Gislaine Henriques Moraes

Modelos e Metodologias de Gestão de TIC para Obtenção da Governança da Segurança da Informação

Monografia apresentada ao PECE - Programa de Educação Continuada da Universidade de São Paulo, para a obtenção do Certificado de Especialização em Tecnologia da Informação – MBA/USP.

Orientador: Prof. Dr. Mauro César Bernardes

São Paulo - SP
2009

DEDICATÓRIA

Ao meu esposo Sidnei e ao meu filho
Gustavo por todo amor, carinho e
compreensão, os quais me
proporcionaram paciência e
persistência para concluir este trabalho
que coincidiu com uma fase muito
difícil da minha vida.

AGRADECIMENTOS

A Deus,

Por me proporcionar este momento e estar sempre presente em minha vida, segurando em minhas mãos, me dando forças e coragem para seguir em frente.

Ao Prof.: Dr. Mauro Cesar Bernardes,
Pelas orientações, diretrizes, paciência e por toda a atenção e incentivos prestados ao longo da realização deste trabalho.

Ao meu pai Felix e a minha mãe Josefa,
Os maiores responsáveis por eu chegar até aqui, que com simplicidade me educaram e me ensinaram os valores mais preciosos: sinceridade e honestidade.

Ao meu esposo Sidnei,
Companheiro de todas as horas, pelo seu amor, incentivo e paciência.

Ao meu filho Gustavo,
Razão da minha vida, por entender os momentos em que precisei estar ausente num período muito importante de nossas vidas.

A minha vozinha Marcionila (*in memorian*),
Pelo seu amor incondicional que, em vida, me ensinou a amar e respeitar o próximo.

Aos amigos Everaldo, Márcia, Marilda, Flávio, Fábio e Stênio,
Que em muitos momentos de dificuldades, sempre me apoiaram e me deram forças para continuar seguindo em frente para vencer este desafio.

RESUMO

A busca crescente na melhoria dos serviços como um diferencial competitivo no mercado fez com que as organizações passassem a considerar a necessidade de um melhor gerenciamento relacionado à Tecnologia da Informação e Comunicação (TIC). Além disso, o alinhamento entre TIC e as estratégias das organizações se faz necessário para o melhor aproveitamento das questões relacionadas a essa área. Enquanto as organizações se tornam cada vez mais dependentes da TIC, percebe-se um aumento de vulnerabilidades e riscos pertinentes a esta área. Isso tem direcionado os administradores que ocupam posições estratégicas a incluírem em suas decisões questões relacionadas à Segurança da Informação.

Uma vez que a Governança da Segurança da Informação é considerada uma responsabilidade desses administradores executivos, ela passa a ser um subconjunto da Governança de TIC e consequentemente da Governança Organizacional.

Diante deste cenário, percebe-se nas organizações a necessidade de investir em modelos e metodologias para um melhor gerenciamento da TIC, entre eles: o ITIL, o COBIT, o *Balanced ScoreCard* e a Norma ISO 17799 (27001). A utilização desses modelos e metodologias direciona a organização no alcance de um controle mais eficaz dos recursos e processos que contribuirão para redução de riscos, além da melhoria na análise dos indicadores desses benefícios aos seus usuários e clientes.

Neste trabalho serão analisados estes modelos e metodologias em busca das melhores práticas que possam ser aplicadas a um *framework* de Governança da Segurança da Informação. Serão investigadas as potencialidades de modelos e metodologias existentes atualmente, de forma que elas possam ser combinadas para atender aos requisitos necessários para a Governança da Segurança da Informação.

Para o desenvolvimento do *framework*, a segurança da informação foi considerada não apenas uma questão técnica, mas um desafio organizacional e de governança que envolve risco, indicadores, gerenciamento e estratégias.

ABSTRACT

The search for service improvement as a competitive differential in the market has forced organizations to consider the need for better management as far as Information and Communication Technology (ICT) is concerned. Furthermore, the alignment between ICT and the strategies of such organizations is vital as it enables a better understanding of the issues related to this area. Whilst the organizations become more and more dependent on ICT, an increase in the vulnerability and risks inherent to this field is perceived. This scenario has directed professionals in strategic positions to consider the questions related to information security when taking their decisions.

Hence, as it is considered part of the responsibilities of executive administrators, the information security governance is now an integrant element of corporate governance, and it needs to be aligned with the ICT governance.

Given the situation above, the necessity to invest on models and methodologies such as ITIL, COBIT, Balanced Scorecard, and ISO 17799 (27001), envisaging the enhancing the management o ITC, comes to light. The application of these models and methodologies not only drives the organization to a more effective level of control of the processes and resources that will contribute to the risk reduction, but it will also allow a better analysis of the indicators of the out coming benefits of such practices to their users and clients.

In this work the models and methodologies mentioned previously will be analyzed with a view to defining the best practices that could be applied to a framework of Information Security Governance. The potentiality of current existing models and methodologies will be analyzed and combined to attend the necessary requirements of the Information Security Governance.

During the development of this framework, Information Security was considered not only a technical question, but also an organizational and managerial challenge that involves risk, indicators, management and strategies.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. Introdução

Nos últimos anos a informação vem sendo cada vez mais reconhecida como um recurso estratégico e um diferencial competitivo para as organizações, assumindo valores econômicos e sociais e impondo a necessidade de ser gerenciada corretamente.

Com o desenvolvimento dos setores da Tecnologia da Informação e Comunicação (TIC), as informações tornaram-se mais difusas, ensejando mais oportunidades e ao mesmo tempo, riscos para as organizações. O crescimento contínuo da digitalização das informações e a maciça utilização da Internet se contrapõem à grande diversidade e ao compartilhamento de técnicas de ataque e invasão e o conseqüente aumento no número de invasões.

Analisando o cenário atual, é possível perceber o crescente aumento das tentativas de fraudes virtuais no Brasil e no mundo, comprometendo a segurança da informação. Segundo o Cert.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, em 2008 houve um aumento de cerca de 39% no número de incidentes quando comparado ao ano anterior (IDGNOW!, 2008f).

Em março de 2008 o país ocupava a oitava posição em um ranking sobre a ocorrência de ataques, elaborado pela empresa Kaspersky. Dois meses depois, passou a ocupar a quinta posição. Segundo a pesquisa, o posicionamento do Brasil no topo do ranking deve-se à facilidade da inclusão digital, ao aumento da participação da classe C na Internet brasileira, à falta de experiência dos novos usuários e da fragilidade na legislação brasileira contra *cibercrimes* (IDGNOW!, 2008c).

É possível identificar que as organizações estão de certa forma vulneráveis aos mais variados tipos de ataques, tornando-as cada vez mais dependentes do correto funcionamento da infra-estrutura de TIC e buscando, aumentar a confiabilidade dos serviços de TIC para a realização dos negócios das organizações.

Diante deste cenário, o gerenciamento correto das questões relacionadas à segurança da informação tornou-se um requisito estratégico para se alcançar o nível de segurança desejável.

Paralelamente percebeu-se a necessidade de gerenciar a TIC de forma a manter uma infra-estrutura segura e confiável. Para alcançar um controle mais eficaz dos recursos e processos que contribuirão para redução de riscos e análise dos indicadores desses benefícios aos seus usuários e cliente, foram desenvolvidos modelos e metodologias que auxiliariam o gerenciamento de TIC, entre eles o ITIL, o COBIT, o *Balanced ScoreCard* e a Norma ISO 17799 (27001). Esses modelos e metodologias estão sendo utilizados nas organizações em auxílio à obtenção da Governança de TIC.

Entretanto, extrapolando a Governança de TIC, a informação passou a exigir um gerenciamento diferenciado para proteção contra os riscos relacionados ao seu uso. Considerando que a Segurança da Informação possui algumas particularidades, as organizações buscaram um modelo que a tratasse de forma diferenciada, tornando-a parte integrante do planejamento estratégico e, dessa forma, estabelecendo a necessidade da Governança da Segurança da Informação.

1.1. Objetivo

O objetivo deste trabalho é investigar as potencialidades de modelos e metodologias existentes atualmente para o alcance da Governança de TIC de forma que elas possam ser combinadas para atender aos requisitos necessários para a Governança da Segurança da Informação.

1.2. Metodologia

Neste trabalho serão analisadas estas particularidades em busca das melhores práticas que possam ser aplicadas ao Modelo de Governança da Segurança da Informação apresentado em Bernardes (2005).

Para o desenvolvimento desse trabalho serão investigados os modelos que definem as "melhores práticas" para a gestão de TIC, por meio dos processos definidos no ITIL, do Guia de Maturidade do COBIT, do modelo organizacional *Balanced Scorecard* e das diretrizes definidas nas normas ISO 17799 (27001).

Com o correlacionamento desses modelos e metodologias pretende-se demonstrar como poderão ser exploradas suas potencialidades para o auxílio na área de Segurança da Informação e para a ampliação do modelo de Governança da Segurança da Informação apresentando naquele trabalho.

Assim, esta monografia está organizada da seguinte forma:

No capítulo 1 serão apresentados os conceitos que envolvem a segurança da informação e algumas formas de ataques e invasões reportados ao Cert.br, que comprometem a segurança da informação.

No capítulo 2 será apresentada uma revisão de literatura sobre Governança da TIC e sobre os principais modelos e metodologias de apoio, como: ITIL, COBIT, BSC e ISO 17799 (27001).

No capítulo 3 será apresentada uma combinação entre os modelos e metodologias citados no capítulo 2 para obtenção de uma Governança da Segurança da Informação, que constitui a proposta apresentada neste trabalho.

No capítulo 4 serão apresentadas as conclusões para este trabalho.

2. Segurança da Informação

O termo Segurança da Informação abrange as políticas, procedimentos e medidas técnicas usadas para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação. Ela pode ser oferecida por um conjunto de técnicas e ferramentas que tem como objetivo proteger hardware, software, redes de comunicação e dados (Laundon & Laundon, 2004).

Com o desenvolvimento da TIC, a informação assumiu *status* de ativo principal das organizações. Essa crescente valorização da informação tem influenciado na Segurança da Informação, que hoje é considerada uma necessidade estratégica que interfere na capacidade com que as organizações realizam suas atividades com eficiência e eficácia (Laia & Lara, 2007).

Em relação à Segurança da Informação, é importante entendermos três conceitos básicos: *confidencialidade*, *integridade* e *disponibilidade*. Há ainda outros três conceitos que são relacionados às pessoas: *autenticidade*, *autorização* e *irretratabilidade* ou *não repúdio,* conforme apresentado a seguir:

- *Confidencialidade*: garantia de que o acesso às informações somente é possível por pessoas autorizadas.
- *Integridade*: garantia da não violação da informação e dos métodos de seu processamento.
- *Disponibilidade*: garantia de que os usuários autorizados, sempre que necessário, obtenham acesso às informações e aos recursos computacionais.
- *Autenticidade:* garantia de que a informação é de fato originária da procedência alegada.
- *Autorização*: ato que garante se um usuário tem o direito de executar certa atividade.
- *Irretratabilidade ou não repúdio*: garantia de segurança que impede uma entidade participante numa dada operação de negar essa participação.

