ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO

Departamento de Engenharia de Computação e Sistemas Digitais

Uma Abordagem Correlacional dos Modelos CobiT / ITIL e da Norma ISO 17799 para o tema Segurança da Informação

Luciano de Oliveira Balbo

Monografia desenvolvida sob orientação do Professor Raymundo Vasconcelos, apresentada à Universidade de São Paulo, como parte dos requisitos para obtenção do título de Especialista em Tecnologia da Informação.

São Paulo, 2007

DEDICATÓRIA

Aos meus pais Gilson e Fátima

A minha irmã Isabela

A minha namorada Xênia

A Deus por me dar saúde.

AGRADECIMENTOS

Ao Prof. Raymundo pelos conselhos e pelo comprometimento na ajuda da criação deste trabalho.

Resumo

A dependência atual das organizações da sua infra-estrutura de TI (Tecnologia da Informação), associado às oportunidades, benefícios e riscos inerentes a essa área, exige que essas organizações passem a considerar a necessidade de um melhor gerenciamento das questões relacionadas à TI. Esse cenário levou ao desenvolvimento de modelos que apresentem as melhores práticas para se obter a Governança da Tecnologia da Informação.

Entretanto, conselhos administrativos atuais precisam se certificar que não somente a TI esteja alinhada com as estratégias da organização, como também se estas estratégias estão tirando o melhor proveito da TI existente. Além disso, as organizações precisam reduzir significativamente os riscos inerentes ao uso da infra-estrutura de TI e simultaneamente obter indicadores dos benefícios de se ter essa infra-estrutura segura.

A proposta de estudo das correlações das metodologias CobiT e ITIL e norma ISO 17799 direcionado para o tema Segurança da Informação, permitirá um controle mais eficaz dos recursos e processos de TI, também contribuirá para redução dos riscos inerentes ao uso da infra-estrutura de TI, e permitirá a análise dos indicadores dos benefícios de se possuir uma infra-estrutura segura. A partir da utilização desse estudo, pretende-se demonstrar que o conhecimento sobre os riscos relacionados à infra-estrutura de TI sejam apresentados de forma objetiva no momento da definição do planejamento estratégico. O modelo CobiT e a norma ISO 17799 foram utilizadas para definição dos objetivos de controle a serem implementados e o modelo ITIL foi utilizado para definir os processos responsáveis pela implementação.

Abstract

The current dependence of organizations on IT infrastructure (Information Technology) demands consideration of the most effective means of IT management, especially in relation to the inherent risks and benefits. This has led to the development of models representing current best practice in Governing Information Technology.

However boards of directors need to assure themselves that IT is not only aligned to the strategies of the organization, but also that these strategies are maximizing the benefits of the existing IT infrastructure. Moreover, organizations need to reduce significantly the inherent risks associated with their IT infrastructures and simultaneously to understand the benefits of a secure environment.

The proposal of this study into the correlations between CobiT and ITIL methodologies and norm ISO 17799 relating to the Security of Information, will suggest a method for the more efficient control of IT resources and processes, which contributes to the reduction of risks while highlighting the benefits of a secure infrastructure. The CobiT model and norm ISO 17799 are used to define the controls and objectives to be implemented and the model ITIL is used to define the processes for implementation.

Palavras-Chave: NBR ISO/IEC 17799, CobiT, Segurança da Informação, ITIL, Tecnologia da Informação.

Lista de Figuras

Lista de Tabelas

Sumário

1. Introdução

Uma análise do cenário atual demonstra que o crescimento e o sucesso das organizações estão diretamente relacionados à necessidade de se manter uma infra-estrutura de Tecnologia da Informação (TI) segura e confiável. A dependência atual das organizações da sua infra-estrutura de TI, associado às oportunidades, benefícios e riscos inerentes a essa área, exige que essas organizações passem a considerar a necessidade de um melhor gerenciamento das questões relacionadas à TI. Esse cenário levou ao desenvolvimento de modelos que apresentem as melhores práticas para se obter a Governança da Tecnologia da Informação.

Entretanto, conselhos administrativos atuais precisam se certificar que não somente a TI esteja alinhada com as estratégias da organização, como também se estas estratégias estão tirando o melhor proveito da TI existente. Eles necessitam assumir cada vez mais a responsabilidade de garantir que as organizações estão oferecendo aos seus usuários um ambiente de TI seguro. Além disso, as organizações precisam reduzir significativamente os riscos inerentes ao uso da infra-estrutura de TI e simultaneamente obter indicadores dos benefícios de se ter essa infra-estrutura segura.

A proposta de estudo das correlações das metodologias CobiT e ITIL e norma ISO 17799 direcionado para o tema Segurança da Informação, permitirá um controle mais eficaz dos recursos e processos de TI, também contribuirá para redução dos riscos inerentes ao uso da infra-estrutura de TI, e permitirá a análise dos indicadores dos benefícios de se possuir uma infra-estrutura segura.

1.1. Objetivos do trabalho

A proposta de estudo das correlações das metodologias CobiT e ITIL e norma ISO 17799 direcionado para o tema Segurança da Informação, permitirá um controle mais eficaz dos recursos e processos de TI, também contribuirá para redução dos riscos inerentes ao uso da infra-estrutura de TI, e permitirá a análise dos indicadores dos benefícios de se possuir uma infra-estrutura segura. A partir da utilização desse estudo, pretende-se demonstrar que o conhecimento sobre os riscos relacionados à infra-estrutura de TI sejam apresentados de forma objetiva no momento da definição do planejamento estratégico. O modelo CobiT e a norma ISO 17799 foram utilizadas para definição dos objetivos de controle a serem implementados e o modelo ITIL foi utilizado para definir os processos responsáveis pela implementação.

Apresentar os aspectos principais das metodologias e normas utilizadas como referência para a elaboração deste estudo correlacional. Demonstrar a aplicabilidade das metodologias e normas utilizadas neste estudo correlacional em um cenário real.

1.2. Motivação do trabalho

A motivação para a utilização dessa estrutura surgiu na identificação de que a dificuldade de extração de conhecimento para a tomada decisão a partir de um grande volume de dados é comum tanto nas decisões relacionadas a negócios (onde geralmente são utilizados os SIGs) quanto no gerenciamento de segurança computacional.

As metodologias utilizadas neste estudo (CobiT e ITIL) e a norma ISO 17799 são ferramentas que atingiram um grau de maturidade elevado e possuem atualmente uma grande aceitação no mercado, isto foi um dos mais importantes fatores na definição de quais metodologias e normas seriam utilizados para a elaboração deste estudo correlacional.

1.3. Metodologia

A proposta de estudo descrita a seguir aborda o detalhamento de metodologias e normas para assegurar um melhor controle e uma utilização mais eficaz dos serviços de TI. Para tal esse estudo valeu-se de uma análise exploratória em alguns documentos do Gartner, do CobiT, do IT Governance, do IT Infrastructure Library e de outras fontes identificados na referência bibliográfica.

Na busca por um modelo capaz de abranger procedimentos associados a Segurança da Informação este trabalho mapeia diversos requisitos reconhecidos pelo mercado e identificados tanto na normativa de segurança mencionada neste trabalho, como na política de segurança das empresas de grande porte. Apartir da definição destes requisitos, é apresentando a correlação dos mesmos com as metodologias e normativas e como produto final uma proposta correlacional dos requisitos em função da análise correlacional.

O estudo também aborda além dos aspectos de Governança da Tecnologia da Informação, Segurança da Informação, Normas e outra ferramentas, com objetivo de enriquecer e servir como material de apoio à ser utilizado para definir os processos e mapear os controles a serem utilizados no estudo correlacional.

2. Governança da Tecnologia da Informação

A informação é reconhecida pelas organizações nos últimos anos como sendo um dos mais importantes recursos estratégicos que necessitam gerenciamento[1]. Atualmente, os sistemas e os serviços de Tecnologia da Informação (TI) 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, do termo inglês *IT Governance*, através da qual se procura o alinhamento da TI com os objetivos da organização. Governança da Tecnologia da Informação define que a TI é um fator essencial para a gestão financeira e estratégica de uma organização e não apenas um suporte aos mesmos.

Governança da Tecnologia da Informação pode ser definida como:

1. 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[2];
2. Capacidade organizacional exercida pelo conselho diretor, gerente executivo e gerente de TI de controlar o planejamento e implementação das estratégias de TI e dessa forma, permitir a fusão de TI ao negócio[3];
3. Especificação das decisões corretas em um modelo que encoraje o comportamento desejável no uso de TI nas organizações[4].

---

[1] Weill & Ross, 2004
[2] ITGI, 2001
[3] Van Grembergen, 2003
[4] Weill & Ross, 2004

Para alcançar a Governança da Tecnologia da Informação as organizações utilizam modelos de gestão que se aplicados asseguram a conformidade com as melhores práticas de processos e segurança da informação. Entre esses modelos, pode-se citar CobiT para a Governança de TI e ITIL para a gestão dos serviços de TI.

2.1. A Lei Sarbanes-Oxley

A Lei americana Sarbanes-Oxley foi originada em 2002, após escândalos corporativos de manipulação de dados contábeis ocorridos em grandes empresas norte-americanas como a empresa de energia Enron, Tyco e a WorldCom na área de telecomunicações. O escopo desta legislação federal se insere no âmbito da governança corporativa, e na ética nos negócios de companhias que possuem capital na Bolsa de Nova York.

Rígidos parâmetros legais foram impostos a estas empresas, aumentando desde o grau de responsabilidade dos executivos da empresa, até as auditorias e advogados contratados que atestarem balanços. As principais exigências incluem clareza na apresentação das informações financeiras, ênfase em assuntos de governança corporativa; processos rigorosos de controle interno; informações financeiras confiáveis e compreensíveis e independência das firmas de auditoria externa encarregada de validá-las.

Embora restrita ao governo norte-americano, a Sarbanes-Oxley é uma legislação que funciona como uma espécie de bola de neve no mercado de tecnologia do mundo todo. No Brasil, essa lei se aplica às empresas com ações negociadas nos mercados de capitais dos Estados Unidos, subsidiárias de empresas multinacionais de capital americano e empresas brasileiras com ações naquele país.

Em suas 1.107 seções, a maior atenção, discussão e trabalho a respeito da Sarbanes-Oxley está sendo focado nas seções 302 e 404 da Lei. A Seção

302 requer que o principal executivo (CEO) e o principal executivo de finanças (CFO) assumam a responsabilidade por definir, avaliar e monitorar a eficácia dos controles internos sobre relatórios financeiros e divulgações da empresa. Estes controles devem ser suficientes e capazes de livrar a instituição dos riscos que possam ameaçar suas principais funções e, com isso, prejudicar respectivas entidades e partes interessadas, como clientes e acionistas.

