Modelagem de governança da segurança da informação com apoio em sistemas de informação

Mauro Cesar Bernardes

Orientador: *Prof. Dr. Edson dos Santos Moreira*

Tese apresentada ao Instituto de Ciências Matemáticas e de
Computação - ICMC-USP, como parte dos requisitos para
obtenção do título de Doutor em Ciências – Ciências de
Computação e Matemática Computacional.

“VERSÃO REVISADA APÓS A DEFESA”

Data da Defesa:	11/10/2005
Visto do Orientador:

USP – São Carlos
Dezembro/2005

Dedico este trabalho aos meus pais e à Elaine, pelo amor que sempre me ofereceram.

Agradecimentos

Ao meu orientador, Prof. Edson dos Santos Moreira, pela confiança, preocupação, dedicação, incentivo e amizade;

À minha família por entender minha ausência ao longo de todo este período;

Ao Centro de Computação Eletrônica por me receber ao longo deste período e fornecer condições para que acompanhasse de perto a utilização do modelo ITIL;

A todos os funcionários da DvEMIC pela amizade e incentivo;

A toda equipe da *Hewlett Packard* pelos conhecimentos transmitidos ao longo da implantação do projeto ITSM/ITIL no CCE e pelo pronto atendimento a qualquer solicitação;

Aos funcionários do ICMC por tanta ajuda ao longo desses anos.

SUMÁRIO

1	Introdução.....	1
1.1	Trabalhos relacionados.....	4
1.2	Objetivos e resultados esperados.....	5
1.3	Metodologia	7
1.4	Organização da Tese	7
2	Segurança Computacional.....	9
2.1	Caracterização das Invasões.....	11
2.2	Principais Formas de Incidentes.....	13
2.3	Principais Formas de Proteção	17
2.4	Políticas de Segurança.....	20
2.6	Necessidade de Governança da Segurança da Informação	21
2.7	Considerações Finais.....	21
3	Sistemas de Informação	23
3.1	Considerações Iniciais.....	23
3.2	Conceitos e Definições para Sistemas de Informação	23
3.3	Classificação dos Sistemas de Informação.....	25
3.4	Tomada de Decisão	28
3.5	Sistemas de Informação e Estruturas de Decisões	32
3.6	Considerações Finais.....	33
4	Extração de Conhecimento de Base de Dados	35
4.1	Considerações Iniciais.....	35
4.2	O Conhecimento.....	35
4.3	Processo de Extração de Conhecimento de Base de Dados	37
4.3.1	Etapas do Processo de Extração de Conhecimento de Base de Dados	37
4.3.2	Elementos de Apoio ao Processo de Extração de Conhecimento de Base de Dados.....	40
4.3.2.1	<i>Data Warehouse</i>	41
4.3.2.2	Métodos Estatísticos no Tratamento dos Dados	45
4.3.3	Visualização dos Dados	46
4.4	Considerações Finais.....	46
5	Necessidade de um Modelo para Governança da Segurança da Informação.....	49
5.1	Considerações Iniciais.....	49
5.2	Governança de Tecnologia da Informação e Comunicação	50
5.3	Governança da Segurança da Informação	52
5.4	Requisitos para um Modelo de Governança de Segurança da Informação.....	54
5.5	Processos e Controles para um Modelo de Governança da Segurança da Informação.....	56
5.5.1	Código de Prática para a Gestão da Segurança da Informação – ISO 17799	57
5.5.2	Modelo COBIT	58
5.5.3	Modelo ITIL.....	61
5.6	Relação dos processos entre os modelos ITIL e COBIT e a norma ISO 17799	65
5.7	Identificação de Requisitos de Segurança a Partir de uma Análise de Risco.....	67
5.8	Considerações finais.....	68
6	Extensão do Modelo ITIL com a Estratégia de CSIRTs.....	71
6.1	Considerações Iniciais.....	71
6.2	Gerenciamento de Incidentes de Segurança Computacional	71
6.3	<i>Computer Security Incident Response Team - CSIRT</i>	73
6.4	Gerenciamento de Incidentes	76

6.5	Categorização dos Serviços em um CSIRT	79
6.6	Gerenciamento de Incidentes	81
6.6.1	Função de Triagem em um CSIRT	82
6.6.2	Função de Análise do Incidente em um CSIRT	83
6.6.3	Função de Divulgação dos Resultados em um CSIRT	83
6.6.4	Função de <i>Feedback</i> em um CSIRT	83
6.7	O Ciclo de Vida de um Incidente	83
6.8	Proposta de Expansão do Modelo ITIL	85
6.8.1	Proposta para a Gerência de Incidentes	86
6.8.2	Proposta para o Processo de Gerenciamento de Problemas	87
6.8.3	Proposta para o Processo de Gerenciamento de Mudanças	88
6.8.4	Proposta de Inclusão do processo de Gerenciamento de Comportamento	89
6.9	Considerações Finais	91
7	Proposta para um Modelo de Governança da Segurança da Informação com Base em Sistemas de Informação	93
7.1	Considerações Iniciais	93
7.2	Utilização da Estrutura de Decisão de Sistemas de Informação Gerenciais	93
7.3	O Nível Operacional	97
7.3.1	Dimensão Controles: Definição dos Objetivos de Controle	97
7.3.2	Dimensão Processos: Implementação dos Objetivos de Controle	98
7.3.3	Dimensão Pessoas: Definição de Papéis e Responsabilidades dos Indivíduos Envolvidos	98
7.3.4	Dimensão Tecnologia: Ferramentas de Apoio ao Modelo	99
7.4	O Nível Tático	99
7.4.1	Dimensão Controles: Definição dos Objetivos de Controle	100
7.4.2	Dimensão Processos: Implementação dos Objetivos de Controle	100
7.4.3	Dimensão Pessoas: Definição de Papéis e Responsabilidades dos Indivíduos Envolvidos	101
7.4.4	Dimensão Tecnologia: Ferramentas de Apoio ao Modelo	101
7.5	O Nível Estratégico	102
7.5.1	Dimensão Controles: Promover Análise de Risco, Auditoria e Definir Objetivos de Controle	102
7.5.2	Dimensão Processos: Auditoria e Monitoração dos Processos estabelecidos	103
7.5.3	Dimensão Pessoas: Auditar e Monitorar as Atividades Exercidas pelos Indivíduos	103
7.5.4	Dimensão Tecnologia: Facilitar Análise de Risco e Extração de Conhecimento	103
7.6	Considerações Finais	104
8	Estudo de Caso: A Segurança Computacional no CCE/USP	105
8.1	Considerações Iniciais	105
8.2	Cenário Encontrado no Início do Projeto	105
8.3	Adoção de Melhores Práticas para Gestão da Segurança Computacional	108
8.3.1	Exemplo 01: Definição de uma Política para Servidores de E-mail	109
8.3.2	Exemplo 02: Coleta de Dados Críticos	111
8.4	Cenário Atual com parte do Projeto Implementado	115
9	Conclusão	119
9.1	Trabalhos Futuros	120
Anexo A		123
Anexo B		131
10	Referências Bibliográficas	137