"Segurança da Informação é a proteção de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ABNT, 2001).

2.1. Invasões e comprometimento da Segurança da Informação

Atualmente, com a facilidade de se conseguir informações e ferramentas relacionadas a ataques, houve um aumento na disseminação de incidentes envolvendo usuários não especializados que são capazes de acionar um servidor de busca e ter acesso a informações detalhadas sobre técnicas de invasão.

Por outro lado, há o Cert.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, que analisa e responde as notificações de incidentes enviadas por usuários e administradores de redes, ajudando a diminuir o número de incidentes. Essas notificações refletem os incidentes e os vários tipos de ataques ocorridos e permitem ao Cert.br manter as estatísticas a ele reportados.

A partir da análise da figura 1 é possível identificar um aumento no número de incidentes reportados ao grupo de resposta a incidente do Cert.br na última década. Tal fato pode ser o resultado do crescimento no número de vulnerabilidades, ou seja, falhas computacionais que, uma vez exploradas, levam à ocorrência de incidentes.

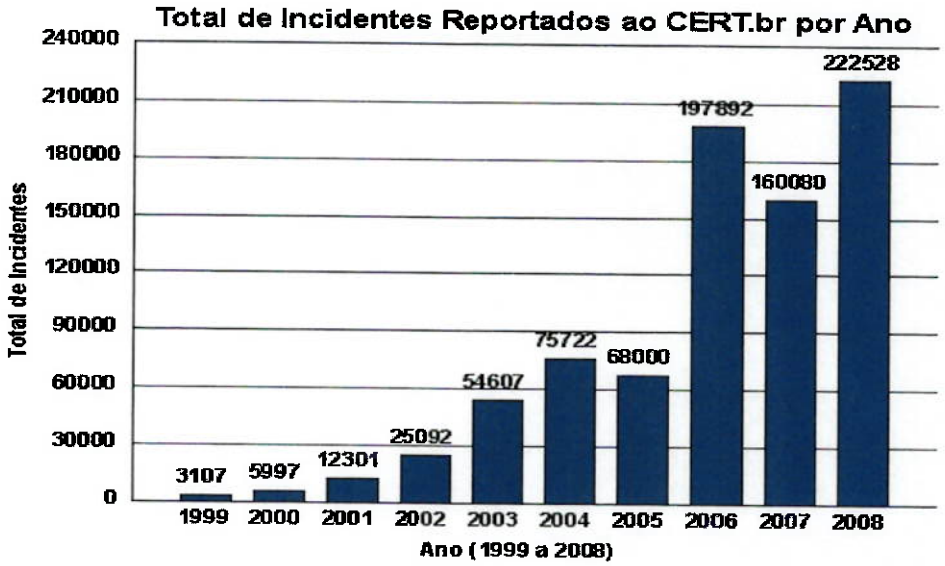

Figura 1 - Incidentes reportados ao CERT.br 1999 a 2008 (CERT.br 2008a)

Segundo Demi Getschko, integrante do Comitê Gestor da Internet no Brasil, em 2006 houve um aumento de incidentes reportados ao Cert.br, devido ao crescimento da sofisticação das fraudes bancárias e financeiras e dos ataques na Internet (NIC.br, 2006b).

O *spam*, termo usado para referir aos *e-mails* não solicitados, também foi um dos motivos do aumento de incidentes em 2006. O CERT.br, divulgou dados onde apontam que 286,7 mil mensagens não solicitadas foram reportadas no mês de janeiro de 2006, enquanto que em 2005 foram cerca de 2,4 mil reclamações (NIC.br, 2006a).

É possível observar que no ano de 2008 houve um aumento no valor das notificações recebidas pelo Cert.br em relação ao ano de 2007. De acordo com o Cert.br quase 89 mil incidentes relacionados a fraude foram registrados apenas no quarto trimestre de 2008 (IDGNOW!, 2008f).

No ano de 2007 é possível observar uma queda no número de incidentes. Isso se deve ao fato de que as notificações relacionadas à propagação de *worms* e *bots* caíram em relação ao ano anterior e ainda à redução de 26% nas tentativas de fraudes financeiras (NIC.br, 2008).

2.2. Formas de ataques

A Segurança da Informação vem se tornando cada vez mais um assunto de vital importância dentro das grandes organizações. Isso se deve ao grande índice de incidentes e ao grande valor da informação nestes últimos anos.

Diante das facilidades de conexão com a Internet, o acesso à informação tornou-se alvo fácil para vários tipos de ameaças. Pode-se observar na figura 2, alguns tipos de ataques reportados ao Cert.br no ano de 2008.

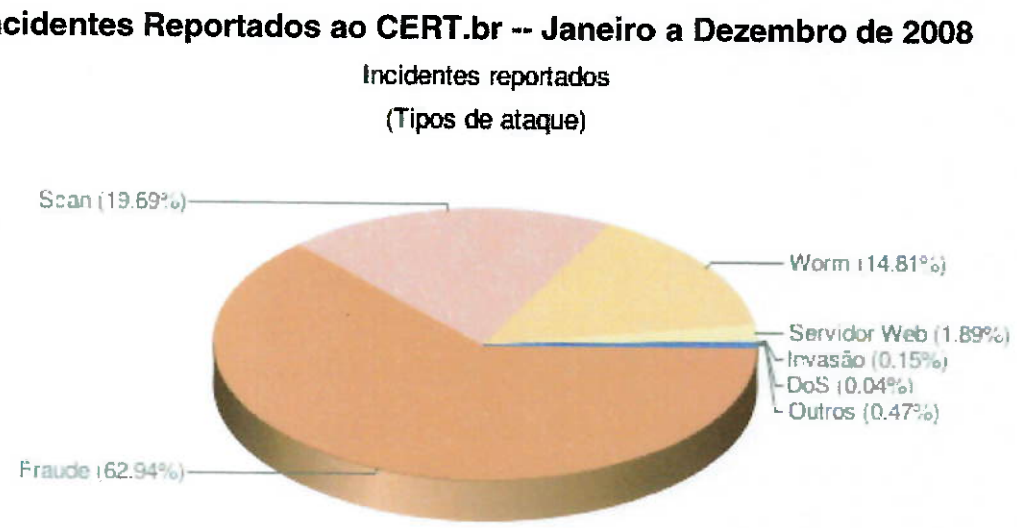

Figura 2 - Tipos de ataques reportados ao CERT.br janeiro a dezembro de 2008 (CERT.br 2008b)

Analisando o gráfico, é possível identificar que os ataques citados como fraude, *scan* e *worm*, são as principais ameaças reportadas neste período.

Segundo o Cert.br, o aumento do índice de fraudes na Internet brasileira no segundo trimestre de 2008, foi impactado devido às notificações de casos de ataques por meio de cavalo-de-tróia e circulação de arquivos protegidos por direitos autorais (IDGNOW!, 2008e).

Outro ataque importante que deve ser citado como um colaborador para o aumento das fraudes é a Engenharia Social. No final de 2006 Graham Cluley, consultor sênior em tecnologia da Sophos, empresa especializada em programas de antivírus, informou que o maior problema, tanto para usuários domésticos como também os corporativos, seria o upgrade na mente das pessoas para aumentar os seus conhecimentos em relação à computação, sensibilizando os usuários em suas ações (IDGNOW!, 2006).

A vulnerabilidade humana tornou-se alvo fácil de ataques por meio da Engenharia Social. O atacante se faz passar por outra pessoa e utiliza meios, como *email* ou ligação telefônica, para persuadir o usuário a fornecer informações ou realizar determinadas ações (CERT.br,2006).

Outro tipo de incidente está relacionado aos *botnets* responsáveis por 31,4% das fraudes em anúncios on-line no quarto trimestre do ano de 2008 (IDGMOW!, 2008a).

Na figura 3, podemos verificar dados referentes a outro tipo de ataque que colocou o Brasil na segunda posição do *ranking* dos países que mais recebeu *spams*, segundo pesquisa realizada pela McAfee – SPAM *Experiment* (IDGNOW!, 2008b).

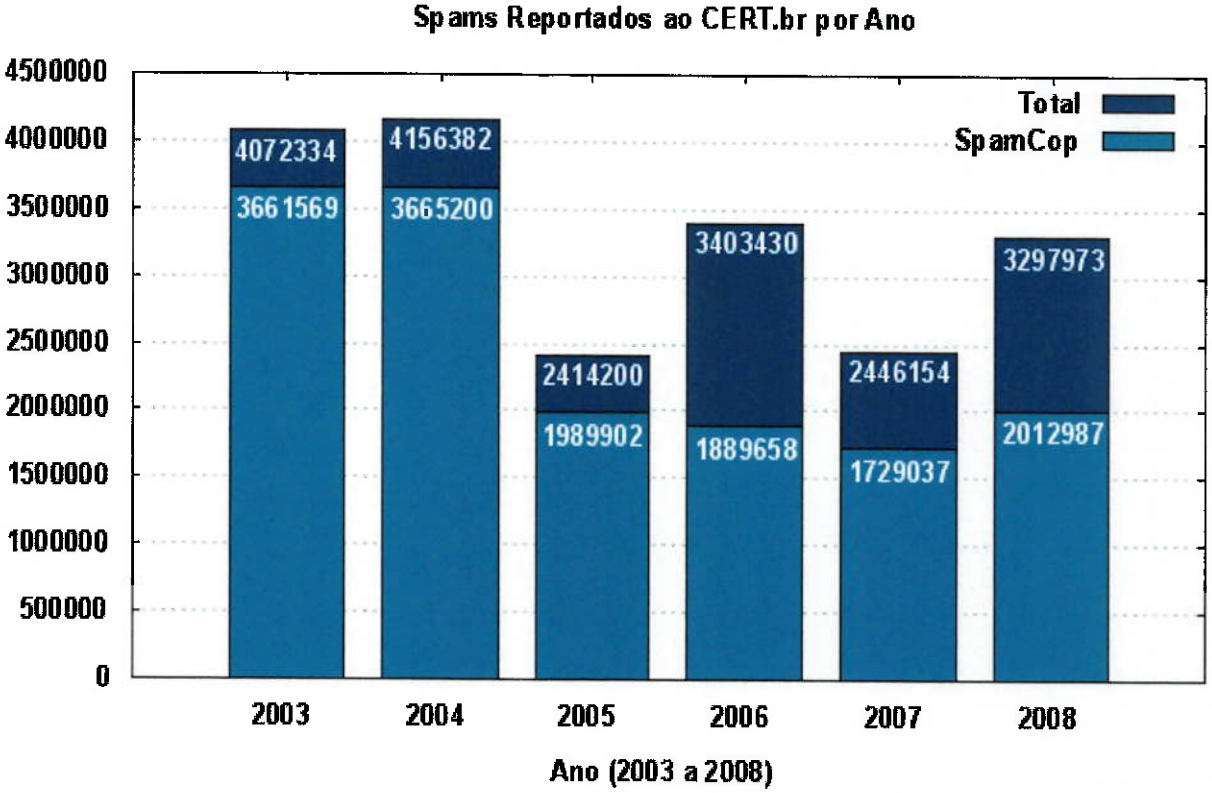

Figura 3 - Valores acumulados de spams: 2003 a 2008 (CERT, 2008c)

Fazendo uma análise em relação ao ano de 2008, é possível identificar um aumento nas tentativas de fraude na *web* brasileira, ano em que o país apresentou um aumento de 209% em comparação com o ano de 2007 e um aumento de 39% no número total de incidentes reportados ao Cert.br (IDGNOW!, 2008f).