Na seção 404 da Lei é tratada a validação dos controles e procedimentos internos sobre os relatórios financeiros, esta avaliação deve ser formal e realizada anualmente por auditores externos. E na seção 409 trata da divulgação imediata, em Tempo Real e em base rápida e corrente, dados que possam impactar a performance financeira da empresa; informações com respeito a mudanças materiais na condição financeira ou operacional da organização.

2.2. A Basiléia II

Com a criação pelo Bank of International Settlements (BIS), o Banco Central dos Bancos Centrais que regula o setor no mundo inteiro, de um Novo Acordo de Capitais, o Basiléia II, as instituições financeiras começaram a se preocupar com a eficiência de seus controles internos e da gestão de riscos operacionais.

As recomendações do Comitê de Supervisão da Basiléia, que criou o Novo Acordo da Basiléia, publicado em Junho de 2004 pelo documento "Convergência Internacional de Mensuração e Padrões de Capital: Uma estrutura Revisada (Basiléia II)", tratam do estabelecimento de critérios mais adequados ao nível de riscos associados às operações conduzidas pelas instituições financeiras para fins de requerimento de capital regulamentar, exigindo que as perdas operacionais previstas sejam deduzidas da base de capital, impondo que as instituições tenham a mensuração, gestão e controle

do Risco Operacional. Este último, conforme descrito pelo Comitê da Basiléia em 2001, é o risco de perdas diretas e indiretas, resultante de falhas em processos internos ou de eventos externos[5], tais como fraudes, relações trabalhistas, danos a ativos, interrupção do negócio e falhas de 17 sistemas, execução e gestão de processo. Na prática, o novo acordo atinge os bancos da seguinte maneira: a instituição que não possuir controles internos eficientes e uma metodologia de avaliação de riscos implementada será obrigada a manter uma quantidade maior de recursos próprios em sua estrutura patrimonial, enquanto que, instituições que investirem nesses itens terão que reter menor volume de recursos, o que tem um impacto determinante na competitividade dos bancos.

Do ponto de vista da área de TI, será necessário a adoção de uma gestão de riscos operacionais para garantir total segurança e confidencialidade dos dados dos clientes, sem o comprometimento da instituição. Além de oferecer uma infra-estrutura de sistemas que assegure a integridade da base de dados e dos relatórios gerenciais, sendo preciso adaptar sistemas e procedimentos dos bancos relacionados à análise e medição do risco operacional. Para permitir uma estratégia de gerenciamento do risco o Basiléia II exige a captação, arquivamento e estruturação de dados históricos relacionados com a instituição nos últimos cinco anos, consolidando na base de dados todas informações sobre fraudes, lavagem de dinheiro, padrões de operações e comportamentos suspeitos, garantindo a existência de um ambiente adequado de controles[6]

2.3. CVM no Brasil[7]

A Lei que criou a CVM (6385/76) e a Lei das Sociedades por Ações (6404/76) disciplinaram o funcionamento do mercado de valores mobiliários e a

[5] CAMARGO, 2003
[6] CAMARGO, 2004
[7] CVM. Disponível em: http://www.cvm.gov.br/port/acvm/atribuic.asp. Acesso em: 07/01/2007

atuação de seus protagonistas, assim classificados, as companhias abertas, os intermediários financeiros e os investidores, além de outros cuja atividade gira em torno desse universo principal.

A CVM tem poderes para disciplinar, normatizar e fiscalizar a atuação dos diversos integrantes do mercado.

Seu poder normatizador abrange todas as matérias referentes ao mercado de valores mobiliários.

Cabe à CVM, entre outras, disciplinar as seguintes matérias:

registro de companhias abertas;
registro de distribuições de valores mobiliários;
credenciamento de auditores independentes e administradores de carteiras de valores mobiliários;
organização, funcionamento e operações das bolsas de valores;
negociação e intermediação no mercado de valores mobiliários;
administração de carteiras e a custódia de valores mobiliários;
suspensão ou cancelamento de registros, credenciamentos ou autorizações;
suspensão de emissão, distribuição ou negociação de determinado valor mobiliário ou decretar recesso de bolsa de valores;

O sistema de registro gera, na verdade, um fluxo permanente de informações ao investidor. Essas informações, fornecidas periodicamente por todas as companhias abertas, podem ser financeiras e, portanto, condicionadas a normas de natureza contábil, ou apenas referirem-se a fatos relevantes da vida das empresas. Entende-se como fato relevante, aquele evento que possa influir na decisão do investidor, quanto a negociar com valores emitidos pela companhia.

A CVM não exerce julgamento de valor em relação à qualquer informação divulgada pelas companhias. Zela, entretanto, pela sua regularidade e confiabilidade e, para tanto, normatiza e persegue a sua padronização.

A atividade de credenciamento da CVM é realizada com base em padrões pré-estabelecidos pela Autarquia que permitem avaliar a capacidade de projetos a serem implantados.

A Lei atribui à CVM competência para apurar, julgar e punir irregularidades eventualmente cometidas no mercado. Diante de qualquer suspeita a CVM pode iniciar um inquérito administrativo, através do qual, recolhe informações, toma depoimentos e reúne provas com vistas a identificar claramente o responsável por práticas ilegais, oferecendo-lhe, a partir da acusação, amplo direito de defesa.

O Colegiado tem poderes para julgar e punir o faltoso. As penalidades que a CVM pode atribuir vão desde a simples advertência até a inabilitação para o exercício de atividades no mercado, passando pelas multas pecuniárias.

A CVM mantém, ainda, uma estrutura especificamente destinada a prestar orientação aos investidores ou acolher denúncias e sugestões por eles formuladas.

Quando solicitada, a CVM pode atuar em qualquer processo judicial que envolva o mercado de valores mobiliários, oferecendo provas ou juntando pareceres. Nesses casos, a CVM atua como "amicus curiae" assessorando a decisão da Justiça.

Em termos de política de atuação, a Comissão persegue seus objetivos através da indução de comportamento, da auto-regulação e da auto-disciplina, intervindo efetivamente, nas atividades de mercado, quando este tipo de procedimento não se mostrar eficaz.

No que diz respeito à definição de políticas ou normas voltadas para o desenvolvimento dos negócios com valores mobiliários, a CVM procura junto a instituições de mercado, do governo ou entidades de classe, suscitar a discussão de problemas, promover o estudo de alternativas e adotar iniciativas, de forma que qualquer alteração das práticas vigentes seja feita com suficiente embasamento técnico e, institucionalmente, possa ser assimilada com facilidade, como expressão de um desejo comum.

A atividade de fiscalização da CVM realiza-se pelo acompanhamento da veiculação de informações relativas ao mercado, às pessoas que dele participam e aos valores mobiliários negociados. Dessa forma, podem ser efetuadas inspeções destinadas à apuração de fatos específicos sobre o desempenho das empresas e dos negócios com valores mobiliários.

2.3.1. Objetivos

De acordo com a lei que a criou, a Comissão de Valores Mobiliários exercerá suas funções, a fim de:

assegurar o funcionamento eficiente e regular dos mercados de bolsa e de balcão;

proteger os titulares de valores mobiliários contra emissões irregulares e atos ilegais de administradores e acionistas controladores de companhias ou de administradores de carteira de valores mobiliários;

evitar ou coibir modalidades de fraude ou manipulação destinadas a criar condições artificiais de demanda, oferta ou preço de valores mobiliários negociados no mercado;

assegurar o acesso do público a informações sobre valores mobiliários negociados e as companhias que os tenham emitido;

assegurar a observância de práticas comerciais equitativas no mercado de valores mobiliários;

estimular a formação de poupança e sua aplicação em valores mobiliários;

promover a expansão e o funcionamento eficiente e regular do mercado de ações e estimular as aplicações permanentes em ações do capital social das companhias abertas.

2.4. CobiT

O CobiT (Control Objectives for Information and Related Technology), foi desenvolvido pelo ISACF (The Information Systems Audit and Control Foundation), e posteriormente passou a ser mantido pelo ITGI (IT Governance Institute).

O CobiT consiste de 3 modelos:

Modelo de Processos de TI (framework)
Modelo para Governança de TI
Modelo de Maturidade de TI

A utilização conjunta desses modelos, paralelamente à metodologia incorporada no CobiT, permite a uma instituição exercer uma efetiva Governança de TI, especialmente aquelas que necessitam adequar-se às normas regulatórias, como a própria Sarbanes-Oxley. A governança é sustentada nas melhores práticas da indústria, e ocorre de forma orientada a processos, cujos graus de maturidade possibilitam o alcance dos objetivos de TI como função habilitadora dos negócios.

2.4.1. Modelo de Processos de TI

Atualmente este conjunto de diretrizes consiste de quatro seções: sumário executivo, o framework, o conteúdo principal (objetivos de controle, diretrizes de gerenciamento e modelos de maturidade) e apêndices. A divisão de conteúdos principais é dividida de acordo com os 34 processos de TI e apresenta o cenário completo de como controlar, gerenciar e medir cada processo.