Lista de Figuras

Figura 2-1. Ciclo de exploração de vulnerabilidades.....	12
Figura 2-2. Sobreposição dos Ciclos de Vulnerabilidades.....	12
Figura 2-3. Mutações em vulnerabilidades e Ferramentas de Ataque.....	13
Figura 2-4. Sofisticação dos Ataques X Conhecimento exigido do Invasor.....	14
Figura 2-5. Posicionamento de Firewall e IDS.....	19
Figura 2-6: Dados (<i>logs</i>) gerados pelos sistemas na tentativa de se proteger um ambiente....	22
Figura 3-1: Representação gráfica simplificada de um sistema de informação.....	24
Figura 3-2. Representação simplificada para Sistemas de Informações Gerenciais (SIGs)	26
Figura 3-3. O processo de gestão integrado com o Sistema de Informações.....	27
Figura 3-4. Relação entre decisão, atividades e controle.....	30
Figura 3-5. Interação da Informação com o Processo Decisório.....	31
Figura 3-6. Os tipos de planejamento nas empresas.....	32
Figura 4-1. Pirâmide do Processo de Conhecimento.....	36
Figura 4-2. Áreas de Apoio ao KDD.....	47
Figura 5-1: Abrangência da Governança e da Gestão de TI.....	52
Figura 5-2. Os domínios de processo do COBIT.....	60
Figura 5-3. Modelo para Gerenciamento de Serviços ITIL.....	62
Figura 5-4. ITIL – Processos a serem utilizados no Nível Operacional.....	64
Figura 5-5. ITIL – Processos a serem utilizados no Nível Tático.....	65
Figura 6-1: As principais funções do serviço de Resposta a Incidentes e suas relações.....	81
Figura 6-2: Processo de Gerenciamento de Incidentes no modelo ITIL.....	83
Figura 6-3. Ciclo de vida da Gerência de um Incidente apresentado pelo CERT/CC.....	84
Figura 6-4: Ciclo de vida da Gerência de Incidentes apresentado pelo modelo ITIL.....	84
Figura 6-5: O modelo ITIL original: <i>Service Support & Service Delivery</i>	85
Figura 6-6: Modelo ITIL adaptado com base nas melhores práticas para a implantação de CSIRTs.....	92
Figura 7-1: Proposta de um modelo de Governança da Segurança da Informação.....	94
Figura 8-1: Análise de Gaps para o cenário descrito em relação a Pessoas, Processos e Tecnologia.....	107
Figura 8-2: Notificações recebidas sobre incidentes de segurança computacional originados na USP em 2004.....	110
Figura 8-3: Taxa de utilização de CPU de um roteador envolvido em um Incidente de Segurança.....	111
Figura 8-4: Taxa de utilização de CPU de um roteador envolvido em um Incidente de Segurança.....	113
Figura 8-5: Ferramenta Service Desk (HPOpenview) com incidentes registrados automaticamente.	114
Figura 8-6: Análise de Gaps para o cenário atual em relação a Pessoas, Processos e Tecnologia.....	118

Lista de Tabelas

Tabela 4-1: Áreas de Trabalho da Estatística.....	46
Tabela 5-1: Relacionamento de Processos entre os modelos ITIL e COBIT e a norma ISO 17799.....	66
Tabela 6-1: Variedade de Objetivos possíveis para o Serviço de Gerenciamento de Incidentes de Segurança Computacional com base alguns tipos de CSIRTs.....	75
Tabela 6-2: Revisão do Processo de Gerenciamento de Incidentes de Segurança Computacional com base em diversos autores.....	78
Tabela 6-3: Correlação das atividades previstas em um CSIRT com as atividades previstas no modelo ITIL mapeadas na Estrutura de Decisões utilizada em Sistemas de Informação...	80
Tabela 7-1: Proposta de estratégia para implementação dos requisitos identificados neste trabalho para um modelo de Governança da Segurança da Informação.....	95
Tabela 7-2: Correlação da ISO 17799 com os modelos COBIT e ITIL como proposta para um modelo de Governança da Segurança da Informação.....	96
Tabela 7-3: Objetivos de Controle identificados no modelo COBIT para o Nível Operacional.....	97
Tabela 7-4: Objetivos de Controle identificados no modelo COBIT para o Nível Tático.....	100
Tabela 7-5: Objetivos de controle identificados no modelo COBIT para o nível Estratégico.....	102

RESUMO

Esta tese descreve um modelo que permitirá ao conselho administrativo a incorporação da Governança da Segurança da Informação como parte do seu processo de Governança Organizacional. A partir da utilização desse modelo, pretende-se que o conhecimento sobre os riscos relacionados à infra-estrutura de Tecnologia da Informação e Comunicação (TIC) seja apresentado de forma objetiva ao conselho administrativo ao longo do planejamento estratégico. O modelo apresentado foi elaborado tendo como base a estrutura de tomada de decisão utilizada pelos Sistemas de Informações Gerenciais. A seguir, foi proposta uma nova dimensão para contemplar: controles (*o que*), processos (*como*), pessoas (*quem*) e tecnologia (*ferramentas automatizadas*). Uma revisão de literatura sobre Governança de TIC foi realizada para a identificação de modelos que pudessem oferecer alguma contribuição ao trabalho. Os modelos COBIT e a norma ISO foram utilizadas para definição dos objetivos de controle a serem implementados em cada nível e o modelo ITIL foi utilizado para definir os processos responsáveis pela implementação. Algumas adaptações foram propostas para alguns processos do modelo ITIL para que o mesmo pudesse contemplar todos os objetivos de controle presentes na norma ISO e no modelo COBIT. Por último, é apresentado um estudo de caso com a implementação do modelo proposto no Centro de Computação Eletrônica da Universidade de São Paulo.

ABSTRACT.

This work describes the development of a model thought to help the administration board of institutions to consider Information Security Governance as part of their global governance structure. The idea is to provide the proper knowledge about the risks posed by the ICT infrastructure in a pragmatic way, allowing for an efficient strategic planning. The model is based on common, proven, decision making strategies used on Information Management Systems. A new dimension is added to those traditional IMS in order to accomplish: control (what), processes (how), people (who) and technology (automated tools). Through a study of some models of management and governance of ICT, the main body of the model was formed. COBIT and the ISO security standard were used to define the control objectives needed in each level. ITIL was adapted to define the implementation of the processes. Finally, a case study shows the implementation of the proposal as part of the information security strategy of the Computing Center of the University of São Paulo.

1 Introdução

Com a proliferação de ferramentas de ataques automáticos pela Internet, a facilidade crescente de se obter informações sobre como quebrar segurança de sistemas computacionais, o lançamento de técnicas modernas para isso e a sua rápida disseminação, o número de tentativas de ataque e o sucesso dessas tentativas tem crescido rapidamente nos últimos anos. Isso pode ser comprovado através de diversas pesquisas realizadas por órgãos especializados em segurança [CERT, 2005a][NBSO, 2005]. Conseqüentemente, torna-se necessário o desenvolvimento constante de novas pesquisas que possam prover mecanismos para incrementar o nível de segurança computacional nas organizações.

No meio computacional, o termo segurança da informação é usado com o significado de minimizar a vulnerabilidade de dados, da informação, do conhecimento e da infra-estrutura de Tecnologia da Informação e Comunicação (TIC) que os suporta. Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou para acessar as informações que ele contém [CERT, 2000].

A segurança computacional está relacionada à necessidade de proteção contra o acesso ou manipulação intencional ou não de informações confidenciais por elementos não autorizados e a utilização não autorizada do computador ou de seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizada nos termos de uma política de segurança [ISO, 2000]. Zorkle e Levit (1996) ainda acrescentam que a segurança computacional vai além da integridade do software e mecanismos de proteção do sistema operacional em uso; ela também é dependente da própria configuração e uso do software com base na política de segurança previamente definida [ZERKLE and LEVITT, 1996].