Em função dessas vulnerabilidades, a informação passou a ser parte integrante do planejamento estratégico das organizações, e necessitava de um modelo de governança. Esse cenário motivou o surgimento do conceito de

Governança da Segurança da Informação, para alinhar as áreas de segurança e Tecnologia da Informação e Comunicação (TIC) com o negócio.

3. Governança de Tecnologia da Informação e Comunicação

A busca para tornar a informação um recurso estratégico aumentou a necessidade das organizações investirem em Tecnologia da Informação e Comunicação (TIC). Com o propósito de alcançar melhorias no desempenho, obtenção de vantagem competitiva e aumentar a participação no mercado, as organizações estão investindo em Governança de TIC.

Esses investimentos visam também a obtenção de informações precisas e na hora certa para facilitar a tomada de decisões e o aumento na economia de escopo, de modo que a organização atenda as necessidades abrangentes dos clientes sem aumento dos custos (ARRUDA & FILHO, 2006).

Algumas vezes, esses investimentos não são bem vistos pela alta direção das organizações, por duvidarem do retorno que proporcionam e dos reais benefícios da tecnologia. Entretanto, a ausência de investimentos pode causar o fracasso de um empreendimento. Diante desta situação, a Governança de TIC aparece como um processo estruturado para gerenciar e controlar as iniciativas de TIC das organizações, garantindo o retorno de investimentos e adição de melhorias nos processos de análise e risco e tomadas de decisões (FAGUNDES, 2004).

Dessa forma, a Governança de TIC tem como objetivos:

- Facilitar a tomada de decisões de TIC;
- Simplificar as operações e/ou serviços de TIC;
- Melhorar o nível de qualidade dos serviços de TIC;
- Estabelecer e manter relacionamento com clientes e fornecedores;
- Maximizar uso de recursos;
- Otimizar custos;
- Gestão de risco (identificar, analisar e mitigar);
- Estabelecer e manter a conformidade com as leis e regulamentos;
- Promover a integração entre Negócio e TIC;
- Gerar valor para empresa.

Para Bernardes (2005), Governança de Tecnologia da Informação e Comunicação é uma estrutura de relacionamento entre processos que dirige e controla uma empresa, alinhando a TIC de acordo com as necessidades da organização.

Em Weill e Ross (2006) Governança de TIC é: "a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização da TIC".

Com a adoção de um modelo de Governança de TIC, espera-se que as estruturas e processos garantam que a TIC suporte e maximize os objetivos e estratégias da organização permitindo controlar a medição, auditagem, execução e a qualidade dos serviços (ARRUDA & FILHO, 2006).

Como forma de alcançar a Governança de Tecnologia da Informação e Comunicação, modelos e metodologias de boas práticas de gestão foram propostos por vários organismos de âmbito mundial, entre eles podemos citar ITIL e COBIT.

Paralelamente, percebe-se a necessidade de uma atenção especial para as questões relacionadas à segurança da informação para se obter o sucesso no gerenciamento da Segurança da Informação. Alguns estudiosos apontam a necessidade e a importância de se obter uma Governança da Segurança da Informação. Como forma de estruturação, é proposto um modelo onde a segurança da informação passa a ser parte integrante do planejamento estratégico das organizações.

Neste trabalho, serão investigadas as potencialidades dos modelos ITIL e COBIT, da metodologia BSC e da norma ISO 17799 (27001) de forma que elas possam ser combinadas para atender aos requisitos necessários para a Governança da Segurança da Informação e Comunicação.

3.1. Modelo ITIL

À medida que as organizações tornaram-se mais dependentes da área de Tecnologia da Informação e Comunicação para satisfazer os objetivos do negócio, foi percebido que investir em maior qualidade de serviços de TIC e sua gestão seria um fator importante para se tornar mais competitivo no mercado.

O modelo ITIL (*Information Technology Infrastructure Library*), foi desenvolvido na Inglaterra pela *Central Computer and Telecommunication Angency* (CCTA), agora *Office of Government Commerce*, no final da década de 80, com a necessidade de ter processos organizados e melhores práticas na área de Tecnologia da Informação e Comunicação.

Composto por um conjunto de melhores práticas, o objetivo do ITIL é suporte e gerenciamento da infra-estrutura. Também visa fornecer serviços com maior qualidade e custos desejáveis aos clientes de Tecnologia de Informação e Comunicação.

O modelo ITIL, que em português quer dizer, Biblioteca de Infra-estrutura de Tecnologia de Informação, foi desenvolvido com o objetivo de alinhar TIC aos negócios da organização. Aborda o gerenciamento do software e a sua implantação, o suporte e gestão dos serviços prestados, o gerenciamento da infra-estrutura de TIC, o gerenciamento de aplicações e o gerenciamento de segurança (ZORELLO, 2005).

Além de auxiliar as organizações no gerenciamento da infra-estrutura de serviços eficientes, as melhores práticas do ITIL provêem melhora na qualidade dos serviços prestados, redução de custos com a eliminação de tarefas redundantes e processos mais ágeis, otimizados e interligados (ESPILDORA, 2004).

Segundo Magalhães e Pinheiro (2007), o ITIL é composto por um conjunto das melhores práticas que definem os processos necessários ao funcionamento de

uma área de TIC com o objetivo de permitir o alinhamento entre a área de TIC e as demais áreas de negócio, conforme mostra a figura 4.

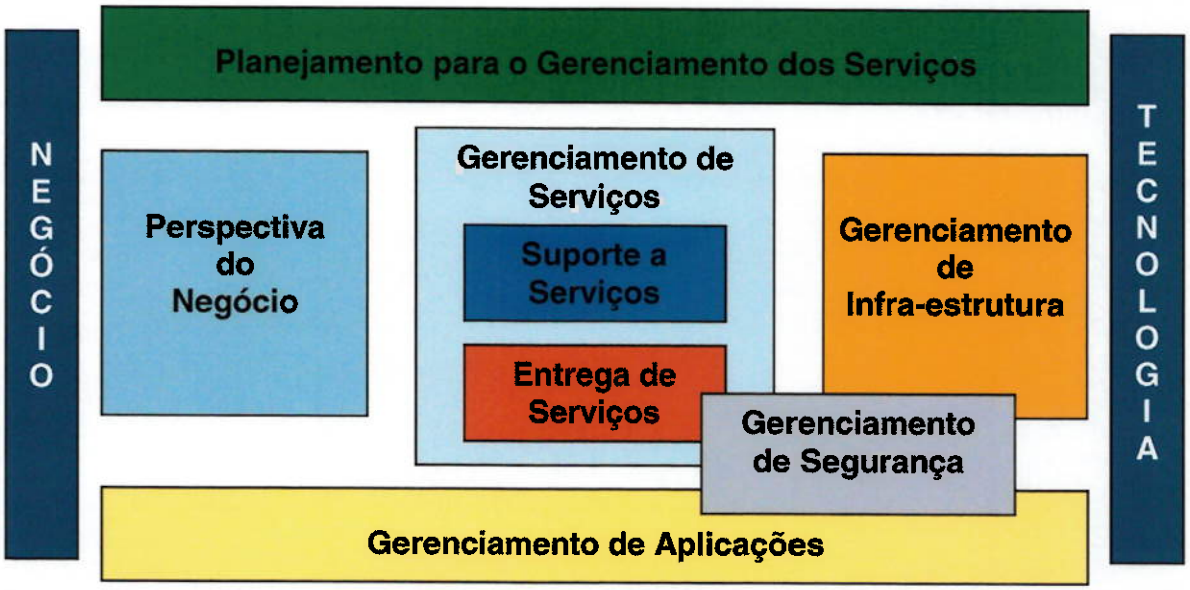

Figura 4 - Estrutura do ITIL

O Gerenciamento de Serviços de TIC se torna necessário para evidenciar o inter-relacionamento entre os processos do ITIL, assim, um processo não pode ser visto de forma isolada dos outros, facilitando desta forma a detecção de problemas a serem solucionados (MAGALHÃES & PINHEIRO, 2007).

A filosofia do ITIL é atender, por meio de suas melhores práticas, as necessidades de cada organização de forma estruturada, auxiliando a organização quanto à priorização da solução de incidentes, desafios e mudanças, impactando na qualidade dos serviços prestados.

Embora o ITIL tenha um módulo que trate do Gerenciamento de Segurança da Informação, ele apenas faz uma referência da norma ISO 17799 a cada processo do módulo Gerenciamento de Serviços.

O módulo de Gerenciamento de Serviços possui duas áreas em que os processos da ITIL são fundamentais para a sua operacionalização que são: Entrega de Serviços e Suporte a Serviços.

3.1.1. Entrega de Serviços (*Service Delivery*)

Os processos de entrega de serviços descritos pelo ITIL pertencem ao nível tático e concentram-se nas atividades de planejamento a longo prazo e na melhoria dos serviços entregues e em utilização pela organização. São eles: (MAGALHÃES & PINHEIRO, 2007).

- Gerenciamento de Nível de Serviço (*Service Level Management*)
  O processo de Gerenciamento de Nível de Serviço é o responsável pela imagem da área de TIC perante toda a organização. Este processo assegura que os serviços de TIC sejam entregues quando e onde as áreas usuárias definirem. Ele pode ser dividido nos seguintes sub-processos:
  - Revisão dos serviços disponibilizados;
  - Negociação com os clientes;
  - Revisão dos contratos de serviços com os fornecedores externos;
  - Desenvolvimento e monitoração dos acordos de nível de serviço;
  - Implementação das políticas e dos processos de melhoria contínua;
  - Estabelecimento de prioridades;
  - Planejamento do crescimento dos serviços;
  - Definição do custo dos serviços em conjunto com o gerenciamento financeiro e da forma de ressarcimento destes custos.

- Gerenciamento de Capacidade (*Capacity Management*)
  O processo de Gerenciamento de Capacidade é o responsável por tornar disponíveis os recursos de infra-estrutura no tempo certo, no volume e custo adequado. Ele pode ser dividido nos seguintes sub-processos:
  - Monitoração do desempenho;
  - Monitoração da carga de trabalho/demanda;
  - Dimensionamento da aplicação;
  - Projeto de recursos;
  - Projeto da demanda;
  - Estabelecimentos de modelos.

- Gerenciamento de Disponibilidade (*Availability Management*)

  O processo de Gerenciamento de Disponibilidade é o responsável por determinar a disponibilidade dos níveis de serviços de TIC a partir de requerimentos do negócio.