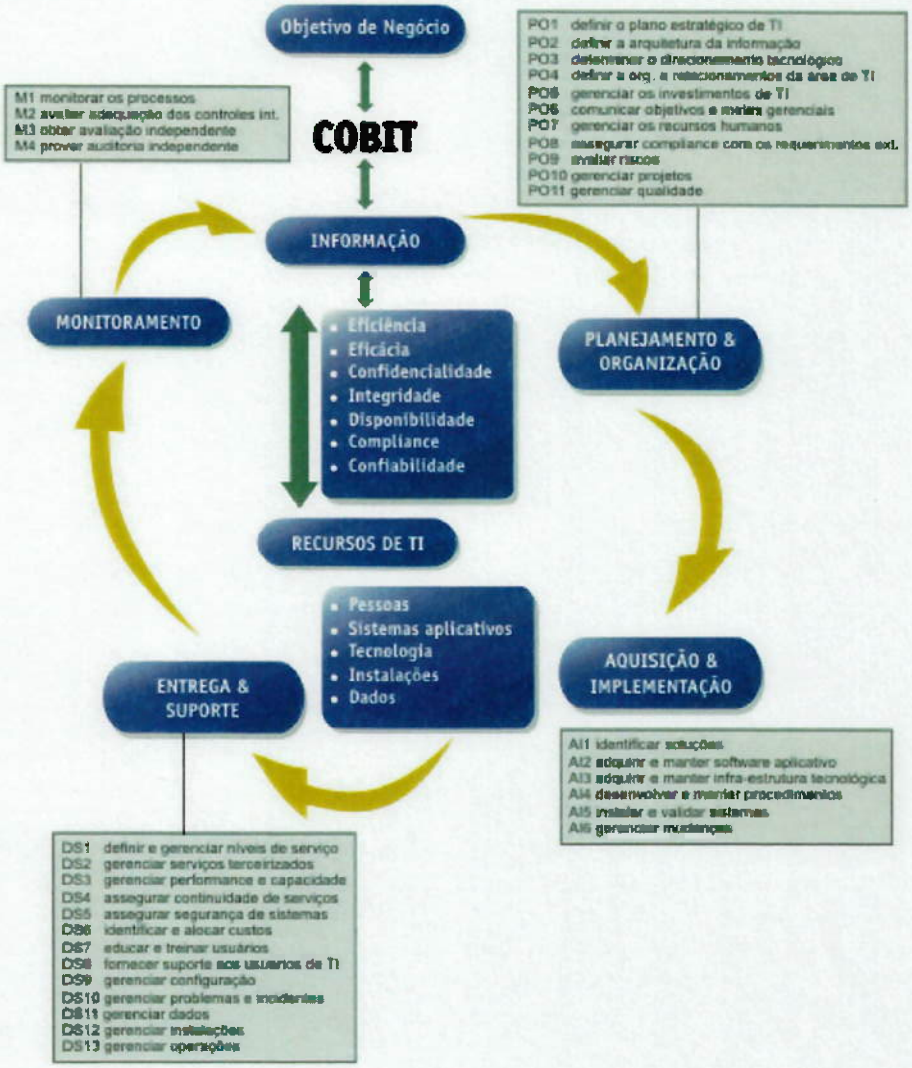
Tradicionalmente os componentes do CobiT são utilizados para auxiliar as organizações na própria preparação para as auditorias e no monitoramento e avaliação dos processos de TI. Para tanto, as boas práticas do CobiT são organizadas em processos, cada qual visando a um objetivo de controle.

Um objetivo de controle é definido como uma declaração de um propósito ou resultado desejado a ser alcançado, por meio da implementação de controles em determinada atividade de TI. Quando atingidos, por meio da implementação eficaz dos respectivos controles, garantem o alinhamento da TI aos objetivos do negócio. A responsabilidade pelo sucesso dos sistemas de controles é, portanto, da alta direção, a qual deve torná-los efetivos.

Controles, segundo o CobiT, são *políticas*, *procedimentos*, *práticas* e *estruturas organizacionais*, projetadas para prover razoável garantia de que os objetivos de negócio serão alcançados, e que eventos indesejáveis serão prevenidos, ou apagados e corrigidos.

Na Figura 1, podem ser identificados os 4 domínios do COBIT (Planejamento & Organização, Aquisição & Implementação, Entrega & Suporte, e Monitoramento), que integram um ciclo de vida repetível no sistema de gestão de TI. Para cada domínio, os processos podem ser identificados nos quadros cinzas respectivos.

Figura 1 – Os 4 domínios do COBIT, Fonte: ITGI



Os processos do CobiT são constituídos por alguns princípios (*Qualidade*, *Confiança* e *Segurança*), cuja representação no modelo acima corresponde aos 7 Critérios de Informação:

Eficácia

Eficiência

Confidencialidade

Integridade

Disponibilidade

Conformidade

Confiabilidade

O grau de importância de cada um desses critérios é uma função do negócio e do ambiente em que a organização opera. Numa avaliação de riscos, esses critérios atribuem pesos diferentes aos Processos do CobiT, em função da importância no alcance dos respectivos Objetivos de Controle.

Por exemplo, no Processo AI5 - *Instalar e Validar Sistemas*, que faz parte do *Domínio Aquisição & Implementação*, os critérios de informação considerados são Eficácia, Integridade e Disponibilidade.

2.4.2. Modelo para Governança de TI

O Modelo de Governança é constituído por componentes associados, que tornam TI um habilitador do negócio. Componentes do modelo:

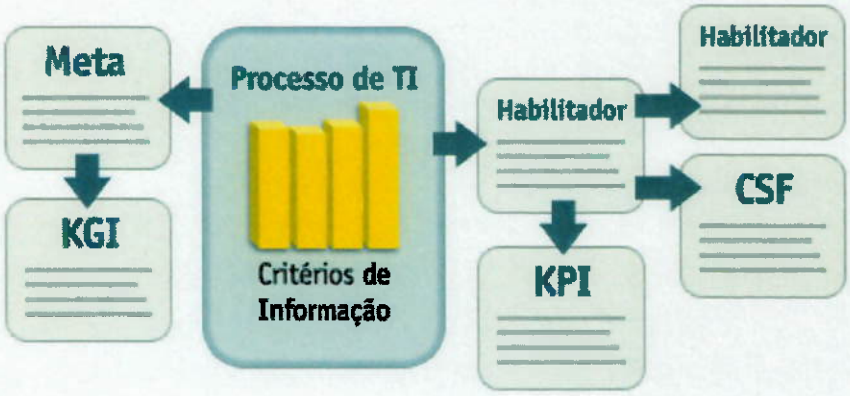
Fatores Críticos de Sucesso (CSFs - *Critical Success Factors*) - O que há de mais importante a ser feito para permitir que uma tarefa ou processo sejam concluídos;
Indicadores de Meta (KGIs - *Key Goal Indicators*) - São os parâmetros utilizados para reconhecer se o Processo alcançou as metas definidas (associadas aos objetivos);
Indicadores de Desempenho (KPIs - *Key Performance Indicators*) - Definem quão bem é o desempenho do Processo, em direção ao que foi definido como objetivo.

Um Processo deve alcançar os objetivos de negócio definidos nos Indicadores de Metas (KGIs). Um *habilitador*, resultante da combinação dos recursos de TI necessários e dos Fatores Críticos de Sucesso (CSFs) definidos para alcançar os referidos objetivos, fornece a informação segundo os Critérios de Informação necessários e é monitorado por Indicadores de Desempenho (KPIs).

Os Critérios de Informação podem ser: Eficácia, Eficiência, Confidencialidade, Integridade, Disponibilidade, Conformidade e Confiabilidade. A combinação desses elementos depende da natureza do Processo de TI.

A Figura 2 correlaciona esses elementos.

Figura 2 - TI como habilitador do Negócio, Fonte: ITGI



Por exemplo, no Processo AI5 - *Instalar e Validar Sistemas*, que faz parte do Domínio "Aquisição & Implementação", o objetivo de negócio é "verificar e confirmar que a solução é apropriada ao propósito desejado".

Para alcançar esse objetivo, um Fator Crítico de Sucesso é "os dados de teste estão disponíveis e representam dados de produção em tipo e quantidade, e o ambiente de teste representa ao máximo o ambiente de produção".

Os Critérios de Informação para esse Processo são: Eficácia, Integridade e Disponibilidade. De acordo com esses Critérios, um Indicador de Meta permite medir a consecução do objetivo. Um exemplo desse indicador é "quantidade reduzida de sistemas em produção não validados".

A habilitação conseguida por meio desse Processo pode ser avaliada por meio de Indicadores de Performance, cujo exemplo é "quantidade de descobertas durante a revisão de qualidade na instalação e validação de sistemas".

2.4.3. Modelo de Maturidade TI

Consiste de critérios de avaliação da Maturidade dos Processos, que viabilizam a decisão de investimentos nos processos considerados mais importantes para a TI, no âmbito da instituição. Paralelamente, permitem uma análise comparativa da evolução de TI frente a outras empresas do mesmo segmento ou de vários segmentos.

Existem 6 níveis de Maturidade, de complexidade crescente:

0. *Inexistente*: falta absoluta de elementos reconhecíveis do processo.
1. *Inicial* ("ad hoc"): reconhece-se, de forma despadronizada, o interesse em tratar da necessidade, ainda que caso a caso.
2. *Repetível*: procedimentos similares seguidos por pessoas distintas, para o mesmo tipo de atividade.
3. *Definido*: procedimentos padronizados e documentados, comunicados por meio de treinamento.
4. Gerenciado: é possível monitorar e medir a conformidade com os procedimentos.
5. Otimizado: processo automatizado e baseado nas melhores práticas.

A Maturidade deve ser avaliada em cada um dos Processos. O nível ótimo correspondente é determinado individualmente, de acordo com a natureza da instituição, ameaças e oportunidades viabilizadas por TI.

O CobiT fornece orientações, específicas para cada processo, do que deve ser trabalhado para atingir determinado nível de Maturidade.

2.4.4. Objetivos e Benefícios

O CobiT procura ocupar o espaço entre a Gestão de Riscos voltada para o Negócio (atendida, por exemplo, pelo COSO - Comitee of Sponsoring Organizations), a Gestão de Serviços em TI (por exemplo, por meio do ITIL) e a Gestão da Segurança da Informação (por exemplo, tratada pela ISO 27001). Esses modelos de gestão consistem de boas práticas específicas segundo sua área foco, e possuem funções complementares.

Dessa forma, o CobiT permite alinhar os objetivos dessas áreas de conhecimento às estratégias e princípios de governança corporativa, garantindo, assim, que os processos e atividades desempenhadas pelas respectivas áreas e funções corporativas concorram de forma sistemática para o alcance os objetivos do negócio e para a redução dos riscos operacionais.

O CobiT assegura aos usuários a existência de controles, inclusive tornando-os responsáveis por parte desses controles, e auxilia o trabalho dos auditores de sistemas e de segurança da informação.

2.5. ITIL[8]

Cada vez mais as organizações serão pressionadas a mostrar que possuem um rígido controle de todos os seus processos de negócios. Como a Tecnologia da Informação é parte integral de praticamente todos estes processos, é fundamental que as empresas alinhem fortemente suas atividades de TI aos seus objetivos de negócios.

Projetos de TI não entregues dentro dos prazos estabelecidos podem acarretar sérios riscos e afetar o planejamento da organização como um todo.

[8] ITIL. Disponível em: http://www.itilsurvival.com/. Acesso em: 15/12/2006

Por esta razão, o controle do ambiente de TI tem se tornado um item de extrema importância e de alta complexidade.

O Gerenciamento dos Serviços de TI (Information Technology Service Management - ITSM) vem ganhando grande destaque, permitindo às empresas contar com um controle da qualidade dos seus processos de TI, mensurando resultados dentro de padrões de eficiência e performance.

Um modelo de excelência em TI compõe-se da integração de diversas práticas de gestão, como por exemplo as de Gerenciamento de Serviços de TI definidas pelo modelo de referência ITIL (Information Technology Infrastructure Library).