Diversos trabalhos de pesquisa nas áreas de gerenciamento e de segurança de redes foram realizados pelo Grupo de Segurança Computacional do *Laboratório Intermídia do ICMC-USP* desde 1990. A continuidade dos projetos e a pesquisa de métodos alternativos de gerenciamento e de segurança de redes têm sido preocupações constantes desse Grupo. Em sua evolução, esses trabalhos podem ser categorizados em seis fases bem-definidas, a saber:

1. Projeto *MultiView* - implementado através da integração de várias ferramentas existentes em UNIX (*gawk, ping, etherfind, etc*) e estruturas de dados complexas em um ambiente gráfico bastante robusto e capaz de visualizar a topologia de rede, mostrar informações de sub-redes e mostrar informações de equipamentos [ODA, 1994]. Nessa fase, ocorreu ainda, a adição de recursos multimídia para vídeo-conferência [LIEIRA, 1995] [MORAES, 1995] e o desenvolvimento de um agente SNMP [CICILIANI, 1994].
2. Projeto *NetTracker*: resultado da evolução do modelo de gerenciamento incluindo administração via WWW, método de extensão dos serviços do gerente e carregamento dinâmico de módulos [MOURO, 1997] [MOURO, MORISHITA & MOREIRA, 1997] [MORISHITA, 1997].
3. A terceira fase, consiste na integração de serviços de detecção de intrusos ao *NetTracker*. Um sistema de detecção de Intrusos baseado em redes neurais já foi desenvolvido e adaptado para que seja possível utilizá-lo através do ambiente *NetTracker* [CANSIAN 1997][CANSIAN et al., 1997a] [CANSIAN et al. 1997b] [CANSIAN et al. 1997c] [BONIFÁCIO et al., 1998a] [BONIFÁCIO et al., 1998b].
4. Na fase quatro foi avaliada a utilização da tecnologia de agentes móveis em um ambiente de gerenciamento de segurança [REAMI, 1998]. A definição de uma arquitetura, a descrição dos cenários de sua utilização, a implementação de um desses cenários e ainda, uma comparação com Sistemas de Detecção de Intrusão monolíticos foram apresentadas [BERNARDES, 1999] [BERNARDES & MOREIRA, 1999] [BERNARDES & MOREIRA, 2000a][BERNARDES & MOREIRA, 2000b] [BERNARDES & MOREIRA, 2000c]. A avaliação de ambientes de agência para agentes móveis também foi pesquisada [PEREIRA FILHO, 2000]. Este último trabalho avaliou as plataformas existentes no sentido de determinar sua indicação para aplicações de segurança computacional e comércio eletrônico. Ainda nesta etapa foi apresentado o projeto de um sistema que tinha como objetivo auxiliar o Administrador de *Web* no monitoramento do acesso da rede através da análise do histórico de acesso (*Logs*) dos servidores *Web*, *Proxy* e *Firewall*, das características dos *hosts* e servidores, e detalhes sobre os usuários que realizaram os acessos [HIROSE, 2000]. Para dar suporte à gama de dados a serem armazenados e analisados foi proposta a utilização da tecnologia de *Data Warehouse*.
5. A utilização de diversos tipos de algoritmos inteligentes para busca de padrões na detecção de intrusão [AMBROSIO et al., 2000] e o desenvolvimento de um módulo

distribuído para captura de pacotes em redes de computadores [TAVARES & MOREIRA, 2001] caracterizam a quinta fase..

6. A fase mais recente das pesquisas é caracterizada pela estruturação das informações sobre segurança computacional para permitir a extração de conhecimentos de forma objetiva. Entre os trabalhos desenvolvidos estão: o levantamento das principais questões de segurança existentes no paradigma de computação ubíqua interativa [MILAGRES, 2004] e pela proposta do uso de ontologias para classificar vulnerabilidades conhecidas, provendo auxílio para a extração de valor semântico para a identificação de vulnerabilidades de mesma natureza [BRANDAO et al, 2004][MARTIMIANO, 2004][MARTIMIANO, 2005].

Conforme demonstrado nesses trabalhos, há diversas fontes de dados que podem e devem ser levadas em consideração no momento da tomada de decisão sobre segurança em um ambiente computacional. Esses dados podem ser de fontes diretamente relacionadas à segurança, como *Logs* de acesso às máquinas que compõem o sistema, *logs* do *firewall*, logs gerados a partir de listas de acesso (*access-lists*) configurados nos roteadores, alertas do Sistema de Detecção de Intrusão, alertas de vulnerabilidades, etc e/ou podem ser de fontes que podem fornecer dados que ajudarão na elaboração de informações que podem caracterizar uma quebra de segurança (como os diversos dados conseguidos via SNMP, estatísticas de taxas de utilização de processador dos diversos elementos que compõem o ambiente, estatísticas da utilização da largura de banda, sobrecarga de memória de equipamentos em uma rede).

Foi demonstrado também nos trabalhos desenvolvidos que a grande dificuldade encontrada na tentativa de elevar o nível de segurança desses ambientes está relacionada à manipulação pelo administrador de um grande volume de dados capturados no ambiente a ser protegido. Com a enorme quantidade de dados disponíveis, provenientes das mais diversas fontes, torna-se extremamente difícil realizar uma análise em tempo hábil para a tomada de decisão antes que um incidente alcance grandes proporções.

O problema da tomada decisão com base em muitos dados ocorre também no processo de tomada de decisões relacionadas a negócios no ambiente empresarial [AUDY & BRODBECK, 2003] [LAUDON & LAUDON, 2004][BIO, 1994][EIN-DOR & SEVGEV, 1978][GUERREIRO, 1989] [COSTA, 2000][CATELI, 1999][OLIVEIRA, 1998]. A solução nesse caso foi a adoção de sistemas de informação, de onde surge a idéia de estruturar um

sistema de segurança computacional nos moldes de um sistema de informação para se obter a base de um modelo para a Governança da Segurança da Informação.

Uma análise do cenário atual demonstra que o crescimento e sucesso das organizações atualmente estão intimamente relacionados com a necessidade de se manter uma infra-estrutura de TIC (Tecnologia da Informação e Comunicação) segura e confiável. A dependência atual das organizações da sua infra-estrutura de TIC, associadas às oportunidades, benefícios e riscos inerentes a essa área, faz com que as organizações passem a considerar a necessidade de uma melhor gerência das questões relacionadas com a TIC. Esse cenário implica na necessidade das organizações em desenvolver modelos para a Governança da Tecnologia da Informação e Comunicação.

Os conselhos diretores atuais necessitam que não somente a TIC esteja alinhada com as estratégias da organização e que devido a estas estratégias, estejam tirando o melhor proveito da TIC existente. Eles terão que assumir cada vez mais a responsabilidade de garantir que as organizações estejam oferecendo aos seus usuários um ambiente de TIC seguro. Além disso, as organizações necessitam de proteção contra os riscos inerentes ao uso da infra-estrutura de TIC e simultaneamente obter indicadores dos benefícios de se ter esta infra-estrutura segura. As organizações precisam de um modelo para a Governança da Segurança da Informação.

1.1 Trabalhos relacionados

É possível encontrar diversos trabalhos apontando a necessidade de um modelo para que as organizações possam alcançar a Governança da Segurança da Informação [BSA, 2003][ITGI, 2001][IIA, 2001][CGTFR,2004][NCSP, 2004][CARUSO, 2003][OGC, 2001B][CERT, 2005b].

Em um trabalho recente, o *CERT® - Coordination Center (CERT/CC)*, um centro especializado em segurança na Internet localizado no *Software Engineering Institute-Carnegie Mellon University*, aponta a atual 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 computacional e incorporar o pensamento sobre segurança por toda a organização e nas ações diárias de governança [CERT, 2005b].