- Gerenciamento de Continuidade de Serviços de TIC (*IT Service Continuity Management*)

  O processo de Gerenciamento de Continuidade de Serviços de TIC é o responsável em validar os planos de contingência, recuperar e disponibilizar os serviços de TIC após ocorrer algum acidente de modo que a organização volte a operar mesmo após ocorrer algum desastre.

- Gerenciamento Financeiro (*Financial Management*)

  O processo de Gerenciamento Financeiro demonstrar para a organização o verdadeiro custo de todos os serviços de TIC para ser entendido e utilizado no processo de tomada de decisão.

3.1.2. Suporte a Serviços (*Service Support*)

Os processos desta área pertencem ao nível operacional e estão relacionados com tarefas diárias necessárias para a manutenção dos serviços de TIC. São eles: (MAGALHÃES & PINHEIRO, 2007).

- Gerenciamento de Configuração (*Configuration Management*)

  O processo de Gerenciamento de Configuração é o responsável pela criação da base de dados de gerenciamento de configuração (*Configuration Management Database – CMDB*) que é constituída pelos itens de configuração (*Configuration Items – Cis*) usados para o gerenciamento dos serviços de TIC. Um item de configuração pode ser um componente físico (microcomputador) ou lógico (software).

- Gerenciamento de Incidente (*Incident Management*)

  O processo de Gerenciamento de Incidente é o responsável pelo tratamento e resolução de incidentes nos serviços de TIC no menor tempo possível. Para sua operacionalização o gerenciamento de incidentes conta com o apoio da Central de Serviços que tem como foco principal gerenciar e comunicar incidentes.

- Gerenciamento de Problema (*Problem Management*)

  O processo de Gerenciamento de Problema é o responsável pela resolução de falhas que afetam o funcionamento dos serviços de TIC, garantindo a correção e prevenção de reincidências e realizando manutenções que garantam a redução de novas ocorrências.

- Gerenciamento de Mudança (*Change Management*)

  O processo de Gerenciamento de Mudança assegura que qualquer mudança no item de configuração (*Configuration Item*) possa ocorrer conforme planejado e autorizado, caso aconteça algum imprevisto.

- Gerenciamento de Liberação (*Release Management*)

  O processo de Gerenciamento de Liberação é o responsável por introduzir as mudanças no ambiente de infra-estrutura de TIC, uma vez que estas mudanças foram desenvolvidas, testadas e empacotadas para implementação.

3.2. Modelo COBIT

O COBIT (*Control Objectives for Information and Related Technology*) foi o principal produto de estudo do *Information Technology Governance Institute* (ITGI), com o objetivo de realizar pesquisas e estudos sobre o tema governança, proteção e segurança da Tecnologia da Informação e Comunicação (MARCIANO, 2007).

Desenvolvido pelo *Information System Audit and Control* (ISACA) e pelo ITGI, o COBIT é considerado a base da governança tecnológica e estabelece métodos

para guiar a área de tecnologia das organizações em relação à qualidade, níveis de maturidade e segurança da informação.

Sendo mais focado para o controle e menos para a execução, o COBIT estabelece métodos formalizados para guiar a área de TIC incluindo qualidade, níveis de maturidade e segurança da informação (BERNARDES, 2007).

O modelo COBIT apóia a Governança de TIC fornecendo um *framework* para assegurar que a TIC esteja alinhada com o negócio, também auxilia a organização fornecendo a informação necessária para atingir seus objetivos.

O COBIT está organizado em 34 processos de TIC, estruturados em 4 domínios: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoramento e Avaliação: (ISACA, 2007).

1) Planejamento e Organização:

Trata dos planos estratégicos e táticos e procura identificar como TIC pode contribuir melhor para atender as metas da empresa.
Processos:
P01 – Definição do planejamento estratégico TIC;
P02 – Definição da arquitetura da informação;
P03 – Determinação do direcionamento tecnológico;
P04 – Definição de Processo de TIC;
P05 – Gerenciamento de Investimentos de TIC;
P06 – Comunicação de objetivos e direcionamento;
P07 – Gerenciamento de recursos humanos de TIC;
P08 – Gerenciar qualidade;
P09 – Avaliar e gerenciar riscos de TIC;
P10 – Gerenciamento de Projetos.

2) Aquisição e Implementação:

Trata de todas as aquisições e implementações realizadas por TIC, pois, para atender a estratégia é preciso identificar, desenvolver ou adquirir, bem como implementar e integrar soluções de TIC.

Processos:

AI01 – Identificar soluções automatizadas;

AI02 – Aquisição e manutenção de sistemas e aplicativos;

AI03 – Aquisição e manutenção de tecnologia de infra-estrutura;

AI04 – Habilitar a operação e uso;

AI05 – Obter recursos de TIC;

AI06 – Gerenciar mudanças;

AI07 – Instalação, homologação de soluções e mudanças.

3) Entrega e Suporte:

O objetivo é entrega dos serviços, que inclui gerenciamento da segurança, gerenciamento da continuidade de serviços, suporte aos usuários, gerenciamento de dados e do ambiente operacional.

Processos:

DS1 – Definição de níveis de serviços;

DS2 – Gerenciamento de serviços de terceiros;

DS3 – Gerenciamento de performance e capacidade;

DS4 – Assegurar a continuidade dos serviços;

DS5 – Assegurar sistema de segurança;

DS6 – Identificar e alocar custos;

DS7 – Educar e treinar usuários;

DS8 – Gerenciar *Service Desk* e incidentes;

DS9 – Gerenciar configurações;

DS10 – Gerenciar problemas;

DS11 – Gerenciar dados;

DS12 – Gerenciar ambiente físico;

DS13 – Gerenciar operações.

4) Monitoramento e Avaliação:

Foca o gerenciamento do desempenho, monitoramento dos controles internos, conformidade com as regulamentações e governança.

Processos:

ME1 – Monitorar e avaliar o desempenho de TIC;

ME2 – Monitorar e avaliar controles internos;

ME3 – Assegurar *compliance* e contratos;

ME4 – Prover Governança de TIC.

Na figura 5, podemos identificar os quatro domínios do COBIT e a ligação entre os processos de negócio da organização, sete critérios da informação e quatro recursos de TIC.

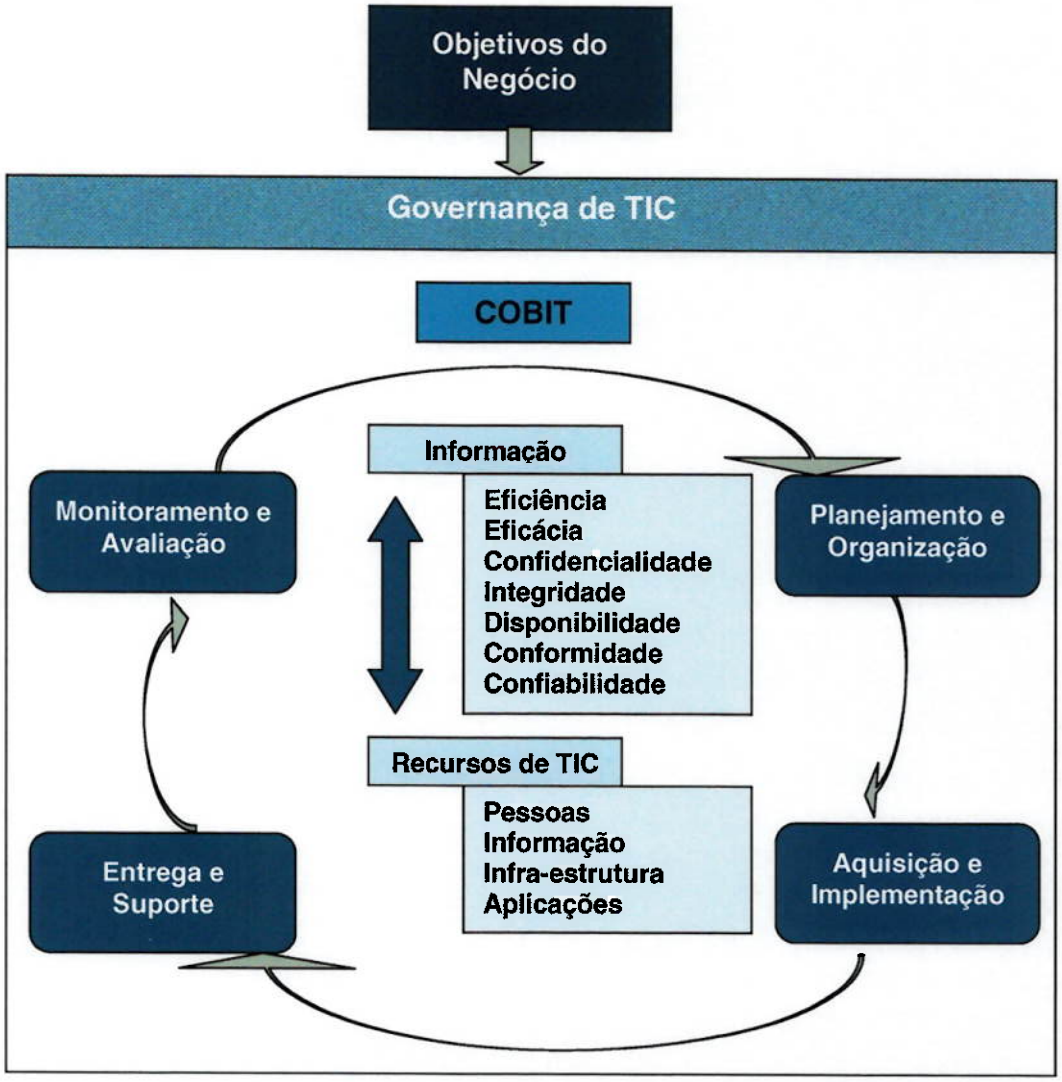

Figura 5 - Os quatro domínios do COBIT (Adaptado de FAGUNDES, 2004).

Para ajudar a área de TIC identificar o nível de maturidade e a evolução dos processos da organização, o COBIT, através de relatórios confiáveis, utiliza o modelo de auditoria CMMS (*Capability Maturity Model for Software*), conforme mostra a figura 6, que estabelece os seguintes níveis:

0) Inexistente: significa que o processo de gerenciamento não foi implementado;

1) Inicial: o processo implementado é realizado sem organização, de modo não planejado;

2) Repetitível: o processo é repetido de modo intuitivo, isto é, depende mais das pessoas do que de um método estabelecido;

3) Definido: o processo é realizado, documentado e comunicado na organização;

4) Gerenciado: existem métricas de desempenho das atividades, o processo é monitorado e constantemente avaliado;

5) Otimizado: as melhores práticas de mercado e automação são utilizadas para a melhoria contínua dos processos.