A ITIL foi desenvolvida pela CCTA (Central Computer and Telecommunication Agency), atualmente chamada OGC (Office of Government Commerce), do Reino Unido, no final dos anos 80, sendo documentada em um conjunto de livros que descrevem um modelo de referência com as melhores práticas para um efetivo Gerenciamento dos Serviços de TI. Embora concebida originalmente para o setor público do Reino Unido, se expandiu rapidamente para as demais organizações dos setores públicos e privados, gerando uma indústria composta por treinamentos, certificações, consultorias, ferramentas de software e um Fórum específico, o itSMF (Information Technology Service Management Forum). Hoje em dia, a ITIL é um padrão adotado globalmente.

O uso efetivo das melhores práticas definidas na ITIL traz inúmeros benefícios às organizações, como: melhoria na utilização dos recursos; maior competitividade; redução de retrabalhos; eliminação de trabalhos redundantes; melhoria da disponibilidade, confiabilidade e segurança dos serviços de TI; qualidade dos serviços com custos justificáveis; fornecimento de serviços alinhados aos negócios, aos clientes e às demandas dos usuários; processos integrados; responsabilidades documentadas e comunicadas amplamente, e registro e controle de lições aprendidas.

A estrutura das publicações da ITIL, é composta pelos livros descritos a seguir:

1. **Service Support** - descreve a função de Service Desk e os processos de Incident Management, Problem Management, Configuration Management, Change Management e Release Management.
2. **Service Delivery** – descreve os processos de Capacity Management, Financial Management for IT Services, Availability Management, Service Level Management e IT Service Continuity Management.
3. **Planning to Implement Service Management** - explica os passos necessários para identificar como uma organização pode alcançar e usufruir os benefícios da ITIL.
4. **ICT Infrastructure Management** - este livro aborda os processos, organização e ferramentas necessários para prover uma infra-estrutura estável de TI e de Comunicações.
5. **Application Management** – é um guia para os usuários de negócios, desenvolvedores e gerentes de serviços que descreve como as aplicações podem ser gerenciadas sob a perspectiva de Gerenciamento de Serviços.
6. **Security Management** - este livro tem conexões com vários outros domínios da ITIL, explicando como gerenciar melhor os níveis de segurança da infra-estrutura de TI.
7. **Business Perspective** - este livro ajuda os Gerentes de Negócios a compreenderem a provisão dos serviços de TI.

As disciplinas de gerenciamento de serviços que estão no centro da biblioteca do ITIL estão divididas em dois grupos distintos: Serviços de Suporte e Serviços de Entrega. Os serviços de entrega estão focados na operação do dia a dia e no suporte aos serviços de TI enquanto os serviços de entrega consideram processos de planejamento de longo prazo.

2.5.1. A Teoria dos Processos do ITIL

A base do modelo de processos do ITIL é fundamentada na teoria de processos proposta pela OGC (2001)[9]. Segundo este princípio, a qualidade de um processo vem do modelo de processo que define os fluxos de trabalho e prove um guia para percorrê-lo. Um modelo de processo permite entender e ajudar a enunciar as características distintas de um processo. Segundo a OGC

[9] Office for Government Commerce - Disponível em: http://www.ogc.gov.uk/guidance_itil.asp Acesso em: 16/12/2006

(2001) um processo pode ser definido como: "uma série conectada de ações, atividades, mudanças, etc., executadas por agentes dentro do objetivo de satisfazer um propósito ou alcançar um objetivo."

Segundo a OGC (2001), definidos os processos, estes devem estar sob controle e uma vez sob controle, estes podem ser repetidos e gerenciados. Desta forma, a partir da definição do grau de controle sobre os processos é possível construir métricas para controlar estes processos.

A saída produzida por um processo deve estar de acordo com as normas operacionais que foram derivadas dos objetivos do negócio. Se o produto esta de acordo com as definições das normas, o processo pode ser considerado efetivo (porque pode ser repetido, medido e gerenciado). Se as atividades são executadas com o mínimo esforço, o processo pode ser considerado efetivo.

2.5.2. A Estrutura da Bibilioteca ITIL

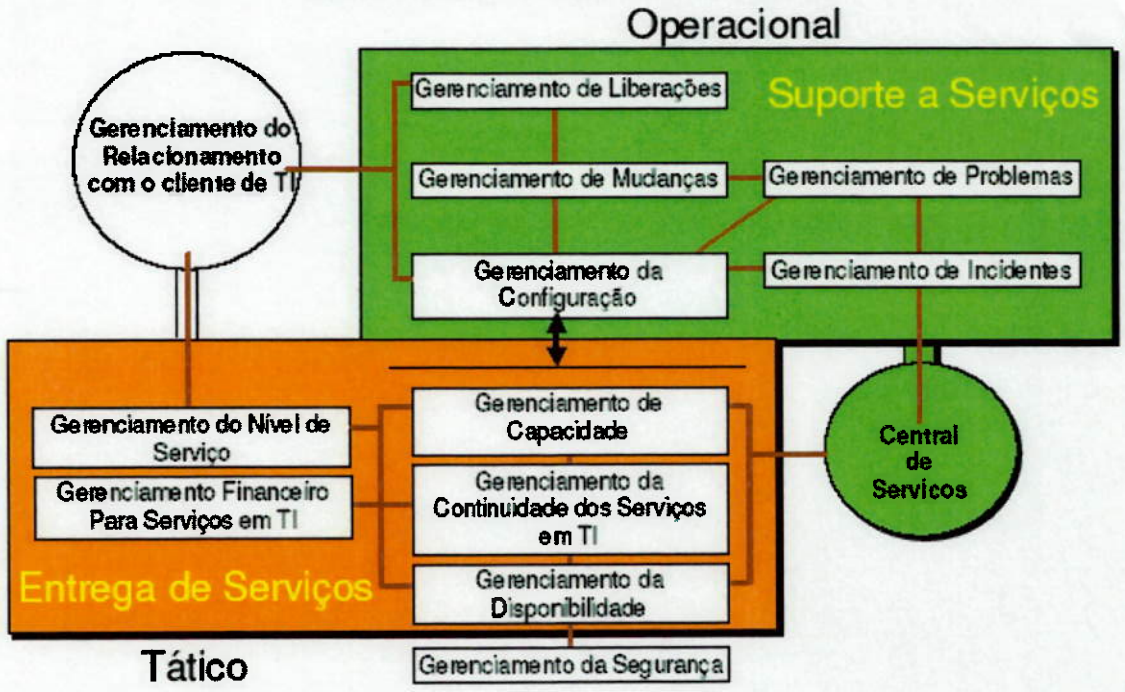
A biblioteca ITIL tem como foco principal a operação e a gestão da infra-estrutura de tecnologia na organização, incluindo todos os assuntos que são importantes no fornecimento dos serviços de TI. Nesse contexto, o ITIL considera que um serviço de TI é a descrição de um conjunto de recursos de TI. Os serviços de suporte do ITIL auxiliam no atendimento de uma ou mais necessidades do cliente, apoiando, desta forma, aos seus objetivos de negócios.

O princípio básico da biblioteca ITIL é o objeto de seu gerenciamento: a infra-estrutura de TI. O ITIL descreve os processos que são necessários para dar suporte à utilização e ao gerenciamento da infra-estrutura de TI. Outro princípio fundamental do ITIL é o fornecimento de qualidade de serviço aos clientes de TI com custos justificáveis, isto é, relacionar os custos dos serviços de tecnologia e como estes trazem valor estratégico ao negócio.

O interesse nesta área deve-se ao fato de que, através de metodologias (processos) padronizadas de Gerenciamento do Ambiente de TI, é possível obter uma relação adequada entre custos e níveis de serviços prestados pela área de TI.

Ao usar o ITIL, a organização se torna capaz de melhorar a qualidade, eficiência e eficácia na prestação de serviços, além de diminuir a exposição ao risco operacional. Os processos ITIL precisam ser implementados para cada organização, pois correspondem a um modelo (apresentado na Figura 3) e não uma regra rígida a ser seguida.

Figura 3 - Modelo do ITIL, Fonte: OGC (2001)



3. Segurança da Informação

A informação é um conjunto de dados que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita de cuidado e proteção.

Como a interconectividade tem crescido, a informação vem sendo cada vez mais exposta à pessoas, ameaças e riscos.

Independente de qual seja a forma que a informação está representada é sempre recomendado que ela seja protegida adequadamente. Com isso segurança da informação é a proteção da informação das ameaças na busca de manter a continuidade do negócio, diminuir os riscos e maximizar retornos.

A segurança da informação é obtida através da implementação de um conjunto de controles e técnicas adequadas, para a proteção da informação. Estas técnicas precisam ser trabalhadas para que sejam atendidas as necessidades de segurança.

3.1. Histórico da NORMA NBR ISO/IEC 17799:2005

O DTI (Departamento de Comércio e Indústria do Reino Unido), com a necessidade de criar uma estratégia de segurança para as informações do Reino Unido, criou em 1987 o CCSC (Comercial Computer Security Center), que tinha como objetivo criar uma norma de segurança que os atendesse.

Como a necessidade era alta, várias empresas e instituições internacionais buscaram estabelecer metodologias e padrões que melhor ajudasse o mercado em suas pendências relativas à Segurança da Informação.

Em 1989 depois de ter criado vários documentos preliminares o CCSC criou a **BS 7799** (Brithish Standart 7799), essa foi uma norma de segurança da

informação destinada a empresas, criada na Inglaterra em 1995 e disponibilizada para consulta pública dividida em duas partes: a primeira (BS 7799-1) em 1995, a segunda (BS 7799-2) em 1998.

A (BS 7799-1) é a parte da norma que é planejada como um documento de referência para pôr em execução "boas práticas" de segurança na empresa.

A (BS 7799-2) é a parte da norma que tem o objetivo de proporcionar uma base para gerenciar a segurança da informação dos sistemas da empresa.

Após um trabalho árduo de internacionalização e consultas públicas, foi aceita em dezembro de 2000, a BS 7799 como padrão internacional pelos países membros as ISO. Isto implica na junção de duas organizações ISO (International Standartization Organization) e IEC (International Engineering Consortium), sendo assim denominada **ISO / IEC 17799:2000**.

A ISO é uma organização internacional formada por um conselho e comitês com membros oriundos de vários países. Seu objetivo é criar normas e padrões universalmente aceitos sobre a realização de atividades comerciais, industriais, científicas e tecnológicas. A IEC é uma organização voltada ao aprimoramento da indústria da informação.

Com isso em dezembro de 2000 a ABNT (Associação Brasileira de Normas Técnicas) também resolveu acatar a norma ISO como padrão brasileiro sendo publicada em 2001 como: **NBR 17799** – Código de Prática para a Gestão da Segurança da Informação. O importante é que a partir dessa publicação passamos a ter um referencial de aceitação internacional.

No segundo semestre de 2005 foi lançada à nova versão da norma, a norma **ISO / IEC 17799:2005**, que cancela e substitui a edição anterior.