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 implementado e uma proposta para se avaliar a dependência das organizações em relação à segurança computacional.

O *IT Governance Institute* apresenta também a necessidade de se ter um modelo para Governança da Segurança da Informação [ITGI, 2001]. Nesse trabalho é apresentada a necessidade da diretoria das organizações se envolver com as questões de segurança computacional. Algumas recomendações serão apresentadas e mapeadas em níveis de maturidade.

1.2 Objetivos e resultados esperados

Apesar da existência de diversos trabalhos apontando a necessidade da elaboração de um modelo para Governança da Segurança da Informação, não há a proposta de um modelo que contemple as necessidades de toda a organização, considerando o nível operacional, o nível tático e o nível estratégico.

O objetivo deste trabalho é apresentar um modelo para Governança da Segurança da Informação baseado na estrutura de tomada de decisões utilizada em Sistemas de Informação, ampliando e completando as propostas dos *frameworks* de avaliação apresentados pelos trabalhos citados.

O modelo proposto deverá permitir que os mais diversos dados sobre segurança computacional, coletados no nível operacional do ambiente a ser protegido, sejam utilizados para gerar informações úteis ao nível tático e o conhecimento esperado pelo conselho administrativo para a realização da missão da organização com o mínimo de riscos possíveis. Para ser consistente e ter capacidade de maximizar o valor do conhecimento entregue ao conselho administrativo, será apresentado um modelo que além de permitir a extração do conhecimento, fornecerá os objetivos de controle, os papéis e responsabilidades do pessoal envolvido, os processos e as recomendações tecnológicas em cada um dos níveis da organização.

Uma vez implementado, espera-se que o modelo de Governança da Segurança da Informação proposto seja capaz de prover um mecanismo para a obtenção dos seguintes resultados:

- **Alinhamento estratégico**
 - Prover conhecimento para que o conselho administrativo tenha as questões relacionadas com a segurança computacional alinhadas às estratégias da organização para a realização de sua missão;
 - Apontar soluções de segurança computacional de acordo com o esperado pelos processos organizacionais;
 - Gerar o conhecimento para que o conselho administrativo possa ter o investimento em segurança computacional alinhado com a estratégia da organização.
- **Gerenciamento de Risco**
 - Realizar análises de Risco e definir o nível de risco aceitável;
 - A partir da análise de risco, escolher os objetivos de controle e o nível de maturidade esperado;
 - Entendimento dos riscos existentes.
- **Disseminação da Cultura de Segurança Computacional através da organização**
 - Estabelecer um conjunto padrão de melhores práticas de segurança computacional baseadas em recomendações amplamente conhecidas;
 - Fornecer processos que permeiem os anseios da organização em termos de pessoas, processos e tecnologia;
 - Implementar a cultura da melhoria contínua da segurança computacional a partir dos modelos de Governança da TIC que possuem as melhores práticas adotadas em larga escala e aprovadas pelas organizações ao redor do mundo;
 - Definir papéis e responsabilidades para as pessoas envolvidas;
- **Medidas de Desempenho**
 - Definir um conjunto de métricas para avaliação dos níveis de maturidade da segurança computacional;
 - Processo de Avaliação com divulgação dos progressos.

- **Recomendações tecnológicas**

- Identificar estratégias tecnológicas que forneçam apoio ao modelo em cada nível da organização.

1.3 Metodologia

Para a definição de um modelo de Governança da Segurança da Informação, será considerada a estrutura dos modelos de tomada de decisão utilizados em Sistemas de Informação. Modelos contendo as melhores práticas para a Governança da TIC serão analisados e adaptados nessa estrutura, incorporando as questões relativas à segurança computacional.

Os modelos para auxílio na Governança da TIC serão analisados na busca das melhores práticas que possam ser aplicadas ao Modelo de Governança da Segurança da Informação.

O modelo ITIL [OGC, 2000] será investigado para prover os processos necessários do modelo. Os objetivos de controle do modelo COBIT [ITGI, 2000] e os controles definidos pela ISO 17799 serão investigados para guiar melhores práticas e fornecer controles específicos para a segurança computacional.

As estratégias de análise de risco serão consideradas numa tentativa de ajudar na identificação de quais objetivos de controle devam ser aplicados a um determinado ambiente em um determinado momento.

1.4 Organização da Tese

Para apresentação desta proposta, esta monografia está organizada da seguinte forma:

No capítulo 2 será apresentada uma contextualização das ferramentas e procedimentos envolvendo a tecnologia de segurança computacional.

No capítulo 3 será apresentada uma revisão de literatura relacionada aos principais conceitos envolvendo a área de sistemas de informação. Esses são imprescindíveis ao fornecimento de requisitos para a proposta deste trabalho.

No capítulo 4 serão apresentadas as metodologias para análise automática de informação com base na Extração de conhecimento de Base de Dados.

No capítulo 5 será apresentada a necessidade de um modelo para Governança da Segurança da Informação. Uma revisão de literatura é apresentada para comprovar esta

necessidade. Ainda nesse capítulo serão apresentados os modelos ITIL e COBIT para Governança de TIC. Será proposta a expansão do modelo ITIL para que seus processos permitam a implantação dos objetivos de controle extraídos do modelo COBIT e da ISO 17799 para obtenção do modelo de Governança da Segurança da Informação.

No capítulo 6 será apresentada a proposta de expansão do modelo ITIL para que o mesmo possa ser utilizado como a base para um modelo de Governança da Segurança da Informação. Essa expansão será feita considerando-se as recomendações existentes para a implantação de Grupos de Resposta aos Incidentes de Segurança Computacional (*CSIRTs-Computer Security Incident Response Teams*).

No capítulo 7 será apresentado o modelo proposto para Governança da Segurança da Informação baseado em Sistemas de Informação.

No capítulo 8 será apresentado um estudo de caso para o ambiente onde o modelo proposto está sendo validado.

Finalmente, o capítulo 9 apresentará as conclusões para esta Tese.

2 Segurança Computacional

Para uma discussão sobre segurança computacional, torna-se necessário primeiramente ter em mente três importantes conceitos básicos de segurança da informação: *confidencialidade*, *integridade* e *disponibilidade*. Deve-se também ter em mente três conceitos relacionados com as pessoas que usam tal informação: *autenticação*, *autorização* e *irretratabilidade/irrevogabilidade*.

Quando informações são lidas ou copiadas por alguém não autorizado a fazê-lo, o resultado é conhecido como perda de *confidencialidade*. Para alguns tipos de informações, *confidencialidade* é um atributo indispensável. Como exemplo, pode-se considerar dados de pesquisas, especificações de um novo produto e estratégias de investimento empresarial.

Em algumas regiões do mundo há uma obrigação moral, e até mesmo legal em alguns casos, de proteger a privacidade dos dados referentes a um indivíduo. Isso é particularmente verdadeiro para bancos e companhias de empréstimo, companhias de cartão de crédito, consultórios médicos etc. Os regulamentos dos Estados Unidos da América, como o *Sarbanes-Oxley*, *Californian Senate Bill 1386* (SB 1386) e o HIPPA (*Health Insurance Portability and Accountability Act*) exigem que as organizações protejam informações de identificação pessoal.

Informações podem ser corrompidas quando disponíveis em uma rede. Quando uma informação é modificada de uma forma não esperada, o resultado é conhecido com perda de *integridade*. Isso significa que mudanças não autorizadas são realizadas nas informações, seja por erro humano ou de forma intencional. Integridade é particularmente importante para informações de segurança críticas usados para atividades como controle de tráfego aéreo, contabilidade financeira, transações bancárias etc.