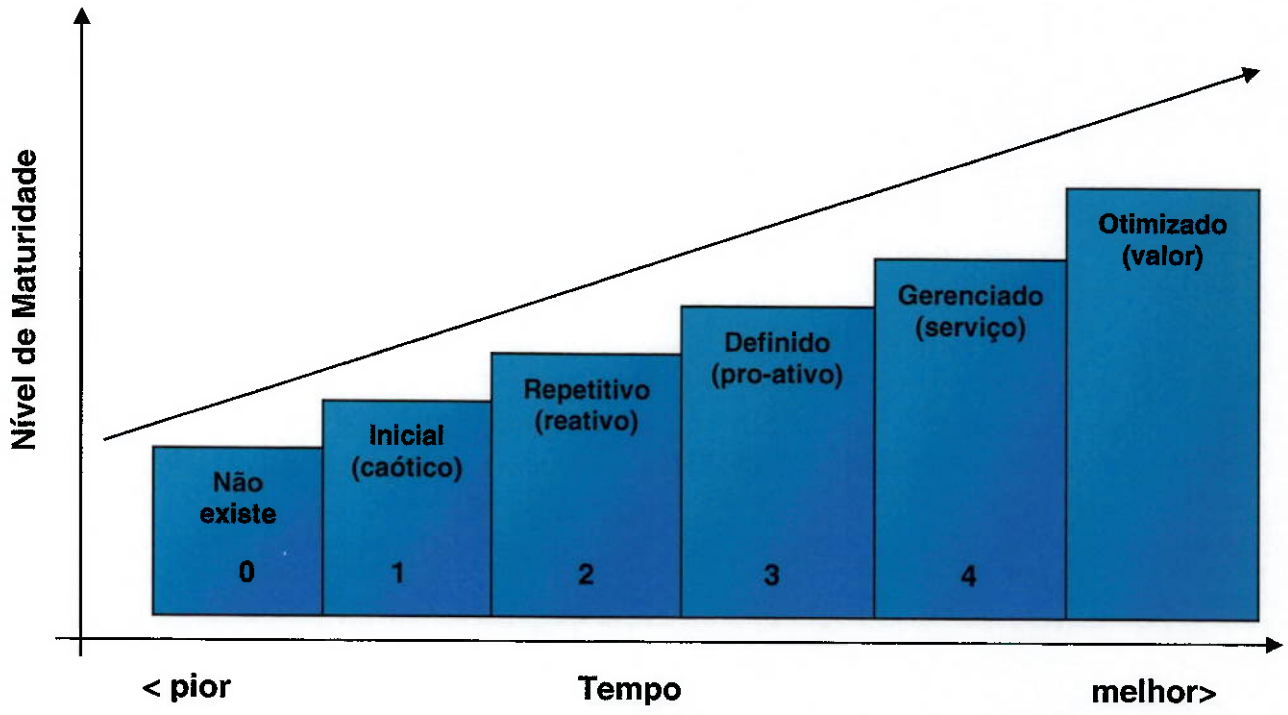

Figura 6 - Modelo de Maturidade dos Processos.

3.3. Metodologia *Balanced Scorecard* (BSC)

Os autores Kaplan e Norton, divulgaram em 1992 um sistema de medição e avaliação de desempenho das organizações, um sistema que anos mais tarde reconhecido pelos próprios autores como um sistema de gerenciamento de estratégias o qual denominaram *Balanced Scorecard* (COSTA, 2006).

Esses mesmos autores definiram o *Balanced Scorecard* como uma ferramenta que traduz a missão e a visão das empresas em um conjunto abrangente de medidas de desempenho que serve de base para um sistema de medição e gestão estratégica.

O objetivo do *Balanced Scorecard* (BSC) é permitir uma melhor gestão no desempenho organizacional baseando-se na visão estratégica e traduzindo-a em indicadores de desempenho.

Inicialmente, o BSC foi desenvolvido para ser um sistema de medição de desempenho, mas após algumas implantações foi possível verificar que o BSC era mais do que um sistema de indicadores e sim, um sistema capaz de comunicar e alinhar as estratégias das empresas (COSTA, 2006).

Com este novo conceito o BSC passou a ser compreendido como um Sistema de Gestão Estratégica, que viabiliza processos gerenciais críticos através de quatro perspectivas, a saber: perspectiva financeira, perspectiva do cliente, perspectiva dos processos internos e perspectiva de aprendizado e crescimento.

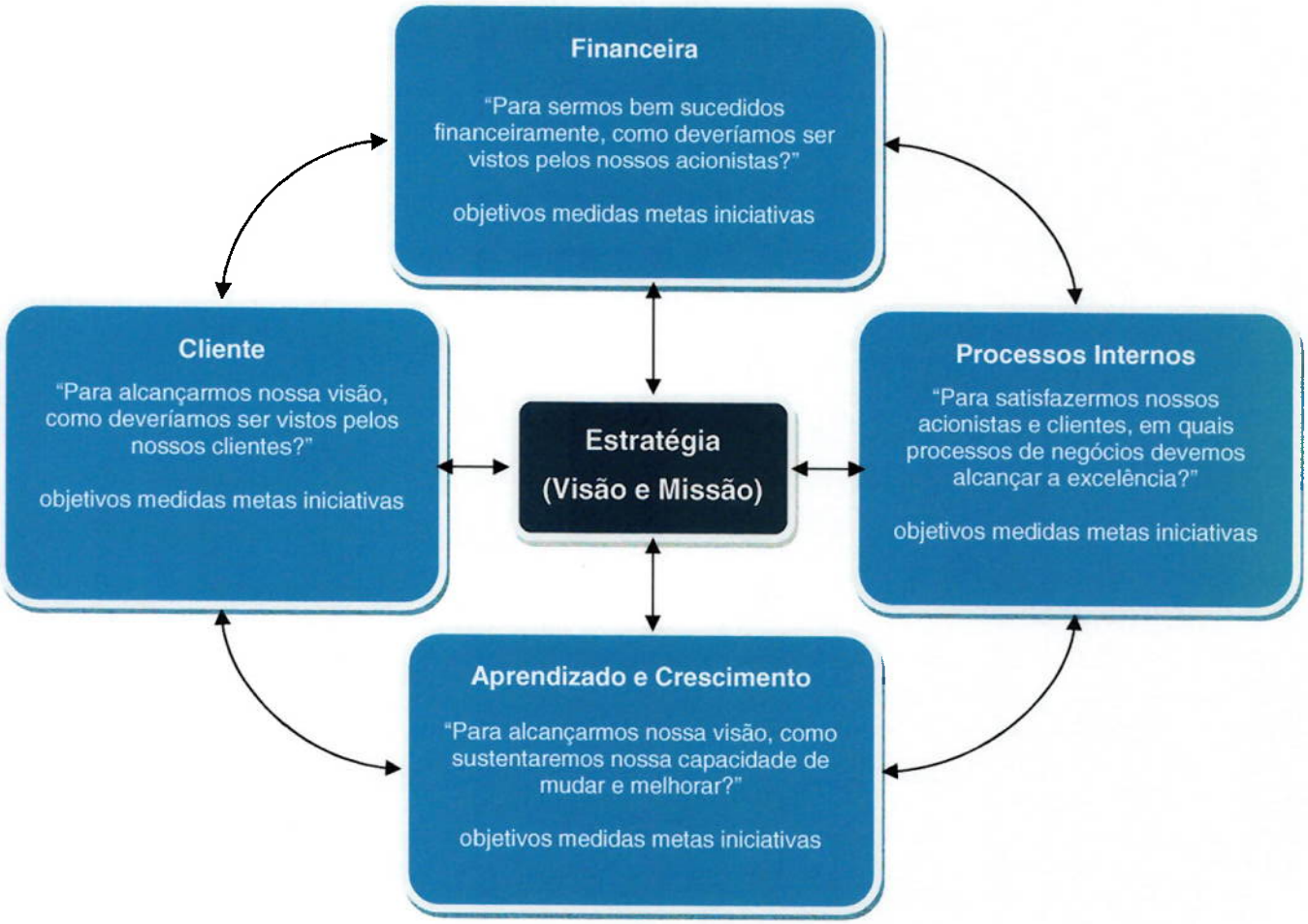

Figura 7 - Estrutura do *Balanced Scorecard* (Adaptado de KAPLAN & NORTON, 1997).

A figura 7 mostra a integração entre os componentes do mapa estratégico e as perguntas que devem ser respondidas quando a empresa estabelece as quatro perspectivas do BSC, tendo a visão e a missão como ponto central.

Para os gestores, o BSC inovou com o mapa estratégico, que em um único relatório reúne as medidas que indicam o alcance das metas necessárias para a criação de valor futuro. Para as empresas isso significa avanço no mercado, redução do tempo de lançamento de novos produtos, qualificação da equipe de trabalho, capacidade em dar respostas rápidas, gerir em longo prazo e serem orientadas para seus clientes (COSTA, 2006).

3.3.1. Perspectiva Financeira

O BSC conserva a perspectiva financeira, visto que as medidas financeiras são valiosas para sintetizar as conseqüências econômicas imediatas de ações

consumadas. As medidas financeiras de desempenho indicam se a estratégia de uma empresa, sua implementação e execução estão contribuindo para a melhoria dos resultados financeiros. Objetivos financeiros estão relacionados à lucratividade sobre o capital empregado ou o valor econômico agregado (KAPLAN & NORTON, 1997).

3.3.2. Perspectiva do Cliente

Nesta perspectiva o BSC permite que os executivos identifiquem os segmentos de clientes e mercado nos quais a unidade de negócio competirá e as medidas do desempenho da unidade nesses segmentos-alvo. Entre as medidas estão a satisfação do cliente, a retenção de clientes, a aquisição de novos clientes, a lucratividade dos clientes e a participação em segmentos-alvo (KAPLAN & NORTON, 1997).

3.3.3. Perspectiva dos Processos Internos

Na perspectiva dos processos internos os executivos primeiro devem definir uma cadeia de valor dos processos internos que tenham início com as necessidades atuais e futuras dos clientes e desenvolvam novas soluções para essas necessidades, depois prosseguir com a entrega dos produtos e prestação dos serviços aos clientes existentes e terminar com o pós-venda (KAPLAN & NORTON, 1997).

Ainda segundos esses autores, os sistemas tradicionais de medição de desempenham visam apenas o controle e a melhoria dos centros de responsabilidade de departamentos internos e no BSC os executivos devem identificar os processos mais críticos para a realização dos objetivos dos acionistas e clientes.

3.3.4. Perspectiva de Aprendizado e Crescimento

Esta perspectiva identifica a infra-estrutura que a empresa deve construir para gerar crescimento e melhoria em longo prazo. O aprendizado e o crescimento

organizacionais provêm de três fontes principais: pessoas, sistemas e procedimentos organizacionais (KAPLAN & NORTON, 1997).

Para Kaplan e Norton (1997), os objetivos financeiros, do cliente e dos processos internos, revelam lacunas entre as capacidades das pessoas, sistemas e procedimentos, que podem ser solucionadas com investimento e reciclagem de funcionários, aperfeiçoamento da tecnologia da informação e dos sistemas, e com alinhamento dos procedimentos e rotinas organizacionais.