3.2. Governança de Segurança da Informação

Ao descrever o cenário atual para o gerenciamento de Segurança da Informação, cria-se a necessidade e justifica-se a importância de se alcançar um 'Modelo de Governança da Segurança da Informação'. Esse modelo deverá ser utilizado pelas organizações para que a Segurança da Informação não seja tratada apenas no âmbito tecnológico, mas reconhecida como parte integrante do planejamento estratégico das organizações no processo de tomada de decisão. O IIA (*The Institute of Internal Auditors*) publicou um trabalho onde destaca que, uma vez que os diretores das organizações são responsáveis pelos bons resultados e pela continuidade da organização que eles governam, eles precisam aprender a identificar atualmente as questões corretas sobre segurança computacional e ainda, considerá-las como parte de sua responsabilidade[10].

Atualmente as responsabilidades acerca da segurança computacional são frequentemente delegadas ao gerente de segurança (*Chief Security Officer*) das organizações, gerando conflitos em relação ao orçamento destinado a essa área e a necessidade de impor medidas que vão além de seu escopo de atuação. Dessa forma, é muito comum encontrar um cenário onde as questões de segurança computacional não são tratadas em um nível de gestão da organização, tendo como conseqüência a falta de recursos para minimizar os riscos existentes ao nível exigido pela estratégia organizacional e definido pela análise de risco. A responsabilidade pelo nível correto de segurança da informação deve ser uma decisão estratégica de negócios, tendo como base um modelo de Governança da Segurança da Informação que contemple uma análise de risco.

Em um relatório do *Corporate Governance Task Force* é proposto que, para proteger melhor a infraestrutura de TI, as organizações deveriam

[10] IAA, 2001

incorporar as questões de segurança computacional em suas ações de governança[11].

Em um trabalho publicado em 2003, o BSA (*Business Software Alliance*) chama a atenção para a necessidade de desenvolver um Modelo de Governança da Segurança da Informação que possa ser adotado imediatamente pelas organizações[12]. Nesse trabalho é sugerido que os objetivos de controle contidos na ISO 17799 devam ser considerados e ampliados para o desenvolvimento de um modelo onde segurança da informação não seja considerada apenas no plano tecnológico, mas parte integrante das "melhores práticas corporativas", não deixando de cobrir aspectos relacionados a pessoas, processos e tecnologia.

Para que as organizações obtenham sucesso no processo de segurança de sua informação, os gestores precisam tornar a segurança computacional uma parte integrante da operação do negócio da organização[13]. A forma proposta para se conseguir isso é a estruturação de um Modelo de Governança da Segurança da Informação como parte do controle interno e políticas que façam parte da Governança Corporativa. Considerando-se esse modelo, a segurança da informação deixaria de ser tratada apenas como uma questão técnica, passando a ser um desafio administrativo e estratégico.

3.3. Requisitos para a proposta de um modelo correlacional para o tema Segurança da Informação

Uma vez que as organizações possuem necessidades distintas, elas irão apresentar abordagens diversas para tratar as questões relacionadas a segurança da informação. Dessa forma, um conjunto principal de requisitos deve ser definido para guiar os mais diversos esforços.

---

[11] CGTFR, 2004
[12] BSA, 2003
[13] ENTRUST, 2004

Na busca por um modelo capaz de abranger procedimentos associados a Segurança da Informação este trabalho mapeia diversos requisitos reconhecidos pelo mercado e identificados tanto na normativa de segurança mencionada neste trabalho, como na política de segurança das empresas de grande porte[14].

1. Os CEOs (*Chief Executive Officers*) precisam de procedimentos para conduzir uma avaliação periódica sobre segurança da informação, revisar os resultados com sua equipe e comunicar o resultado para o conselho administrativo;
2. Os CEOs precisam adotar e patrocinar boas práticas corporativas para segurança computacional, sendo municiados com indicadores objetivos que os façam considerar a área de segurança computacional como um importante centro de investimentos na organização, e não apenas um centro de despesas;
3. Organizações devem conduzir periodicamente uma avaliação de risco relacionada à informação como parte do programa de gerenciamento de riscos;
4. Organizações precisam desenvolver e adotar políticas e procedimentos baseados na análise de risco para garantir a segurança da informação;
5. Organizações precisam estabelecer uma estrutura de gerenciamento da segurança da informação para definir explicitamente o que se espera de cada indivíduo (papéis e responsabilidades);
6. Organizações precisam desenvolver planejamento estratégico e iniciar ações para prover a segurança adequada para a rede de comunicação, os sistemas e a informação;
7. Organizações precisam tratar segurança da informação como parte integral do ciclo de vida dos sistemas;
8. Organizações precisam divulgar as informações sobre segurança computacional, treinando e educando os indivíduos;

14 http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=27628

9. Organizações precisam conduzir testes periódicos e avaliar a eficiência das políticas e procedimentos relacionados a segurança da informação;
10. Organizações precisam criar e executar um plano para remediar vulnerabilidades ou deficiências que comprometam a segurança da informação;
11. Organizações precisam desenvolver e colocar em prática procedimentos de resposta a incidentes;
12. Organizações precisam estabelecer planos, procedimentos e testes para prover a continuidade das operações;
13. Organizações precisam usar as melhores práticas relacionadas à segurança computacional, como a ISO 17799[15], para medir o nível alcançado em relação à segurança da informação.

Tendo como base a estrutura de tomada de decisão em sistemas de informação gerenciais, este trabalho propõe a correlação dos princípios citados anteriormente em três níveis: Operacional, Tático e Estratégico. A organização nesses níveis irá permitir a evolução de dados (nível operacional) em informação (nível tático) e ainda, em conhecimento (nível estratégico) que possa ser útil aos gestores no desenvolvimento do planejamento estratégico das organizações.

O modelo proposto neste trabalho está estruturado para prover o conhecimento necessário para motivar os administradores a patrocinar a utilização das melhores práticas de segurança computacional em todos os níveis da organização.

Dessa forma, o modelo é capaz de apontar as melhores práticas a serem seguidas em cada um dos níveis da organização, contemplando três pontos principais em cada um desses níveis:

1) O que se espera de cada indivíduo (o que deve e o que não deve ser feito);

[15] ISO, 2000

2) Como cada indivíduo poderá verificar se está cumprindo o que é esperado (indicadores de produtividade);
3) Quais métricas devem ser utilizadas para medir a eficiência dos processos executados e apontar ajustes que necessitam ser aplicados.

Estruturado dessa forma, o modelo permitirá o trabalho proativo e a identificação de quais melhores práticas devem ser implementadas em determinado momento a uma organização.

3.4. Outras Normas e Ferramentas

Na área de segurança da informação existem vários documentos e normas que tratam diretamente ou indiretamente da segurança da informação, na qual, o objetivo maior é apresentar orientações e sugestões ao Gestor na aplicação da boa prática da política de segurança.

Este trabalho apresenta um histórico e uma série de normas e ferramentas que auxiliam ou auxiliaram (como ferramenta ou referência para a criação de normas mais recentes) na manutenção da segurança de um determinado nicho tecnológico.

3.4.1. Orange Book[16]

O "The Orange Book" representou o marco "zero", do qual nasceram vários padrões de segurança, cada qual com a sua filosofia e métodos proprietários, contudo visando uma padronização mundial. Houve um esforço para a construção de uma nova norma, mais atual e que não se detivesse

[16] Orange Book. Disponível em: http://www.dynamoo.com/orange/summary.htm. Acesso em: 15/12/2006

somente na questão da segurança de computadores, mas sim na segurança de toda e qualquer forma de informação. Este esforço foi liderado pela ISO (International Organization for Standardization).

Em 1977 o Departamento de Defesa dos Estados Unidos, formulou um plano sistemático para tratar do Problema Clássico de Segurança, o qual daria origem ao "DoD Computer Security Initiative", que, por sua vez, desenvolveria um "centro" para avaliar o quão seguro eram as soluções disponibilizas. A construção do "centro" gerou a necessidade da criação de um conjunto de regras a serem utilizadas no processo de avaliação. Este conjunto de regras ficaria conhecido informalmente como "The Orange Book", devido a cor da capa deste manual de segurança.

Mesmo que o "Orange Book", atualmente, seja considerado um documento "ultrapassado", podemos considerá-lo como o marco inicial de um processo mundial e contínuo de busca de um conjunto de medidas que permitam, a um ambiente computacional, ser qualificado como seguro. Esta norma de segurança permitiu e continua permitindo a classificação, por exemplo, do nível de segurança fornecido pelos sistemas operacionais atualmente utilizados, como é o caso: do OpenBSD, do FreeBSD, do NetBSD, do Solaris, do AIX, do QNX, dos vários "sabores" de Linux e até mesmo das várias versões do Windows. Como a classificação era realizada pelo "centro" ficou mais fácil comparar as soluções fornecidas pela indústria, pelo mercado e pelo meio acadêmico de uma forma geral, o que não era possível até então. Outro fator a ser lembrado é que o "Orange Book", dentro de sua "formalidade", permite, de uma maneira simples, especificar o que deve ser implementado e fornecido por um software, para que ele seja classificado em um dos níveis de segurança pré-estipulados, permitindo assim que este também seja utilizado como fonte de referência para o desenvolvimento de novas aplicações e para o processo de atualização ou refinamento de aplicações já existentes e em uso.

3.4.2. Common Criteria[17]

A norma ISO 15408 (Common Criteria) é uma combinação de esforços dos governos dos EUA, Canadá, Alemanha e França para unificar as suas normas para sistemas considerados seguros.

Atualmente estamos na versão 2.1 do Common Criteria e o objetivo desta norma é avaliar um sistema e não certificá-lo. O volume 2 desta norma é um catálogo de componentes de segurança. Exemplos destes componentes são: classe de auditoria e integridade dos logs dos eventos. O que se deve definir, no contexto da certificação para o CFM (Conselho Federal de Medicina), é o conjunto de componentes de segurança que define a segurança de um Prontuário Eletrônico (documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo de forma eletrônica e informatizada).

3.4.3. Norma ISO/IEC TR 13335[18]

Formalmente denominada de Guidelines for the Management of IT Security (GMITS), a norma (ISO/IEC TR 13335:1998) é composta por 5 partes envolvendo a área de TI:

A Parte 1 – Concepts and Models for IT Security, publicada em 1996, fornece uma visão geral dos conceitos e modelos fundamentais usados na gestão de segurança de TI.