A informação também pode ser apagada ou tornar-se inacessível, resultando na falta de *disponibilidade*. Isto significa que pessoas que são autorizadas a acessar a informação não podem fazê-lo.

Disponibilidade é freqüentemente o atributo mais importante em negócios que dependem da informação. Disponibilidade de uma rede é importante quando se depende da conexão com a rede para realização de atividades essenciais à execução da missão da organização. Quando um

usuário não pode acessar a rede ou serviços específicos suportados por ela, diz-se que houve uma falha conhecida como uma negação do serviço (*DoS - Denial of Service*).

Para tornar a informação disponível para aqueles que precisam dela e são autorizados a acessá-la, organizações usam autenticação e autorização. A autenticação é utilizada para provar que o usuário é quem diz ser. Esse processo envolve algo que o usuário conheça (como uma senha), algo que ele tenha (como um *smartcard*) ou algo sobre o usuário que prove sua identificação (com o uso de recursos biométricos). Autorização, por sua vez, é o ato de determinar se um usuário particular (ou sistema computacional) tem o direito de executar certa atividade, como a leitura de um arquivo ou a execução de um programa. Autenticação e autorização são processos empregados em conjunto. Os usuários precisam ser autenticados antes de executarem uma atividade que eles estão autorizados a executar. A segurança torna-se mais forte quando o resultado de uma autenticação não pode ser negado posteriormente (ou seja, o usuário não poderá negar que executou uma determinada atividade). Este processo é conhecido como não-repúdio.

Atualmente é muito fácil o ganho de acesso não autorizado à informação em uma rede insegura e, de modo inverso, está cada vez mais difícil identificar os invasores. Mesmo que os usuários não possuam nada importante armazenado em seus computadores, um computador desprotegido pode ser explorado para ser utilizado como “a porta de entrada” para o acesso não autorizado às informações de uma organização que estejam armazenadas em outros equipamentos interconectados.

Em muitas vezes, informações aparentemente simples podem contribuir para o comprometimento de um sistema computacional. Informações que os invasores consideram úteis incluem quais hardwares, softwares, configurações, tipo de conexão com a rede, número de telefones e procedimentos de acesso e autorização estão sendo utilizados. Informações relacionadas à segurança podem permitir que indivíduos não autorizados ganhem o acesso a importantes arquivos e programas e dessa forma, comprometer a segurança do sistema. O seguinte são exemplos de informações importantes: senhas, informações pessoais e chaves de criptografia, versões de sistemas etc.

Conforme relatos de respeitadas centros mundiais especializados em segurança computacional, como exemplo o CERT.org e o NBSO, não é possível garantir 100% de segurança quando se está conectado à Internet [NBSO, 2005] [CERT, 2005a]

Diversas estatísticas demonstram que entre os afetados encontram-se grandes bancos e companhias financeiras, companhias de seguro, órgãos governamentais, hospitais, provedores de serviços de redes, universidades, etc. Entre as invasões, muitas irão acarretar perda financeira de forma direta, como exemplo uma transferência monetária, e/ou indireta, como exemplo o comprometimento da imagem da organização.

2.1 Caracterização das Invasões

É difícil caracterizar pessoas que causam incidentes. Um invasor pode ser um adolescente curioso sobre o que pode e o que não pode fazer na Internet, um estudante que criou um novo software, um indivíduo em busca de um algum lucro, um espião pago para roubar informações de uma empresa ou um país estrangeiro buscando conseguir alguma vantagem competitiva, política ou econômica, etc.

Embora a definição da palavra invasão não inclua o conceito de um usuário interno fazendo mau-uso dos recursos a que tem acesso, ela é muitas vezes empregada nesse sentido em trabalhos sobre segurança computacional e também o será neste trabalho. Assim, uma invasão também pode ser causada por um funcionário legítimo de uma empresa ou por um consultor que ganhou acesso a informações da rede enquanto desenvolve um trabalho na organização.

O invasor pode encarar um ataque contra uma organização como uma busca por entretenimento, um desafio intelectual, uma sensação de poder, um protesto político, ganho financeiro etc.

O que realmente se sabe acerca dos invasores é que eles trabalham em comunidade e compartilham informações. Invasores identificam sistemas malconfigurados e divulgam esta informação, além de usarem esses sistemas para troca de software pirata, envio de *spam*, troca de informações etc. Com isso, pode-se concluir que informações sobre vulnerabilidades são disseminadas de forma muito mais rápida entre invasores do que entre administradores de sistema.

Observando a Figura 2-1, é possível concluir que na maioria dos casos os administradores só se dão conta de uma nova vulnerabilidade após esta estar largamente difundida entre os invasores. Com isso, os administradores necessitam estar constantemente à procura de furos de segurança e aplicar *patches* de atualização. Quanto mais tempo se leva para descobrir a vulnerabilidade e aplicar tais *patches*, maior a probabilidade de o sistema tornar-se comprometido.

Figura 2-1: Ciclo de exploração de vulnerabilidades (Adaptadas de [CERT, 2000])

Como existe certa demora no lançamento de *patches* de segurança e uma grande dificuldade dos administradores se manterem constantemente atualizados, tem-se um cenário em que uma rede pode alcançar um estado altamente vulnerável muito rapidamente.

Além dos fatos citados anteriormente, é possível observar que em função do grande número de vulnerabilidades descobertas a cada dia, seus ciclos se sobrepõem, conforme ilustrado na Figura 2-2.. Exemplificando, este efeito foi claramente comprovado por *worms* e vírus de alcance mundial que surgiram nos últimos anos, especialmente com o *Code Red* [CERT,2001a], *Sircam*[CERT,2001b] e *Nimda*[CERT,2001d].

Figura 2-2: Sobreposição dos Ciclos de Vulnerabilidades

Algumas ferramentas que exploraram as vulnerabilidades podem ainda sofrer mutações e comportarem-se de forma diferente da originalmente identificada, conforme ilustrado na Figura 2-3. Assim, ressurgem como uma ameaça algum tempo após os administradores terem desviado seu foco de atenção para outros ciclos. Apesar de muitas vezes não ressurgirem com o mesmo potencial de ameaça, variações freqüentemente tomam um tempo considerável dos administradores no processo de sua eliminação.

Figura 2-3: Mutações em vulnerabilidades e Ferramentas de Ataque

Um dos primeiros exemplos desta mutação que alcançou proporções mundiais foi o *Code Red* sofrendo mutação para o *Code Red II (Code Blue)* [CERT,2001c].

Com base nessas informações, fica evidente a necessidade das organizações se estruturarem para identificar as vulnerabilidades no menor tempo possível, permitindo manter os níveis de serviço acordados para a realização de seu negócio. Ao encontro dessa necessidade, este trabalho propõe um modelo para Governança da Segurança da Informação, conforme será descrito nos capítulos 5 e 7.

2.2 Principais Formas de Incidentes

Conforme pode ser observado na Figura 2-4, a última década apresentou uma grande evolução das ferramentas e nos métodos utilizados para se invadir um sistema. Inicialmente era necessário que um invasor possuísse um grande conhecimento sobre sistemas computacionais e linguagens de programação para que alcançasse sucesso em suas tentativas. Isso se devia principalmente à inexistência de ferramentas próprias para esse tipo de ação.

Entretanto, com o passar dos anos, diversas ferramentas e métodos foram sendo desenvolvidos e disseminados. Com isso, o conhecimento necessário para se conseguir êxito em uma invasão diminuiu de forma alarmante, conforme ilustrado na Figura 2-4.

Figura 2-4: Sofisticação dos ataques X Conhecimento exigido do Invasor (Adaptado de [CERT, 2000]).

