maio de 2009.

Rezende, Denis Alcides. **Sistemas de Informações organizacionais: guia prático para projetos em cursos de administração, contabilidade e informática**. São Paulo: Atlas, 2005.

Shaun Posthumus, R. S. A framework for the governance of information security. **Computers & Security 23, p. 638-646**. Elsevier Ltd. 2004.

Solms, Basie von. Information Security governance: COBIT or ISO 17799 or both? **Computers & Security 24, p. 99 – 104.** Elsevier Ltd. 2005.

Thompson K, von Solms R. **Integrating information security into corporate culture**. Tese de mestrado. Port Elizabeth Technikon, 2003.

Spafford, George. **The Benefits of Standard IT Governance Frameworks**. Abril, 2003. Disponível em: <http://www.itsmwatch.com/itil/article.php/2195051>. Acessado em 22 de Maio de 2009.