---

[17] Common Criteria. Disponível em: http://www.commoncriteriaportal.org. Acesso em: 15/12/2006
[18] Norma ISO/IEC TR 13335. Disponível em: www.contacta.com.br/rodrigo/mestrado/referencias.htm. Acesso em 15/12/2006

A Parte 2 – Managing and Planning IT Security – da norma, publicada em 1997, trata do relacionamento da área de segurança da informação com as demais áreas da organização, principalmente a área de segurança corporativa. De maneira semelhante ao padrão BS7799, a Parte 2 sugere a criação de um comitê interdisciplinar que envolva as diversas áreas da empresa principalmente os responsáveis pelos ativos e pelas informações. Este comitê deve reunir-se periodicamente para definir os níveis aceitáveis de risco, cobrar e acompanhar resultados e reavaliar o projeto de segurança da informação quando necessário. A cláusula 7 da Parte 2 especifica um fluxo de planejamento e gerenciamento do projeto de segurança da informação, além de definir uma série de responsabilidades, com a orientação das atribuições dos atores do processo.

Publicada em 1998, a Parte 3 – Techniques for the Management of IT Security descreve técnicas de gestão de segurança para a área de TI. Ela pode ser utilizada em conjunto com a norma BS7799-2, que sugere quais os processos (e não apenas as técnicas, como na ISO 13335-3) devem ser implantados na condução da gestão de segurança. Vale observar ainda que a Parte 3 trata a gestão de risco em praticamente todas as cláusulas, através de técnicas de análise de risco.

A Parte 4 – Selection of Safeguards – foi publicada em 2000 e fornece um catálogo de contramedidas e um guia para a seleção destas.

A Parte 5 – Management Guidance on Network Security – complementa a parte 4 da norma, acrescentando fatores relevantes para a conexão de sistemas em redes, tendo sido publicada no ano de 2001.

3.4.4. Norma IEC 61508[19]

[19] Norma IEC 61508. Disponível em: http://www.controleinstrumentacao.com.br/arquivo/ed_104/cv5.html. Acesso em: 15/12/2006

A norma internacional (IEC 61508:1998) enfoca, através de uma abordagem genérica, as atividades do Ciclo de Vida de Segurança para os Sistemas Elétricos, Eletrônicos e Eletrônicos Programáveis (E/E/PES) que são utilizados para desempenhar funções de segurança. Neste sentido, esta norma vem sendo elaborada com o objetivo de desenvolver um policiamento técnico consistente para todos os sistemas elétricos/eletrônicos relacionados com a segurança.

Os principais objetivos desta norma são: tratar sistematicamente todas as atividades do ciclo de vida de um sistema instrumentado de segurança; habilitar que os desenvolvimentos tecnológicos dos produtos se realizem em ambiente sistemático de segurança funcional; ressaltar as melhorias dos Programmable Eletronic Safety (PES - sistema para controle, proteção ou monitoração baseado em um ou mais dispositivos eletrônicos programáveis) nos aspectos de desempenho e de viabilidade econômica e; uniformizar conceitos e servir de base para elaboração de normas setoriais.

Embora esta norma esteja sendo direcionada para sistemas elétricos/eletrônicos de segurança, evidentemente sua orientação pode ser aproveitada em sistemas de segurança implementados através de outras tecnologias, como por exemplo, mecânica, hidráulica ou pneumática. Esta norma está subdividida em 7 partes. As partes 1, 2, 3 e 4 da IEC 61508 são publicações de segurança básicas, tendo, respectivamente, as seguintes denominações: (1) Requisitos Gerais; (2) Requisitos para Sistemas Elétricos, Eletrônicos e Eletrônicos Programáveis (E/E/PES); (3) Requisitos de Software e; (4) Definições. As partes 5 e 6 apresentam, respectivamente, um Guia para Aplicação da Parte 1 (métodos de determinação dos níveis de integridade de segurança) e um Guia para a Aplicação das Partes 2 e 3. A parte 7 contém uma Bibliografia de Técnicas e Medidas.

A norma IEC 61508 adota uma abordagem baseada em risco, tratando-o como uma combinação de probabilidades e conseqüências de ocorrência. O termo utilizado, Segurança Funcional, é uma característica de sistemas relacionados com a segurança. Nesses sistemas, o conceito Segurança é uma

característica do equipamento, incluindo o sistema de controle associado que pode produzir o risco.

Os níveis de integridade de segurança representam medidas internas do sistema adequadas para lidar com o risco. Este conceito direciona a padronização de duas classes de requisitos que devem ser especificados antes do início do processo de desenvolvimento do sistema de segurança. A primeira classe de requisito diz respeito às Funções de Segurança, que devem ser especificadas através do documento denominado "Especificação dos Requisitos Funcionais de Segurança". A segunda classe de requisitos está relacionada com a Integridade de Segurança, devendo ser documentada através do relatório "Especificação dos Requisitos de Integridade de Segurança".

Decidir qual modelo adotar também não é tarefa fácil. Assumindo que os objetivos de TI serão atingidos por meio de dimensões como estruturas e regras, processos, tecnologia, pessoas, controles e métricas, todos os modelos listados apresentam pontos fortes e limitações.

3.4.5. Coso[20]

Em 1985, foi criada, nos Estados Unidos, a National Commission on Fraudulent Financial Reporting (Comissão Nacional sobre Fraudes em Relatórios Financeiros), uma iniciativa independente, para estudar as causas da ocorrência de fraudes em relatórios financeiros/contábeis. Esta comissão era composta por representantes das principais associações de classe de profissionais ligados à área financeira. Seu primeiro objeto de estudo foram os controles internos. Em 1992 publicaram o trabalho "Internal Control - Integrated Framework" (Controles Internos – Um Modelo Integrado). Esta publicação tornou-se referência mundial para o estudo e aplicação dos controles internos, e é a base que fundamenta o presente texto.

[20] Coso. Disponível em: http://www.auditoriainterna.com.br/coso.htm. Acesso em: 15/12/2006

Posteriormente a Comissão transformou-se em Comitê, que passou a ser conhecido como COSO – The Comitee of Sponsoring Organizations (Comitê das Organizações Patrocinadoras). O COSO é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa. É patrocinado por cinco das principais associações de classe de profissionais ligados à área financeira nos Estados Unidos, conforme apresentado na Tabela 1.

Tabela 1 – Principais associações de classe de profissionais ligados à área financeira nos Estados Unidos		
AICPA	American Institute of Certified Public Accounts	Instituto Americano de Contadores Públicos Certificados
AAA	American Accounting Association	Associação Americana de Contadores
FEI	Financial Executives	Executivos Financeiros
IIA	The Insititute of Internal Auditors	Instituto dos Auditores Internos
IMA	Institute of Management Accountants	Instituto dos Gestores Contábeis

O Comitê trabalha com independência, em relação a suas entidades patrocinadoras. Seus integrantes são representantes da indústria, dos contadores, das empresas de investimento e da Bolsa de Valores de Nova York. O primeiro presidente foi James C. Treadway, de onde veio o nome "Treadway Comission". Atualmente John Flaherty ocupa a presidência.

3.4.6. Norma ISO/IEC 27000[21]

Este conjunto de normas ISO/IEC é o mais importante referencial de Segurança da Informação. Estas normas substituíram a normas **BS 7799-2** (referente à Gestão de Segurança da informação) e **ISO 17799** (Código de Boas Práticas da Gestão de Segurança da Informação).

Na família 27000, novos segmentos serão abordados sob normas que variam de 27000 à 27009.

[21] FARIAS JR., Ariosto. "A Família ISO/IEC 27000" em Security Review: Conteúdo Editorial, Janeiro/fevereiro 2006, ano II, número 66, pp. 8-10.

No Brasil, apenas seis organizações até o momento atual conseguiram obter o certificado ISO27001: Serasa, Banco Matone, Samarco, Módulo Security, Unisys e SERPRO.

Como resultado destas novas normas, a listagem das normas ISO de Segurança da Informação será a seguinte:

- **NÚMERO: ISO IEC NWIP 27000 TÍTULO:** Information Security Management Systems - Fundamentals and Vocabulary APLICAÇÃO: Este projeto de norma tem como objetivo apresentar os principais conceitos e modelos relacionados com segurança da informação SITUAÇÃO: Este projeto de norma encontra-se ainda nos primeiros estágios de desenvolvimento, denominado de NWIP-New Work Item Proposal. A previsão para publicação como norma internacional é 2008-2009.
- **NÚMERO: ISO IEC 27001:2005**[22] **TÍTULO:** Information Security Management Systems-Requirements SITUAÇÃO: Norma aprovada e publicada pela ISO em Genebra, em 15.10.2005. No Brasil, a ABNT publicou como Norma Brasileira NBR ISO IEC 27001 no primeiro trimestre de 2006. APLICAÇÃO: Esta norma é aplicável a qualquer organização, independente do seu ramo de atuação, e define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação. A ISO IEC 27001 é a norma usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Portanto, uma organização que deseje implantar um SGSI deve adotar como base a ISO IEC 27001.
- **NÚMERO: ISO IEC 27002:2005 TÍTULO:** Information Technology - Code of practice for information Security Management SITUAÇÃO: Norma aprovada e publicada pela ISO em Genebra, em 15.06.2005. No Brasil, a ABNT publicou como Norma Brasileira NBR ISO IEC 17799 no dia 24 de agosto de 2005 APLICAÇÃO: Esta norma é um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma

[22] Disponível em: http://www.abntonline.com.br/consultanacional/. Acesso em: 16/12/2006

organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.

- **NÚMERO: ISO IEC 1st WD 27003 TÍTULO:** Information Security Management Systems-Implementation Guidance SITUAÇÃO: Este projeto de norma encontrase em um estágio de desenvolvimento, denominado de WD-Working Draft. A previsão para publicação como norma internacional é 2008-2009 APLICAÇÃO: Este projeto de norma tem como objetivo fornecer um guia prático para implementação de um Sistema de Gestão da Segurança da Informação, baseado na ISO IEC 27001.
- **NÚMERO: ISO IEC 2nd WD 27004 TÍTULO:** Information Security Management- Measurements SITUAÇÃO: Este projeto de norma encontra-se em um estágio onde vários comentários já foram discutidos e incorporados ao projeto. A previsão para publicação como norma internacional é 2008-2009 APLICAÇÃO: Este projeto de norma fornece diretrizes com relação a técnicas e procedimentos de medição para avaliar a eficácia dos controles de segurança da informação implementados, dos processos de segurança da informação e do Sistema de Gestão da Segurança da Informação.
- **NÚMERO: ISO IEC 2nd CD 27005 TÍTULO:** Information Security Management Systems-Information Security Risk Management SITUAÇÃO: Este projeto de norma já se encontra em um estágio mais avançado, pois vem sendo discutido há mais de dois anos. A previsão para publicação como norma internacional é 2007. APLICAÇÃO: Este projeto de norma fornece diretrizes para o gerenciamento de riscos de segurança da informação.