3.4. Norma ISO/IEC 17799 (27001)

O *British Standards Institute* (BSI) criou em 1995 a BS 7799 – *Code of Practice for Information Security Management*, uma das primeiras normas para atender aos anseios das grandes organizações em relação ao estabelecimento de normas e padrões que refletissem as melhores práticas de mercado relacionado com a segurança dos sistemas de informações (PRODEMGE, 2007).

Homologada no ano de 2000 como ISO/IEC 17799:2000, a norma BS 7799 foi aceita pelos países membros do ISO (*International Standards Organization*), e em 2001 foi traduzida e adotada pela como NBR 17799, pela Associação Brasileira de Normas Técnicas (ABNT) – Código de Práticas para a Gestão da Segurança de Informação.

A norma ISO/IEC 17799 é um código de práticas com orientações para gestão de segurança da informação. Apresenta uma descrição geral das áreas normalmente consideradas importantes quando da implantação ou gestão de segurança da informação na organização (SANTOS JUNIOR et all,2006).

O objetivo dessa norma é fornecer recomendações para a gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implantação ou manutenção da segurança em suas organizações (MARTINS, 2005).

Atualmente, a norma ISO 17799 evoluiu para ISO 27001, um conjunto de normas mais organizadas pela ISO que trata dos seguintes aspectos: Política de Segurança, Plano de Continuidade do Negócio, Organização da Segurança, Segurança Física e Ambiental, Controle de Acesso, Legislação, dentre outros (BERNARDES & MOREIRA, 2005).

Ainda segundo esses autores, a ISO 27001 trata a informação como patrimônio importante da organização a ser protegido. Por meio da Análise de Risco, a norma ISO 27001 permite a organização avaliar riscos e implementar controles para preservar a Confidencialidade, Integridade e Disponibilidade da informação, garantindo a continuidade do negócio prevendo uma melhor relação de custo benefício.

Abaixo, um breve histórico da evolução das normas ISO/IEC 27001 (FERREIRA & ARAÚJO, 2008):

- 1995: publicada a primeira versão da BS 7799-1;
- 1998: publicada a primeira versão da BS 7799-2;
- 1999: publicada uma revisão da BS 7799-1;
- 2000: publicada a primeira versão da norma ISO/IEC 17799;
- 2001: publicada a primeira versão da norma no Brasil, NBR ISO/IEC 17799;
- 2002: publicada revisão da norma BS 7799 parte 2;
- 2005: agosto: publicada a segunda versão da norma no Brasil, NBR ISO/IEC 17799;
- 2005: outubro: publicada a norma ISO 27001;
- 2006: publicada a norma no Brasil, NBR ISO/IEC 27001;
- 2007: julho: alterado apenas o nome da norma NBR ISO/IEC 17799 para NBR ISO/IEC 27002.

Segundo Santos (2007), a norma ISO 17799 é um "código de práticas" e a norma ISO/IEC 27001 é composta de requisitos para Sistemas de gestão de Segurança da Informação e pode ser adotada por organizações de qualquer porte e de diferentes setores industriais e de serviços. Essa adoção, que consequentemente

leva a certificação de um ambiente seguro, afirma para clientes e fornecedores o fato de que a Segurança da Informação estar sendo levada a sério.

A norma ISO 27001 tem como objetivo assegurar a gestão da Segurança da Informação, no uso e manipulação de dados e informação, melhorando a satisfação do cliente e a imagem da organização.

4. Governança da Segurança da Informação

Considerando a dependência atual das organizações do correto funcionamento de sua área de Tecnologia da Informação e Comunicação para a realização de sua missão, as ações relacionadas com a Segurança da Informação cada vez mais deixam de ser uma responsabilidade exclusiva da área de TIC. Com isso, a segurança da informação passa a ser considerada um grande desafio para os gestores das organizações. Os gestores atuais necessitam incorporar as responsabilidades relacionadas com a Segurança da Informação em seu processo de tomada de decisão.

Além disso, os administradores atuais necessitam que não somente a TIC esteja alinhada com as estratégias da organização e que essas estratégias estejam tirando o melhor proveito da infra-estrutura de TIC existente. Eles terão que assumir cada vez mais a responsabilidade de garantir que as organizações estejam oferecendo aos seus usuários e clientes um ambiente de TIC seguro e confiável.

As organizações necessitam de proteção contra os riscos inerentes ao uso da infra-estrutura de TIC e simultaneamente obter indicadores dos benefícios de uma infra-estrutura segura e confiável. Dessa forma, além da Governança de TIC as organizações precisam estruturar especificamente a Governança da Segurança da Informação.

É possível encontrar estudos apontando a necessidade de um modelo para que as organizações possam alcançar a Governança da Segurança da Informação (BSA, 2003) (ITGI, 2006) (CGTFR,2004) (KAVAVIK et all,2003).

Em um estudo do CERT® - *Coordination Center* (CERT/CC), um centro especializado em segurança na Internet localizado no *Software Engineering Institute-Carnegie Mellon University*, aponta a necessidade das organizações estabelecerem e manterem a cultura de uma conduta organizacional para a segurança da informação. Eles procuram motivar as organizações a expandirem

seus modelos de Governança incluindo questões de segurança da informação e incorporar o pensamento sobre segurança por toda a organização, em suas ações diárias de governança corporativa (CERT, 2007).

Como resultado de uma força tarefa formada nos Estados Unidos em dezembro de 2003 para desenvolver e promover um *framework* de governança coerente para direcionar a implementação de um programa efetivo de segurança da informação, é apresentado ao público um documento descrevendo a necessidade de Governança da Segurança da Informação (CGTFR, 2004). Este trabalho apresenta também recomendações do que é necessário ser colocado em prática e uma proposta para se avaliar a dependência das organizações em relação à segurança da informação.

O *IT Governance Institute* apresenta também a necessidade de se ter um modelo para Governança da Segurança da Informação (ITGI, 2006). Nesse trabalho é apresentada a necessidade das diretorias das organizações se envolverem com as questões de segurança da informação.

4.1. Estruturando a Governança da Segurança da Informação

Um modelo para Governança da Segurança da Informação pode ser estruturado como um subconjunto da Governança de TIC e, consequentemente, da governança organizacional. Esse modelo fornecerá um guia para o alinhamento das questões de segurança da informação com o plano estratégico da organização.

Ao descrever o cenário atual para o gerenciamento de Segurança da Informação, muitas fontes na literatura apontam a necessidade e a importância de se alcançar um Modelo de Governança da Segurança da Informação que possa ser utilizado pelas organizações, de modo 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 da informação e ainda, considerá-las como parte de sua responsabilidade.

Atualmente as responsabilidades acerca da segurança da informação 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 observar um cenário onde as questões de segurança da informação não são tratadas em um nível de gestão da organização, tendo como conseqüência a falta de recursos para minimizar os riscos existentes no patamar exigido pela estratégia organizacional. A responsabilidade pelo nível correto de segurança da informação deverá 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 infra-estrutura de TIC, as organizações deveriam incorporar as questões de segurança da informação em suas ações de governança corporativa (CGTFR, 2004).

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. Esse trabalho sugere que os objetivos de controle contidos na ISO 27000 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 com as pessoas, processos e tecnologia (PRODEMGE, 2007)

Para que as organizações obtenham sucesso na segurança de sua informação, os gestores precisam tornar a segurança da informação uma parte

integrante da operação do negócio da organização. A forma proposta para se conseguir isso é utilizar 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.

Um modelo de Governança da Segurança da Informação deverá considerar as observações apresentadas anteriormente e apresentar-se fortemente acoplado ao modelo de Governança de TIC, detalhando e ampliando seu escopo de atuação na área de interseção com a segurança da informação.

Assim, a Governança da Segurança da Informação pode ser entendida como uma prática que garante que o tema Segurança da Informação seja tratado em harmonia e adequadamente com as necessidades de negócios e as estratégias de uma organização.

A Governança da Segurança da Informação deve ser descrita como um conjunto de responsabilidades e práticas relacionadas à segurança da informação e exercidas pela alta administração e gerentes executivos. Possui como meta prover estratégias de segurança para a organização, assegurando que os objetivos apresentados em seu planejamento estratégico sejam realizados, que os riscos sejam verificados e evitados e certificando ainda, que os recursos da empresa estão sendo usados com responsabilidade (ITGI, 2006).

Com base nessas observações, este trabalho apresenta a proposta de utilização de modelos e metodologias de Gestão de TIC para a obtenção da Governança da Segurança da Informação, conforme apresentado a seguir.

Nesta proposta a Governança da Segurança da Informação é vista como o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação.

4.2. *Balanced Scorecard* aplicado à Segurança da Informação

Para o estabelecimento da governança da segurança da Informação, torna-se mandatório que os controles e também os procedimentos elaborados sejam monitorados para verificar se estão funcionando de acordo com o planejado, deixando claro aos gestores os seus níveis de eficiência.

Neste caso o BSC (*Balanced Scorecard*) é uma ferramenta que pode auxiliar as organizações na identificação e representação das medidas de desempenho e dos resultados das estratégias de segurança da informação em prática. Esses indicadores possibilitarão aos gestores o gerenciamento do risco a tomada de decisão com elevado grau de assertividade. O BSC irá auxiliar ainda na tarefa de comunicar, ajustar, alinhar a estratégia da empresa com as iniciativas na área de segurança da informação, alcançando uma meta comum.

Dentro da perspectiva financeira, o BSC irá mostrar indicadores relacionados a gastos com implantação de sistemas de segurança, infra-estrutura existente e capacitação de funcionários. Cada uma dessas medidas faz parte de uma cadeia de causa e efeito e permite que a unidade de negócio alcance seus objetivos estratégicos minimizando os riscos.

A perspectiva do cliente busca a satisfação do cliente no que diz respeito ao ativo informação. Uma organização que é responsável por guardar informações sigilosas deve garantir aos seus clientes confidencialidade, integridade e disponibilidade. Assim, as organizações são capazes de manter e/ou adquirir novos clientes. As medidas geradas nessa perspectiva mostram a satisfação, fidelidade e retenção.

Na perspectiva dos processos internos, o BSC ajuda a identificar os processos críticos da organização. Na Segurança da Informação esta perspectiva auxilia a organização a proteger-se dos riscos quanto ao uso de sistemas de informação. Nessa perspectiva o gerenciamento dos processos ligados a segurança da informação, garante maior qualidade nos serviços prestados.

Na perspectiva de aprendizado e crescimento o objetivo do BSC é investir em infra-estrutura: pessoas, sistemas e procedimentos organizacionais. Na Segurança da Informação esse investimento também tem grande importância. Assim sendo Investir em treinamento garante para as organizações funcionários habilitados e motivados; investir em sistemas garante aperfeiçoamento em novas tecnologias proporcionando maior segurança da informação e investir em procedimentos organizacionais garante alinhamento dos incentivos aos funcionários e índices de melhoria dos processos críticos.

4.3. Modelo ITIL aplicado à Segurança da Informação

O modelo ITIL descreve detalhadamente os processos relativos à entrega e suporte de serviços. Esses processos serão utilizados para guiar a implementação dos objetivos de controle do modelo COBIT.