Hoje em dia, uma vez conectado à Internet, qualquer pessoa pode acionar um serviço de busca e, pesquisando por palavras chaves, terá acesso a informações sobre como atacar equipamentos e obter softwares para invasão simples de serem utilizados. Além de a Internet ser o principal meio pelo qual a maioria das intrusões ocorre, é também através dela que são largamente disponibilizados e veiculados documentos explicando e demonstrando técnicas de invasão, furos de segurança e casos de monitoração de intrusões em andamento. É possível encontrar com facilidade documentos do tipo “receita de bolo”, que ensinam técnicas de intrusão detalhadamente. Ainda que sejam técnicas simples, podem ser altamente destrutivas, tendo-se em vista que boa parte das redes conectadas à Internet não possui um completo domínio das questões relacionadas com a segurança.

Todas essas ferramentas e métodos para invasão a sistemas computacionais podem ser categorizados em diversas classes. Entre as principais encontram-se as seguintes:

- **Prob** - Um *probe* é caracterizado por uma tentativa não usual de ganhar acesso a um sistema ou de descobrir informações sobre o mesmo. Os *probes* são algumas vezes seguidos por um evento de segurança mais sério, mas eles muitas vezes são resultados de curiosidade ou confusão.

- **Scan** - Um *scan* é simplesmente um grande número de *probes* feito a partir de uma ferramenta automatizada. Os *scans* podem algumas vezes ser o resultado de um sistema malconfigurado ou outro erro, mas eles são freqüentemente os anúncios de um ataque mais direcionado a um sistema em que o invasor encontrou alguma vulnerabilidade.
- **DoS (Denial of Service)** - A meta em um ataque *DoS* não é obter acesso não autorizado a máquinas ou dados, mas impedir que usuários legítimos utilizem um sistema. Este ataque consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços.
- **DDoS (Distributed Denial of Service)** - Os ataques *DDoS* são o resultado da união de negação de serviço e intrusão distribuída. Os ataques *DDoS* podem ser definidos como ataques *DoS* diferentes partindo de várias origens, disparados simultânea e coordenadamente sobre um ou mais alvos. Resumidamente são ataques *DoS* em larga escala.
- **Sniffer** - Um *sniffer* é um programa que captura pacotes que estão trafegando em uma rede. Tais pacotes podem conter nomes de usuários, senhas e informações proprietárias que trafegam decodificados pela rede. De posse de uma grande quantidade de nomes de usuários e senhas o usuário pode lançar um ataque de larga escala a um sistema. Uma vez que para a instalação de um *sniffer* não é necessária uma conta privilegiada, este recurso é largamente utilizado em redes de computadores.
- **Código Malicioso** - Código malicioso é o termo utilizado para designar programas que, quando executados, causarão resultados indesejados a um sistema. Os usuários do programa não estão cientes de suas ações até que os danos sejam descobertos. Nesta classe de software estão incluídos os seguintes : *Trojan horses* (*cavalos de tróia*), *vírus* e *worms*. Os *trojan horses* e os vírus estão usualmente ocultos em um programa legítimo ou arquivos que os invasores alteraram para fazer mais do que se espera deles. Os *worms* são programas que se multiplicam automaticamente e se espalham sem intervenção humana depois que são inicializados. Vírus são programas que se multiplicam automaticamente, mas usualmente requerem uma ação humana para se espalharem inadvertidamente para outros programas ou outros sistemas. Esta

classe de programa pode levar a perdas sérias de dados, perda de desempenho, indisponibilidade (*denial-of-service*) e outros tipos de incidentes de segurança.

- **Spam** - *Spam* é mensagem não solicitada. Sua definição em termos práticos refere-se ao envio abusivo de mensagens de correio eletrônico não solicitadas, geralmente em grande quantidade, distribuindo propaganda, correntes, esquemas de "ganhe dinheiro fácil" etc. É o envio de mensagens de correio eletrônico tentando forçar a leitura pela pessoa que recebe e que, normalmente, não optou por este recebimento. No ambiente Internet, *spam* significa enviar uma mensagem qualquer para uma grande quantidade de usuários, sem primeiro verificar a utilidade do conteúdo da mensagem para aqueles destinatários. O autor do *spam* é conhecido como "*spammer*". Apesar de aparentemente não causar perdas diretas aos sistemas que recebem um *spam*, quando bem planejado um *spam* pode levar o sistema alvo a experimentar a indisponibilidade de seus serviços de e-mail.
- **Mail Bomb** - Trata-se da técnica de enviar uma grande quantidade de mensagens eletrônicas a um destinatário. Em geral, o agressor usa um script para gerar um fluxo contínuo de mensagens e sobrecarregar a caixa postal de alguém. A sobrecarga tende a provocar negação de serviço (DoS) no servidor de e-mail.
- **Spoofing** - Um *spoofing* ocorre quando invasores autenticam uma máquina em nome de outra forjando pacotes de um *host* confiável. Nos últimos anos, essa definição foi expandida para abranger qualquer método de subverter a relação de confiança ou autenticação baseada em endereço ou em nome de *host*. Entre as mais conhecidas encontram-se as seguintes: *spoofing* de IP, *spoofing* de ARP e *spoofing* de DNS.
- **Comprometimento de Conta** - Um comprometimento de conta é o uso não autorizado de uma conta por alguém que não é seu proprietário, não considerando os privilégios de sistema e *root*. Um comprometimento de conta pode expor a vítima a perdas de dados, roubo de dados ou serviços etc.

Todos os exemplos acima podem ser utilizados individualmente ou em conjunto para comprometer a *confidencialidade*, *integridade* ou *disponibilidade* dos sistemas e, conseqüentemente, tornando-os inseguros.

Essa conjuntura de computadores, redes e comunicações inseguras deve-se, em parte, ao modo como a Internet foi projetada. O principal foco do projeto da Internet, e mais basicamente

do protocolo TCP/IP, estava muito distante dos atuais usos da Internet. Seu projeto previa inicialmente o uso por instituições militares e de pesquisa. O crescimento e a popularização da Internet, o surgimento de aplicações de comércio eletrônico, a interligação das redes das diversas filiais de uma empresa e muitas outras características e serviços oferecidos pela Internet de hoje, não eram sequer supostas pelos seus projetistas e técnicos. O crescimento da Internet levou a uma mudança no foco e no perfil dos usuários e das aplicações da rede. Em vista disso, muitos dos protocolos, serviços, sistemas operacionais e softwares que são utilizados na Internet não foram projetados e especificados com as devidas preocupações com relação à segurança. Originalmente, no UNIX, as senhas circulavam totalmente abertas pela rede, o protocolo TCP/IP não previa nenhum esquema de criptografia dos dados ou autenticação das máquinas e usuários envolvidos em uma conexão.

Os sistemas atuais, como o Windows NT/2000/XP, foram criados em cenários com preocupações específicas sobre segurança. Porém ainda não se mostraram soluções totalmente confiáveis devido a diversos fatores, o que acarretaram falhas e furos de segurança que são descobertos a cada dia e notificados pelo fabricante.

Outro aspecto das novas formas de ataque é que elas focalizam a infra-estrutura da rede, como roteadores e *firewalls*, e a capacidade de disfarçar seu comportamento. Invasores têm utilizado *trojan horses* para esconder suas atividades dos administradores de rede. Por exemplo, invasores alteram programas de autenticação e *login* para que eles possam acessar os sistemas sem gerar arquivos de *logs* de suas atividades. Invasores também podem criptografar o resultado de suas atividades, como informações capturadas por um *sniffer*. Mesmo se o administrador encontrar os *logs* da ferramenta utilizada para captura de informações, é muito difícil ou impossível determinar quais informações foram comprometidas.