4. Processos e Controles mapeados na correlação dos Modelos CobiT e ITIL e a Norma ISO 17799

Este trabalho propõe a combinação das potencialidades dos modelos CobiT e ITIL e da norma ISO 17799. Esses modelos vêm sendo utilizados isoladamente pelas organizações nos últimos anos e representam as melhores práticas desenvolvidas, testadas e aprovadas por especialistas ao redor do mundo.

4.1. Relacionamento dos processos

Para que o modelo CobiT, o modelo ITIL e a norma ISO 17799 possam ser utilizados neste estudo, este trabalho apresentará uma correlação entre os objetivos de controle apresentados no modelo CobiT e os apresentados na norma ISO 17799. Também serão apresentados quais objetivos de controle são referenciados pelos processos descritos no modelo ITIL (Suporte a Serviços e Entrega de Serviços).

A Tabela 2 a seguir apresenta a proposta deste trabalho para estruturação dos objetivos de controle em níveis organizacional, tático e estratégico.

Comparado ao modelo CobiT, o modelo ITIL descreve de forma detalhada os processos relativos ao suporte e entrega de serviços, mas não cobre todos os requisitos de controle relacionados ao gerenciamento de TI descritos pelo CobiT para este domínio. Alguns objetivos de controle do modelo CobiT no domínio planejamento e organização são tratados superficialmente através dos processos do modelo ITIL. O modelo ITIL não aborda o domínio de Monitoramento do modelo CobiT.

O modelo ITIL não está focado em descrever o que deve ser abordado no gerenciamento de TI. Seus processos estão estruturados e detalhados para indicar como implementar e quem (papéis e responsabilidades).

Tabela 2 - Relacionamento de Processos entre os modelos ITIL e COBIT e a norma ISO 17799

	Objetivos de Controle do COBIT	Objetivos de Controle do COBIT referenciados na ISO 17799	Objetivos de Controle do COBIT referenciados no modelo ITIL
Nível Estratégico	PO – Planejamento e Organização		
	PO1-Definir um Plano Estratégico de TI		
	PO2-Definir a Arquitetura da Informação	X	
	PO3-Determinar a Direção Tecnológica	X	Superficialmente
	PO4-Definir a Organização e Relacionamentos de TI	X	Superficialmente
	PO5-Gerenciar o Investimento em TI		Superficialmente
	PO6-Comunicar metas e diretivas gerenciais	X	
	PO7-Gerenciar Recursos Humanos	X	
	PO8-Garantir Conformidade com Requisitos Externos	X	
	PO9-Avaliar Riscos	X	
	PO10-Gerenciar Projetos		
	PO11-Gerenciar Qualidade		
Nível Operacional e Nível Tático	AI - Aquisição e Implementação		
	AI1-Identificar Soluções Automatizadas	X	X
	AI2-Adquirir e Manter Software Aplicativo	X	X
	AI3-Adquirir e Manter Infra-estrutura Tecnológica	X	X
	AI4-Desenvolver e Manter Procedimentos	X	X
	AI5-Instalar e Validar Sistemas	X	X
	AI6-Gerenciar Mudanças	X	X
	DS – Entrega e Suporte		
	DS1-Definir e Gerenciar Níveis de Serviço	X	X
	DS2-Gerenciar Serviços de Terceiros	X	X
	DS3-Gerenciar Desempenho e Capacidade	X	X
	DS4-Garantir Continuidade dos Serviços	X	X
	DS5-Garantir Segurança de Sistemas	X	
	DS6-Identificar e Alocar Custos		X
	DS7-Educar e Treinar Usuários	X	
	DS8-Auxiliar e Aconselhar Clientes	X	X
	DS9-Gerenciar Configuração	X	X
	DS10-Gerenciar Problemas e Incidentes	X	X
	DS11-Gerenciar Dados	X	X
	DS12-Gerenciar instalações	X	
	DS13-Gerenciar a Operação	X	X
Nível Estratégico	M – Monitoramento		
	M1–Monitorar os Processos	X	
	M2–Avaliar a Adequação do Controle Interno	X	
	M3–Obter certificação Independente		
	M4–Providenciar Auditoria Independente		

Após uma avaliação de cada objetivo de controle descrito no modelo CobiT, este trabalho propõe uma categorização nos níveis operacional, tático e estratégico.

5. A utilização da estrutura de decisão de sistemas de Informação Gerenciais

O ponto de partida para a construção do modelo proposto neste trabalho consiste na definição de uma estrutura baseada nos modelos de tomada de decisão em Sistemas de Informações Gerenciais.

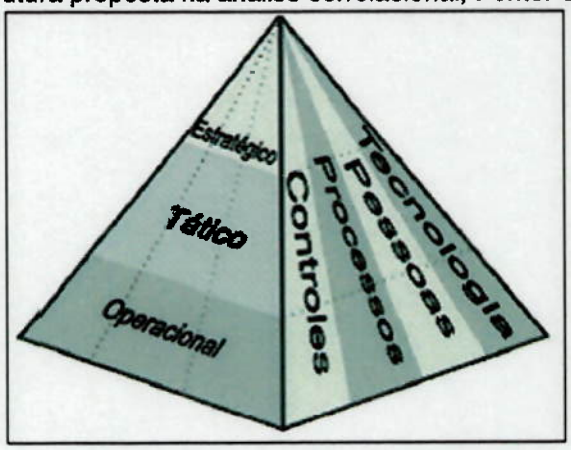
Essa estrutura consiste de uma divisão em 3 níveis: nível operacional (dados do dia-a-dia, pontuais), nível tático (informação obtida a partir de dados agrupados, sintetizados, totais, percentuais, acumulados, plurais, etc) e nível estratégico (conhecimento macro, objetivo e relacionado a todo o ambiente interno e externo).

Nessa estrutura, um *Data Warehouse* será responsável por armazenar os mais diversos tipos de dados relacionados a segurança computacional provenientes do ambiente e que serão úteis no processo a extração do conhecimento necessário ao gestor para o planejamento estratégico da organização.

O processo de extração de conhecimento da base de dados terá no nível operacional os dados como matéria prima bruta. Através dos processos descritos no modelo ITIL, o sistema de informação permitirá que esses dados sejam coletados e armazenados (nível operacional) e a seguir, trabalhados para que possam gerar informação no nível tático. A partir dos processos de auditoria, monitoração, definição de níveis de maturidade descritos no modelo COBIT e das técnicas para a extração de conhecimento das bases de dados, essas informações serão estruturadas em conhecimento útil e objetivo para os gestores das organizações.

Para que o conhecimento gerado maximize seu valor, este trabalho propõe a estruturação dos requisitos propostos na seção 3.3 de uma forma que possam ter enfoque também em controles, processos, pessoas e tecnologias, compondo uma matriz 3x4 que pode ser representada através da proposta apresentada na Figura 4.

Figura 4 – Estrutura proposta na análise correlacional, Fonte: CMU/SEI, 1993



Na dimensão controles-processos-pessoas-tecnologia o modelo proposto irá abordar:

a. Controles (o que): Relação dos objetivos de controle a serem aplicados;
b. Processos (como): Descrição dos processos necessários para implementação dos objetivos de controle;
c. Pessoas (quem): Papéis e responsabilidades dos indivíduos envolvidos com os processos e objetivos de controle definidos;
d. Tecnologia (ferramentas): Identificação das ferramentas automatizadas de apoio à implementação dos processos e do sistema de informação gerencial.

Nos níveis operacional-tático-estratégico o modelo se refere a:

a. Operacional: Atividades diárias, cotidianas e reativas;

b. Tático: Atividade proativas com revisões periódicas, busca contínua pela qualidade e possibilidade de planejamento em longo prazo;
c. Estratégico: Gerar conhecimento para permitir a visão organizacional para as questões de segurança computacional a partir de avaliações, auditorias, definição de níveis de maturidade dos objetivos de controle definidos e processos de extração de conhecimento de base de dados.

Na Tabela 3 é apresentada a correlação entre os requisitos propostos para um modelo correlacional e as estratégias propostas neste trabalho para sua implementação.

Tabela 3 – Proposta de estratégia para implementação dos requisitos identificados neste trabalho

Requisitos mapeados neste trabalho	
1. Os CEOs (Chief Executive Officers) precisam ter um mecanismo para conduzir uma avaliação periódica sobre segurança da informação, revisar os resultados com sua equipe e comunicar o resultado para a mesa diretora.	Modelo COBIT
2. CEOs precisam adotar e patrocinar boas práticas corporativas para segurança computacional, sendo municiados com indicadores objetivos que os façam considerar a área de segurança computacional como um importante centro de investimentos na organização, e não apenas um centro de despesas.	Modelo COBIT e Modelo ITIL
3. Organizações devem conduzir periodicamente uma avaliação de risco relacionada à informação como parte do programa de gerenciamento de riscos.	Modelo COBIT e Análise de Risco
4. Organizações precisam desenvolver e adotar políticas e procedimentos baseados na análise de risco para garantir a segurança da informação.	Modelo COBIT e norma ISO 17799
5. Organizações precisam estabelecer uma estrutura de gerenciamento da segurança para definir explicitamente o que se espera de cada indivíduo (papéis e responsabilidades).	Modelo ITIL expandido
6. Organizações precisam desenvolver planos e iniciar ações para prover a segurança adequada para a rede de comunicação, os sistemas e a informação.	Modelo ITIL (gerência de continuidade)
7. Organizações precisam tratar segurança da informação como parte integral do ciclo de vida dos sistemas.	Modelo COBIT e Modelo ITIL
8. Organizações precisam divulgar as informações sobre segurança computacional, treinando e educando os indivíduos.	Modelo ITIL expandido
9. Organizações precisam conduzir testes periódicos e avaliar a eficiência das políticas e procedimentos relacionados a segurança da informação.	Modelo COBIT e modelo ITIL
10. Organizações precisam criar e executar um plano para remediar vulnerabilidades ou deficiências que comprometam a segurança da informação.	Modelo ITIL expandido
11. Organizações precisam desenvolver e colocar em prática procedimentos de resposta a incidentes.	Modelo ITIL expandido
12. Organizações precisam estabelecer planos, procedimentos e testes para prover a continuidade das operações.	Modelo COBIT e Modelo ITIL

13. Organizações precisam usar as melhores práticas relacionadas à segurança computacional para medir a performance da segurança da informação.	Modelo COBIT, Modelo ITIL e norma ISO 17799

Considerando a estratégia de implementação dos requisitos identificados neste trabalho para o estudo correlacional das metodologias e normas, a Tabela 4 apresenta (visão macro) a proposta como resultado deste estudo.