Dentro destes conceitos, o ITIL utiliza-se de um *Service Desk* que tem como função detectar problemas, incidentes causados por serviços de TIC que podem causar danos aos sistemas de informação da organização. Todo e qualquer incidente reportado deve ser registrado, monitorado para uma resolução rápida e prevenção de futuros incidentes. A utilização do ITIL irá disciplinar o tratamento de incidentes, sendo desejável a correta categorização daqueles relacionados ao comprometimento da segurança da informação.

É a partir desse registro que o Gerenciamento de Incidentes busca contornar o(s) incidente(s) a fim de restaurar os serviços afetados, o mais rápido possível, tratando os que representam maior impacto com prioridade.

A fim de evitar recorrências de um mesmo incidente, o gerenciamento de problemas busca descobrir a causa raiz dos incidentes para posteriormente adequar as mudanças necessárias na infra-estrutura da TIC.

Dessa forma, as organizações buscam a melhoria contínua dos seus processos, como forma de evoluir visando ganho de tempo, gastos, retrabalho, dando continuidade aos serviços e os mantendo ativos e disponíveis.

Os processos da ITIL podem ser utilizados como base para alcançar a conformidade com as normas ISO/IEC 20.000 e ainda, estruturar os processos descritos nas normas ISO/IEC 27001:2006 e ISO/IEC 17799:2005.(FERREIRA & ARAÚJO, 2008).

4.4. Modelo COBIT aplicado à Segurança da Informação

Por meio de relatórios confiáveis de auditoria, o COBIT avalia o nível de maturidade dos processos, ajudando a área de TIC a identificar o grau de evolução dos processos da organização permitindo sua evolução.

A partir deste relatório é possível identificar as metas e os objetivos de controles a serem atingidos pela organização, uma vez que o COBIT avalia o alinhamento estratégico da área TIC.

O Domínio Entrega e Suporte irá tratar as preocupações relacionadas como a entrega dos serviços solicitados, incluindo o *Service Delivery*, a gestão da segurança da informação e continuidade, o suporte aos usuários, e o gerenciamento dos dados e das instalações.

A utilização do COBIT irá permitir o a estruturação dos procedimentos que permitirão tratar a adequação das questões relacionadas à confidencialidade, integridade e disponibilidade.

4.5. A importância das pessoas no contexto da Segurança da Informação

Para haver sucesso na implantação e manutenção na área de Segurança da Informação, o capital humano também dispõe de atenção. É imprescindível investir em treinamento e conscientização quando o assunto é Segurança da Informação.

Programas de divulgação e conscientização também devem fazer parte da rotina da organização para assegurar que a cultura da organização possa mudar e colaborar com a Segurança da Informação.

É importante deixar claro os cuidados que cada usuário deve ter em relação ao uso dos sistemas de informação e que manter o sigilo em relação aos vários procedimentos de segurança é essencial para evitar eventuais transtornos.

O papel das pessoas dentro das organizações se faz tão importante quanto os sistemas que elas utilizam. De nada vale investir em equipamentos, sistemas de segurança se as pessoas que os utilizam não sabem das ameaças, cuidados e precauções que devem ser tomadas para evitar os riscos que afetam a segurança da informação.

4.6. Modelos e Metodologias para a Governança da Segurança da Informação

Para a obtenção da governança da segurança da informação é possível a utilização de modelos e metodologias existentes atualmente, combinando suas potencialidades e aplicá-las na área de segurança da informação. Aproveitando a experiência adquirida pelas organizações na utilização isolada ou em conjunto desses modelos e metodologias, é possível estruturar um *framework* de gestão que irá alinhar os resultados providos pela área técnica com os anseios administrativos.

A figura 8 apresenta como esses modelos e metodologias se relacionam e em que níveis organizacionais deverão ser aplicados.

No cenário atual de competição intensa, as organizações buscam cada vez mais sobreviver para não perder o mercado. Assim, se torna cada vez mais importante para as organizações, estabelecerem objetivos e estratégias para conquistarem novos clientes e manterem os atuais. Surge então a necessidade de um Planejamento Estratégico, pois é ele quem irá direcionar as organizações em relação à implantação dos seus objetivos e estratégias de forma eficiente e eficaz.

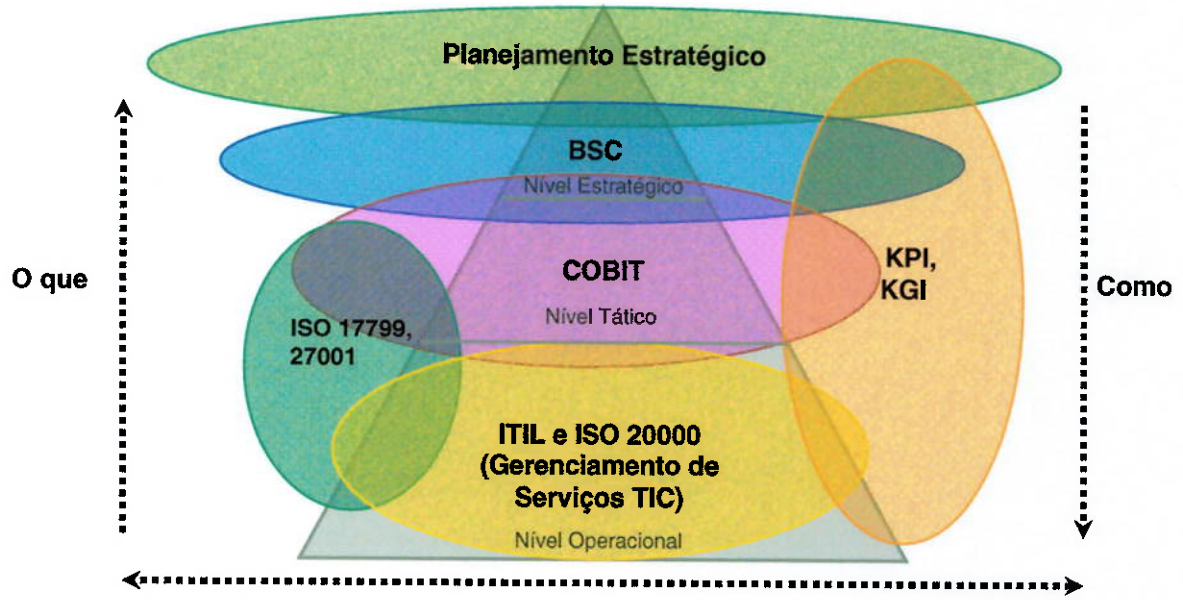

Figura 8 – Modelos e metodologias para a obtenção da governança de Segurança da Informação e seus níveis organizacionais.

O Planejamento Estratégico estabelece diretrizes para a gestão do negócio, auxilia na tomada de decisões que irão influenciar no sucesso das organizações, direcionando-as ao caminho que desejam chegar, para realização dos seus sonhos, sua visão de futuro e sua missão. (LUZIO, 2005).

Segundo Vieira (2007), o Planejamento Estratégico deverá seguir a seguinte seqüência: definir a missão do sistema de informação, avaliar o ambiente, avaliar os objetivos e estratégias da empresa, definir as políticas, os objetivos e as estratégias do sistema de informação, avaliar as necessidades de informação da empresa, montar o plano mestre de desenvolvimento, desenvolver o plano de necessidade de recursos, avaliar o projeto e desenvolver os planos do projeto.

Os indicadores (KPI – *Key Performance Indicator* e KGI – *Key Goal Indicator*) fornecem o controle para a melhoria dos processos proporcionando às organizações maior objetividade na tomada de decisões. Por meio desses indicadores as organizações são capazes de avaliar se estão atendendo os objetivos e estratégias definidas no Planejamento Estratégico. Em um modelo de governança da segurança da informação, esses indicadores serão úteis na avaliação do nível de maturidade dos processos de segurança definidos na organização e os seus respectivos riscos.

Para auxiliar as organizações, o BSC ajuda a verificar se as estratégias estão sendo desenvolvidas e se as metas estão sendo alcançadas. O *Balanced Scorecard* torna as decisões organizacionais mais balanceadas visando atender os objetivos da do negócio.

Por meio dos indicadores, que serão organizados pelo BSC, o COBIT irá auxiliar a organização no entendimento e gerenciamento dos riscos associados ao uso da Tecnologia da Informação. Sua estrutura de controles possui padrões aceitos como os melhores praticados para o estabelecimento de controles e padrões de segurança na área de Tecnologia da Informação (FERREIRA & ARAÚJO, 2008).

O relatório do nível de maturidade dos processos fornecidos pelo COBIT irá direcionar a organização dos processos de suporte e entrega de serviços de TIC utilizando o ITIL como referência. Com isso, é possível a estruturação de processos para o alcance de serviços inovadores e de alta qualidade, alinhados com os processos de negócio.

Com ênfase em prevenção, a ISO 17799 (ISO 27001) fornece as normas de segurança da informação que irão tratar os processos garantindo um ambiente seguro, entrega e suporte de serviços com qualidade e orientar as organizações na implantação de ações para contribuir na Gestão da Segurança da Informação. A ISO 17799 (27001) irá auxiliar as organizações na aplicação de ações em relação à segurança da informação e na melhoria contínua dos seus processos (ciclo PDCA – *Plan, Do, Check, Act*).

5. Considerações finais

Ao entender que a informação é um ativo valioso para o funcionamento e até mesmo para a vantagem competitiva das organizações, é importante que se haja uma atenção maior quanto a sua segurança.

A Segurança da Informação baseia-se em princípios, tais como: confidencialidade, disponibilidade e integridade. Se um desses princípios for violado, significa que houve uma quebra, um incidente de segurança da informação, podendo causar à organização alvo perdas diretas ou indiretas.

Para garantir que os riscos em relação à Segurança da Informação sejam reduzidos, modelos e metodologias são utilizados pelas organizações para melhor entender e gerenciar os riscos em relação ao uso da TIC.

Assim sendo, para que as organizações saibam buscar a melhor alternativa para a tomada de decisões, surge a necessidade da Governança da Segurança da Informação para o alinhamento entre as questões relacionadas com a Segurança da Informação e o Planejamento Estratégico.

Este trabalho apresenta uma proposta para a estruturação de um modelo de Governança da Segurança da Informação utilizando modelos e metodologias - ITIL, COBIT, BSC e ISO 17799 (27001) - de forma combinada, aproveitando suas potencialidades e permitindo que as organizações possam mapear as questões relacionadas à Segurança da Informação em um nível estratégico.

6. Referências

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.

ARRUDA, P.A.F; SILVA FILHO, J.B. – Governança de tecnologia da informação para micro e pequenas empresa: um estudo de caso na cidade de Fortaleza, 2006. Disponível on-line em: http://www.technetbrasil.com.br/academia/provas/materiais/Apostila_ISO17799_Modulo1.pdf . Visitado em 23/06/2008.

BERNARDES, M.C. – Modelagem de governança da segurança da informação com o apoio em sistemas de informação. Dissertação (Doutorado) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo. São Carlos, 2005.