Armados com conhecimento sobre uma vulnerabilidade específica, técnicas de engenharia social e ferramentas automáticas para roubar informações que possam levar ao acesso de sistemas, invasores freqüentemente conseguem acessar redes e *hosts*.

2.3 Principais Formas de Proteção

Em função das vulnerabilidades e tendências a incidentes discutidas anteriormente, observa-se que a tarefa do administrador de rede torna-se extremamente sobrecarregada com administração dos recursos necessários para a administração de segurança. Fica evidente que

devido ao grande número de alertas e vulnerabilidades descobertas que trafegam diariamente pela Internet, torna-se necessário que exista nas organizações alguém ou uma equipe que ocupe uma posição destinada exclusivamente à administração das questões relativas a segurança computacional.

Uma grande variedade de tecnologias tem sido desenvolvida para ajudar organizações e administradores a proteger seus sistemas e informações contra invasores. Essas tecnologias ajudam a detectar atividades suspeitas, proteger contra ataques ou operações não usuais e a responder a eventos que afetam a segurança. Entre as principais, destacam-se as seguintes:

- **Firewall** - Um *firewall* é uma coleção de hardware e software projetado para examinar o tráfego em uma rede e os serviços requisitados. Ele é basicamente um dispositivo que impede que pessoas externas acessem sua rede. Esse dispositivo é em geral um roteador, um computador, um computador isolado que executa um filtro de pacotes independente (*standalone*), um software *proxy* ou um *firewall-in-a-box*, a *saber*, (um dispositivo proprietário de hardware que desempenha as funções de filtro e *proxy*. Seu propósito é eliminar do fluxo aqueles pacotes ou requisições que não se encaixam nos critérios de segurança previamente estabelecidos pela organização em sua Política de Segurança [ANONYMOUS, 2000].

Uma vez que os *firewalls* são tipicamente a primeira linha de proteção contra invasores, sua configuração deve ser cuidadosamente implementada e testada antes que conexões sejam estabelecidas entre a rede interna e a Internet. O *firewall* fundamenta-se no fato de que normalmente a segurança é inversamente proporcional a complexidade. Assim, proteger máquinas de uso geral onde são executadas diferentes aplicações e de variados portes é uma tarefa complicada, pois é muito improvável que nenhuma das várias aplicações apresente falhas que possam ser exploradas para violar a segurança do sistema. Dessa forma, fica muito mais fácil garantir a segurança isolando as máquinas de uso geral de acessos externos, usando uma barreira de proteção que impeça a exploração das possíveis falhas.

- **Sistema de Detecção de Intrusão (SDI)** - A detecção de intrusão é a prática de utilizar ferramentas automatizadas e inteligentes para detectar tentativas de invasão em tempo real. Apesar do uso dos diversos esquemas de segurança existentes, ainda existe a possibilidade de ocorrência de falhas nesses esquemas e, portanto, é desejável a existência de sistemas capazes de realizar a detecção de tais falhas e informar o

administrador da rede. Tais sistemas são conhecidos como sistemas de detecção de intrusão (SDI). Intrusões são difíceis de detectar porque existem muitas formas pela qual elas podem acontecer. Intrusos podem explorar as fraquezas conhecidas da arquitetura dos sistemas ou explorar o conhecimento de um sistema operacional para conseguir a autenticação normal de um processo. A tentativa de retirar uma falha do sistema pode introduzir uma nova falha ou expor uma falha existente, dando a oportunidade para um novo ataque.

Na Figura 2-5 é apresentada a localização do IDS e do *firewall* em uma rede local, através do uso da DMZ (*demilitarized zone*), que o termo utilizado para designar um computador ou uma pequena rede localizada entre uma rede interna confiável, como a rede corporativa, e uma rede externa não confiável, como a Internet.

Diversas outras formas de proteção estão sendo utilizadas atualmente. Cada uma apresenta seu ponto forte e também sua fragilidade. Informações mais detalhadas podem ser encontradas em [CHAPMAN, 1992][WACK & CARNAHAN, 1994][BELLOVIN & CHESWICK, 1994][ANONYMOUS, 2000].

Figura 2-5: Posicionamento de *Firewall* e Sistemas de Detecção de Intrusão (SDI) usando a técnica de DMZ.

2.4 Políticas de Segurança

Uma política de segurança é um conjunto de normas, regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos.

Um dado sistema é considerado seguro em relação a uma política de segurança, caso garanta o cumprimento das leis, regras e práticas definidas nessa política. Uma política de segurança provê formas de preservação da confidencialidade, integridade e disponibilidade da informação [ISO, 2000]

Uma política de segurança deve incluir regras detalhadas definindo como as informações e recursos da organização devem ser manipulados ao longo de seu ciclo de vida, ou seja, desde o momento que passam a existir no contexto da organização até quando deixam de existir.

As regras que definem uma política de segurança são funções das designações de sensibilidade, associadas aos recursos e informações, tais como: não classificado, confidencial, secreto e ultra-secreto, do grau de autorização das entidades tais como: indivíduos ou processos agindo sob o comando de indivíduos, e das formas de acesso suportadas por um sistema.

A implantação de uma política de segurança baseia-se na aplicação de regras que limitam o acesso de uma entidade às informações e recursos, com base na comparação do seu nível de autorização relativo a essa informação ou recurso, na designação da sensibilidade da informação ou recurso e na forma de acesso empregada. Assim, a política de segurança define o que é e o que não é permitido em termos de segurança, durante a operação de um dado sistema. A base de uma política de segurança é a definição do comportamento autorizado para os indivíduos que interagem com um sistema.

Uma quebra de segurança pode ser definida como uma ação ou conjunto de ações que vão contra a política de segurança vigente. A política de segurança é criada com as necessidades particulares de cada local. Desta forma, o que é considerado uma quebra de segurança pode variar conforme o local. A política de segurança irá definir o que pode ou não pode ser feito, por quem, sob quais circunstâncias. Um Plano de Emergência, nos quais se definem os procedimentos a serem tomados frente a uma invasão, quais são os recursos que devem ser prioritariamente protegidos, que nível de risco é aceitável, além de resolver questões éticas e polêmicas, como, por exemplo, se o administrador ou chefe tem o direito de ler o e-mail dos funcionários. Uma vez que se tenha tudo definido e que cada usuário e administrador esteja

ciente dessa política, tem-se um quadro onde é fácil determinar se uma ação é considerada uma quebra de segurança e que medidas podem ser tomadas.

2.6 Necessidade de Governança da Segurança da Informação

No ambiente empresarial globalizado atual, o significado de informação é amplamente aceito e sistemas de informação estão verdadeiramente presente em toda organização. A dependência cada vez maior das organizações de seus sistemas de informação, associada aos riscos, benefícios e oportunidades providos pela infra-estrutura de TIC, torna a Governança de TIC uma necessidade crescente. Diretorias e gerentes precisam se certificar que a TIC está em consonância com as estratégias empresariais.

Gerentes executivos têm a responsabilidade de certificar que a organização provê a todos os usuários um ambiente seguro de sistemas de informação. Além disso, organizações precisam proteger-se dos riscos inerentes ao uso de sistemas de informação, enquanto reconhecem simultaneamente os benefícios provenientes de se ter um sistema de informação seguro.

Assim, à medida que a dependência das organizações de seus sistemas de informação aumenta, percebe-se o aumento da necessidade de segurança nesses sistemas, o que acarreta necessidade de Governança da Segurança da Informação, conforme será discutido no Capítulo 5.