Tabela 4 - Correlação da ISO 17799 com os modelos CobiT e ITIL

	Operacional	Tático	Estratégico
Controles	> ISO 17799 > COBIT: Entrega e suporte > COBIT: Aquisição e Implementação	> ISO 17799 > COBIT: Entrega e suporte	> ISO 17799 > Análise de Risco > COBIT: Auditoria > COBIT: Monitoramento > COBIT: Planej. e Organização
Pessoas	> ITIL: Suporte a Serviços (adaptado)	> ITIL: Entrega de Serviços (expandido)	> COBIT: Auditoria > COBIT: Monitoramento
Processos	> ITIL: Suporte a Serviços (adaptado)	> ITIL: Entrega de Serviços (expandido)	> COBIT: Auditoria > COBIT: Monitoramento
Tecnologia	> Ferramentas de Workflow > Ferramentas de Gerenciamento (coleta de dados) > Data Warehouse	> Ferramentas de Workflow > Ferramentas de Gerenciamento (coleta de dados) > Data Warehouse > Ferramentas para testes de vulnerabilidade e penetração > Ferramentas para análise de logs	> Ferramentas automatizadas para análise de Risco > Ferramentas automatizadas para a extração de conhecimento

Este trabalho propõe a utilização dos modelos CobiT e ITIL pelo fato de possuírem uma coleção das melhores práticas para auxiliar a Governança da Tecnologia da Informação, compiladas a partir da experiência profissional e práticas de especialistas que desenvolvem suas pesquisas pelo mundo todo. Esses modelos são reconhecidos e adotados em larga escala internacionalmente. Uma vez que a norma ISO 17799 possui os objetivos de controle específicos e detalhados para o gerenciamento de segurança computacional, ela será utilizada como base para o modelo. Os objetivos de

controle relacionados às melhores práticas para segurança computacional serão identificados no modelo CobiT e serão utilizados para ampliar a abrangência da ISO 17799. A avaliação em níveis de maturidade proposta pelo CobiT para cada objetivo de controle irá incorporar à norma ISO 17799 a capacidade de obtenção de um processo contínuo de melhoria da qualidade da segurança computacional dos serviços de TI oferecidos.

Esses objetivos de controle, que são apresentados em alto nível pelo modelo CobiT e de forma detalhada pela norma ISO 17799, deverão ser mapeadas para os processos descritos no modelo ITIL. Dessa forma, este trabalho propõe que o modelo CobiT e a ISO 17799 sejam utilizados para fornecer o que (objetivos de controle) precisa ser implementado, enquanto o modelo ITIL será utilizado para detalhar como isso será feito através de seus processos no nível operacional e tático e ainda, quem será responsável por fazê-lo.

5.1. Aplicabilidade do estudo: *Continuidade do Negócio*

Requisito Associado: *Organizações precisam desenvolver e adotar políticas e procedimentos baseados na análise de risco para garantir a segurança da informação.*

Uma análise de risco é proposta para ser realizada no nível estratégico de forma a apontar, com base no planejamento estratégico da organização, quais requisitos de controle devam ser implementados e o nível de maturidade esperado para cada um deles. A análise de risco irá fornecer conhecimento aos gestores para que identifiquem a necessidade de investimento em medidas para eliminar os riscos envolvidos na execução do planejamento estratégico.

Abrangência dos procedimentos:

- Levantamento do ambiente de TI corporativo, políticas e procedimentos em uso, mapeamento das políticas formais e informais, procedimentos de segurança e do ambiente de TI;
- Diagnóstico dos aspectos de segurança lógica e física: procedimentos para gerenciamento de acessos a rede e sistemas; antivírus; criptografia; gerenciamento do inventário de software; controle de acesso físico e ambiental; movimentação de ativos de TI;
- Revisão dos procedimentos de contingência;
- Testes de invasão, internos e externos;
- Gerenciamento e tratamento dos riscos através de ações para adequar o ambiente de TI às necessidades de negócios da organização, e conseqüentemente, diminuir o nível de exposição a riscos.

Resultado previsto:

- Relatório detalhado contendo a descrição das atividades efetuadas, a identificação dos riscos e vulnerabilidades encontradas, a classificação de risco e impacto no negócio, e recomendações de solução em curto, médio e longo prazo, mediante a análise dos riscos, controles e níveis de exposição.

Principais Benefícios:

- Gerenciamento formal dos riscos que posteriormente pode ser utilizado para obtenção de certificações internacionais;
- Mapeamento da situação real de exposição dos ativos de informação;
- Implementação de controles e mecanismos de segurança apropriados;
- Adoção de soluções baseadas em medidas preventivas;
- Definição e atribuição de responsabilidades.

6. Conclusão

Este trabalho apresentou a proposta de um estudo correlacional dos Modelos CobiT e ITIL e a Norma ISO 17799 para o tema Segurança da Informação utilizando como base a Estrutura de Decisão dos Sistemas de Informações Gerenciais (SIGs), dividida em nível operacional, nível tático e nível estratégico. A motivação para a utilização dessa estrutura surgiu na identificação de que a dificuldade de extração de conhecimento para a tomada decisão a partir de um grande volume de dados é comum tanto nas decisões relacionadas a negócios (onde geralmente são utilizados os SIGs) quanto no gerenciamento de segurança computacional.

A necessidade apontada pelas organizações de se alcançar um modelo onde o conhecimento relacionado às questões de segurança computacional esteja disponível de forma objetiva para o conselho administrativo ao longo de todo o processo de tomada de decisão para a execução negócio, conduziu este trabalho a considerar as questões de Governança da Tecnologia da Informação.

Para o desenvolvimento deste estudo, foram identificados e apresentados alguns requisitos. Esses requisitos foram mapeados numa estrutura matricial que contempla os níveis de decisão (operacional, tático e estratégico) e as dimensões que amparam cada um desses níveis de decisão (Controle, Processos, Pessoas e Tecnologia). Considerando essa estrutura matricial, que possui uma abrangência ampla, foi possível o desenvolvimento de um modelo que permite o alinhamento estratégico entre Segurança da Informação e o Negócio da Organização.

O modelo apresentado considerou a utilização das melhores práticas dos principais modelos de apoio à Governança de TI em função desses modelos terem sido desenvolvidos por especialistas, testados e implementados por uma grande quantidade de organizações ao redor do mundo. A estrutura matricial do modelo desenvolvido irá permitir a definição de níveis de maturidade isoladamente para controles, processos, pessoas e tecnologia em

cada um dos níveis de decisão. Isso facilitará a evolução do modelo e permitirá que as falhas sejam atacadas de forma pontual.

A combinação do modelo CobiT com a norma ISO 17799 e o modelo ITIL permitirá a utilização das potencialidades de cada uma dessas propostas para o desenvolvimento de um modelo único que facilite identificar: o que, quem, como e que recursos tecnológicos utilizar para o alcance da Governança Corporativa.

7. Referências bibliográficas

ABNT – Associação Brasileira de Normas e Técnicas. Tecnologia da informação – Código de prática para a gestão da segurança da Informação. NBR ISO/IEC 17799. 30/09/2001.

BSA - BUSINESS SOFTWARE ALLIANCE. Information Security Governance: Toward a Framework for Action. October 2003. Disponível on-line em http://www.bsa.org/usa/research/. Visitado em 05/12/2006.

CGTFR-CORPORATE GOVERNANCE TASK FORCE REPORT. Information Security Governance: A Call to Action.April, 2004. Disponível on-line em: http://www.cyberpartnership.org/InfoSecGov4_04.pdf. Visitado em 05/12/2006.

ENTRUST. Information Security Governance (ISG): An Essential Element of Corporate Governance. April, 2004. Disponível on-line em: http://www.entrust.com/governance/. Visitado em 08/12/2006.

ISO-International Organization for Standardization/ International Eletrotechnical Committee. Information technology- Code of practice for information security management. Reference number ISO/IEC 17799:2000(E).

OGC-Office of Government Comerce. ITIL: The Key to Managing IT Services – Best Practice for Service Support. Printed in the United Kingdom for the Stationery Office, 2001. ISBN0 11 330015 8.

OGC. IT Infrastructure Library: Planning to Implement ServiceManagement. London: OGC, 2002.

PAULK, M.C.; CURTIS, B; CHRISSIS, M.B.;WEBER, C.V. Capability Maturity Model for Software, version 1.1. Technical Report, Carnegie Mellon Software Engeneering Institute, CMU/SEI-93-TR-024, February 1993. Disponível on-line em: http://www.sei.cmu.edu/cmm/. Visitado em 11/30/2006.

IIA-THE INSTITUTE OF INTERNAL AUDITORS. Information Security Governance: What Directors Need to Know. (2001). The Critical Infraestructure Assurance Project. ISBN 0-89413-457-4. Disponível on-line em http://www.theiia.org/. Visitado em 11/30/2006.

ITGI-THE IT GOVERNANCE INSTITUTE.COBIT: Control Objectives for information and related Technology. Printed in the United States of America, 2000. ISBN: 1- 893209-13-X.

ITGI-THE IT GOVERNANCE INSTITUTE. Information Security Governance: Guidance for Boards of Directors and Executive Management. Printed in the USA, 2001. ISBN 1-893209-28-8. Disponível on-line em: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=6672. Visitado em 12/12/2006.

RUDD, Colin. An Introductory Overview of ITIL. Publicado por iTSMF ltd, Webbs Court, United Kingdom, 2004. Version 1.0a. Disponível online em: http://www.itsmf.com/publications/ITIL/Overview.pdf. Visitado em 30/11/2006.

VAN GREMBERGEN, Wim. Strategies for Information Technology Governance. Idea Group Publishing, 2003. ISBN 1-591140-140-2.

WEILL, Peter; Ross, Jeanne W. IT Governance: how top performers manage IT decision rights for superior results. Harvard Business School Publishing, 2004. ISBN 1-59139-253-5.

MC Bernardes, E dos Santos Moreira. UM MODELO PARA INCLUSÃO DA GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO. Disponível em: http://scholar.google.com/url?sa=U&q=http://www.linorg.cirp.usp.br/SSI/SSI2005/artigos/14275.pdf. Acesso em: 30/11/2006

WEILL, Peter; Ross, Jeanne W. Governança de TI: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores. M. Books do Brasil Editora Ltda, 2006. ISBN 85.89384-78-0.

SORTICA, Eduardo Almansa, CLEMENTI, Sérgio, CARVALHO, Tereza Cristina Melo Brito. Governança de TI: Comparativo entre COBIT E ITIL. Artigo Técnico. Congresso Anual de Tecnologia da Informação – FGV-EAESP. São Paulo, 2004. 14 p.

GHERMAN, Marcelo. Principais caracteristicas do framework COBIT. São Paulo: Sicurezza, 2005. MODULO SECURITY. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=459&pagenumber=0&idiom=0 . Acesso em: 11/12/2006