BERNARDES, M.C.; MOREIRA, E.S. – Um Modelo para a Inclusão da Governança da Segurança da Informação no Escopo da Governança Organizacional. Anais do Simpósio de Segurança em Informática. São José dos Campos: CTA/ITA/IEC, 2005: 3778p. Disponível on-line: http://www.linorg.cirp.usp.br/SSI/SSI2005/artigos/14275.pdf. Visitado em 19/05/2008.

BUSINESS SOFTWARE ALLIANCE – Information Security Governance: Toward a Framework for Action. Disponível on-line em: http://www.bsa.org. Visitado em 31/01/2008.

CERT CORDINATION CENTER, *Governing for Enterprise Security.* (2007), http://www.cert.org/governance/ges.html. Visitado em 10/03/2009.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES - Cartilha de Segurança para a Internet – Parte IV: Fraudes na Internet, 2006. Disponível on-line em: http://cartilha.cert.br. Visitado em 09/06/2008.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES – Estatísticas, 2008. Disponível on-line em: http://www.cert.br/stats/incidentes/. Visitado em 19/02/2008.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES – Estatísticas, 2008. Disponível on-line em: http://www.cert.br/stats/incidentes/2008-jan-dec/tipos-ataque.html.. Visitado em 19/02/2008.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES – Estatística, 2008 Disponível on-line em: http://www.cert.br/stats/spam/. Visitado em 04/02/2009.

CORPORATE GOVERNANCE TASK FORCE REPORT. *Information Security Governance: A Call to Action.* April, 2004. Disponível on-line em: www.cyberpartnership.org/InfoSecGov4_04.pdf. Visitado em 10/03/2009.

COSTA, A. P. P. – Balanced Scorecard – Conceitos e Guia de Implementação, 2006. Editora Atlas. ISBN 85-224-4256-8.

ESPILDORA, F.G. – Modelo ITIL, 2004. Disponível on-line em: http://www.serpro.gov.br/imprensa/publicacoes/tematec/tematec/2004/ttec72Visitado em 21/01/2009.

FAGUNDES, E.F. – COBIT um kit de ferramentas para a excelência de TI, 2004. Disponível on-line em: http://www.efagundes.com/artigos/COBIT.htm. Visitado em 31/10/2008.

FERREIRA, F.N.F.; ARAÚJO, M. T. – Política de Segurança da Informação – Guia Prático para Elaboração e Implementação. Editora Ciência Moderna, 2008. ISBN 978-85-7393-771-8.

IDGNOW! – Botnets são responsáveis por 31,4% das fraudes em anúncios online, 2008. Disponível on-line em: http://idgnow.uol.com.br/seguranca/2009/01/28/botnets-

sao-responsaveis-por-31-4-das-fraudes-em-anuncios-online/. Visitado em 02/02/2009.

IDGMOW! – Brasil é o segundo país que mais recebe spams no mundo, diz McAfee, 2008. Disponível on-line em: http://idgnow.uol.com.br/internet/2008/07/02/brasil-e-o-segundo-pais-que-mais-recebe-spams-no-mundo-diz-mcafee. Visitado em 30/01/2009.

IDGNOW! – Brasil sobe em ranking de infecções impulsionado por inclusão digital, 2008. Disponível on-line em: http://idgnow.uol.com.br/seguranca/2008/06/05/brasil-sobe-em-ranking-de-infeccoes-impulsionado-por-inclusao-digital/IDGNoticiaPrint_view. Visitado em 09/06/2008.

IDGNOW! – Brasileiros estão sujeitos a ataque que forja site em URL autêntica, 2008. Disponível on-line em: http://idgnow.uol.com.br/seguranca/2008/07/29provedores-brasileiros-falham-em-teste-para-deteccao-de-brecha-n-dns. Visitado em 05/08/2008.

IDGNOW! - Sophos: Engenharia Social está em alta, 2006. Disponível on-line em: http://idgnow.uol.com.br/seguranca/2006/12/01/idgnoticia.2006-12-01.8218432008/IDGNoticia_view/. Visitado em 27/01/2009.

IDGNOW! – Tentativas de fraude na web brasileira crescem 96% no 2° trimestre, 2008. 2008. Disponível on-line em: http://idgnow.uol.com.br/seguranca/2008/07/15/tentativas-de-fraude-na-web-brasileira-crescem-96-no-2o-trimestre. Visitado em 28/07/2008.

IDGNOW! – Tentativas de fraude na web brasileira cresceram 209% em 2008, 2008. Disponível on-line em: http://idgnow.uol.com.br/seguranca/2009/01/28/tentativas-de-fraude-na-web-crescem-209-em-2008-diz-cert.br. Visitado em 30/01/2009.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION - IT Governance Institute Cobit 4.1 Expert, 2007. Disponível on-line em:

http://www.isaca.org/Content/ContentGroups/CoBIT2/Downloads/COBIT4.1-executive_summary-membership.pdf. Visitado em 27/02/2009.

KAPLAN, R.S.; NORTON D. P. – A Estratégia em Ação – Balanced Scorecard. Editora Campus. 1997. ISBN 85-352-0149-1.

KAVAVIK R.B.; CARUSO J. B.; PIRANI J. A. - *Information Technology Security: Governance, Strategy and Practice in Higher Education*. EDUCASE Center for Applied Research, 2003. Disponível on-line em:http://net.educause.edu/ir/library/pdf/ers0305/rs/ers0305w.pdf. Visitado em 10/03/2009.

LUZIO, F.F. – Fazendo a Estratégica Acontecer: como Implantar as iniciativas do *Balanced Scorecard.* Editora Luzio, 2005. ISBN 85-98129-02-X.

MAGALHÃES, I.L.; PINHEIRO, W.B. – Gerenciamento de Serviços de TI na Prática: uma abordagem com base na ITIL – inclui ISSO/IEC 20.000 e IT Flex. Novatec Editora, 2007. ISBN 978-85-7522-106-8.

MARTINS, A.B. Uma abordagem Metodológica Baseada em Normas e Padrões de Segurança – Estudo de Caso Cetrel S/A, 2005. Disponível on-line em: http://www.linorg.cirp.usp.br/SSI/SSI2004/Poster/P03_ssi04.pdf. Visitado em 23/06/2008.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - CERT.br registra aumento de 8% nas tentativas de fraudes reportadas em 2007, 2008. Disponível on-line em: http://www.nic.br/imprensa/releases/2008/rl-2008-01.htm. Visitado em 18/12/2008.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - Envio de spam disparou em janeiro e passou de 286 mil mensagens no país, 2008. Disponível on-line em: http://www.nic.br/imprensa/clipping/2006/midia27.htm. Visitado em 18/12/2008.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - Fraudes Eletrônicas estão se sofisticando, alerta integrante do comitê Gestor da Internet, 2006. Disponível on-line em: http://www.nic.br/imprensa/clipping/2006/midia141.htm. Visitado em 18/12/2008.

COMPANHIA DE TECNOLOGIA DA INFORMAÇÃO DO ESTADO DE MINAS GERAIS - Segurança da Informação. Algumas recomendações para um modelo de governança da segurança informação, 2007. Disponível on-line em: http://www.prodemge.gov.br/images/stories/volumes/volume7/algumasrecomendacoes.pdf. Visitado em 19/05/2008.

SANTOS V. M. – Plano de Continuidade dos Negócios Baseado na NORMA ISSO/IEC 27001:2005. Dissertação – Escola Politécnica da Universidade de São Paulo. São Paulo, 2007. Disponível on-line em http://www.pece.org.br/cursos/TI/monografias/MBA-MONO-VanessaSantos.pdf. Visitado em 12/02/2008.

SANTOS JUNIOR, A.R.; FONSECA, F.S.S.; COELHO, P.E.S. – Entendendo e Implementando a Norma ABNT NBR ISSO/IEC 17799:2005, 2006 Disponível on-line em:http://www.technetbrasil.com.br/academia/provas/materiais/Apostila_ISO17799_Modulo1.pdf. Visitado em 05/11/2008.

THE IT GOVERNANCE INSTITUTE - Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition. Printed in the USA, 2006. ISBN 1-933284-29-3. Disponível on-line em: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=6672. Visitado em 03/02/2009.

VIEIRA, F. M. – Gerenciamento de Projetos de Tecnologia da Informação. Editora Campus, 2007. ISBN 85-352-2273-1.

WEILL, P.; ROSS, J. W. – Governança de TI, Tecnologia da Informação. Editora M. Books do Brasil, 2006. ISBN 85.89384-78-0.

7. Glossário

Antivítus: Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.
Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.

Cavalo-de-tróia: Programa normalmente recebido com um "presente" que além de executar funções para as quais aparentemente projetados, também executa outras funções normalmente maliciosas e sem conhecimento do usuário.

Chief Security Officer: Gerente de segurança das organizações.

Cibercrimes: É a palavra dada a uma prática que consiste em fraudar a segurança de computadores ou redes empresariais. Este crime pode ser promovido de diversas maneiras: disseminação de vírus que coletam e-mails para venda de *mailing*; distribuição material pornográfico (incluindo pedofilia); fraudes bancárias; violação de propriedade intelectual e direitos conexos ou mera invasão de sites para deixar mensagens difamatórias como forma de insulto a outras pessoas.

Compliance: É o conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da instituição ou empresa, bem como evitar, detectar e tratar qualquer desvio ou inconformidade que possa ocorrer.

Bots: Programa que, alem de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam*.

Botnets: Redes formadas por diversos computadores infectados com *bots*. Podem ser usados em atividades de negação de serviço, esquemas de fraude, envio de *spam*.

Framework: É uma abstração que une códigos comuns entre vários projetos de software provendo uma funcionalidade genérica. Um framework pode atingir uma funcionalidade específica, por configuração, durante a programação de uma aplicação.

Fraudes: É qualquer crime ou ato ilegal para lucro daquele que se utiliza de algum logro ou ilusão praticada na vítima como seu método principal.

Invasão: Ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

KGI: Indicadores de Meta (KGIs - *Key Goal Indicators*) - São os parâmetros utilizados para reconhecer se o processo alcançou as metas definidas, associadas aos objetivos.

KPI: Indicadores de Desempenho (KPIs - *Key Performance Indicators*) - Definem quão bem é o desempenho do processo, em direção ao que foi definido como objetivo.

Scan: Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores.

Service Desk: O *Service Desk* é responsável por monitorar o processo de resolução de todos os Incidentes registrados. O *Service Desk* é o dono (*Owner*) de todos os incidentes.

Spam: Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente

comercial, este tipo de mensagem também é referenciada como *UCE* (do Inglês *Unsolicited Commercial E-mail*).

Stakeholders: Em português, parte interessada ou interveniente, é um termo usado em administração que refere-se a qualquer pessoa ou entidade que afeta ou é afetada pelas atividades de uma empresa.

Upgrade: Atualizar, modernizar, tornar (um sistema, software ou hardware) mais poderoso ou mais atualizado adicionando novo equipamento ou atualizando o software com sua última versão.

Vulnerabilidade: Falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Worms: Programa capaz de se propagar automaticamente através de redes, enviando cópias a si mesmo de computador para computador.