2.7 Considerações Finais

Para cada forma de ataque existente, há às vezes mais de uma ferramenta disponível, algumas livres para *download* na Internet, e que podem ser utilizadas por qualquer pessoa que tenha acesso a elas. Em contrapartida, existe uma grande quantidade de ferramentas e metodologias que podem auxiliar na tarefa de proteção dos sistemas.

Pode-se dizer que uma das formas de se mensurar o grau de segurança de um sistema é estabelecer uma relação entre os diversos tipos de ferramentas/métodos utilizados para a quebra de segurança em um sistema e a utilização de ferramentas/métodos conhecidos para torná-los seguros.

Todos os métodos, técnicas e ferramentas apresentadas neste capítulo geram uma enorme quantidade de dados (*logs*) acerca do ambiente que se quer proteger, conforme apresentado na Figura 2-6. Como se já não bastasse essa vasta quantidade de dados, ainda há um grande número

de alertas de segurança que precisam ser analisados, compreendidos e, na maioria dos casos, ter as respectivas medidas de correção colocadas em prática no menor tempo possível. Cabe ao administrador de segurança manter-se informado e levantar as fraquezas nos sistemas sob sua responsabilidade, transformando todos esses dados em informações e extrair conhecimentos úteis em tempo hábil. Além disso, na maioria das organizações é obrigação do administrador de segurança avaliar e implementar mecanismos que possam aumentar o grau de segurança desses sistemas.

Figura 2-6: Dados (logs) gerados pelos sistemas na tentativa de se proteger um ambiente.

O maior problema existente atualmente em relação à forma como esta análise está sendo feita é o incremento constante dos dados, tornando essa análise muitas vezes lenta e difícil.

Vale ressaltar que, baseado em experimentos citados por Russo & Shoemaker (1993), o problema onde há um excesso de informação pode ser tão prejudicial quanto a sua falta [RUSSO & SHOEMAKER, 1993]. Segundo os autores, “informações adicionais simplesmente sobrecarregam as pessoas, podendo causar inconsistência e erros”, de forma que é necessário estabelecer métodos eficientes para sua análise.

3 Sistemas de Informação

3.1 Considerações Iniciais

Como visto no capítulo anterior, a gerência das questões relativas à segurança computacional torna-se cada dia mais complexa, em função da enorme quantidade de dados que necessita ser analisada diariamente para se garantir um bom nível de segurança nos sistemas computacionais. Esses dados são provenientes de diversas fontes de dados, o que dificulta em muito esse processo. Uma vez que a tomada de decisão baseada numa grande quantidade de dados também está presente no ambiente de sistemas de informações, este capítulo apresenta os conceitos envolvendo esses sistemas na tentativa de se obter subsídios para a proposta de utilizá-los em auxílio a gerência de segurança computacional.

3.2 Conceitos e Definições para Sistemas de Informação

Em seu trabalho, Deghi (1999) apresenta um estudo aprofundado sobre as diversas definições apresentadas na literatura para Sistemas de Informação [DEGHI, 1999]. Segundo ele, infelizmente há quase tantas definições de sistemas de informação quanto o número de pessoas que escrevem sobre o assunto. Essa idéia é reforçada por Simcsik (1993) onde se encontra que, “mesmo com todos os conhecimentos de informática que possuímos hoje em dia, teríamos dezenas de definições diferentes” [SIMCSIK, 1993].

Entre as diversas definições apresentadas, destacam-se as seguintes:

- “O processo de transformação de dados em informação que são utilizadas na estrutura decisória da empresa, proporcionando, ainda, a sustentação administrativa para otimizar os resultados esperados” [OLIVEIRA, 1998];
- “Uma série de elementos ou componentes inter-relacionados que coletam (entrada), manipulam (processo), disseminam (saída) os dados e informações, e fornecem um mecanismo de *feedback*” [STAIR, 1996];
- “Um conjunto de recursos humanos, materiais, tecnológicos e financeiros agregados segundo uma seqüência lógica para o processamento de dados e a correspondente tradução em informações “ [GIL, 1995].

- “O objetivo do subsistema de informação é dar o adequado suporte informativo ao subsistema de gestão, tanto no nível gerencial, planejamento e controle, bem como no nível da execução das atividades operacionais” [GUERREIRO, 1989];
- “Um sistema integrado homem-máquina que provê informações para dar suporte às funções de operação, administração e tomada de decisão na empresa” [DAVIS, 1982];
- “Um grupo de pessoas, um conjunto de manuais e equipamentos de processamento de dados voltados para a seleção, armazenamento, processamento e recuperação de dados, com vista à redução de incertezas na tomada de decisões, através do fornecimento de informação para os executivos a tempo para que eles possam usá-las da maneira mais eficiente” [MURDICK&ROSS, 1975];

Seguindo sua definição, Gil ainda apresenta que o Sistema de Informação deve trabalhar *dados* para produzir *informações*, ou seja, a *informação* é o *dado* ou o conjunto de *dados* trabalhados [GIL, 1995]. Dessa forma, o *dado* é a matéria-prima do produto final da *informação*.

Com base nessas definições, pode-se chegar a uma representação gráfica simplificada para um sistema de informação, apresentado na Figura 3-1.

Figura 3-1: Representação gráfica simplificada de um sistema de informação

Ainda com base nas definições apresentadas, verifica-se que criar um sistema de informação efetivo requer o entendimento da empresa, de sua estrutura, de suas políticas, de seu funcionamento intrínseco, seu processo de gerenciamento e finalmente, a tecnologia da informação que permitirá que se modele o sistema. Assim, os elementos de gerenciamento, técnicos e organizacionais devem trabalhar de modo integrado para criar o sistema de informação da empresa. Muitas dessas definições enfatizam a utilização do sistema de informação na estrutura decisória da empresa.

3.3 Classificação dos Sistemas de Informação

Segundo Ein-Dor & Sevgev (1986), as informações são utilizadas pelas organizações de várias maneiras, sendo que as principais consistem nas suas operações correntes e nas tomadas de decisões administrativas [EIN-DOR & SEVGEV, 1986].

Nas operações correntes, as informações proporcionam à organização a consecução das suas atividades diárias, enquanto que nas tomadas de decisões administrativas, as informações não são utilizadas rotineiramente como nas operações. Estas são usadas especificamente para resolver determinado problema, ou seja, em conformidade com a necessidade dos gestores.

Seguindo essa linha, Bio(1994) classifica os sistemas de informação em dois principais grupos [BIO, 1994]:

- Sistemas de apoio às operações, conhecidos como *Sistemas de Informações Operacionais (SIOs)* e;
- Sistemas de apoio à gestão, conhecidos como *Sistemas de Informações Gerenciais (SIGs)*.

3.3.1 Sistemas de Informação Operacionais

Conforme observado em Bio (1994), os Sistemas de Informação Operacionais (SIOs) são sistemas processadores de transações, ou seja, sistemas que servem para o processamento de transações rotineiras [BIO, 1994].

O autor ainda divide os SIOs em duas categorias: *os sistemas processadores de transações*, tais como sistemas de folha de pagamento, compras, faturamento etc.; e *os sistemas para a tomada de decisões voltadas para a operação*, envolvendo uma reunião de muitas transações, tais como sistema de planejamento e controle de produção, custos, contabilidade etc.

Essas duas classes de sistemas se sobrepõem, uma vez que os sistemas processadores de transações envolvem, freqüentemente, alguma tomada de decisão. Por outro lado, as decisões decorrentes dos sistemas para a tomada de decisões voltadas para a operação são mais importantes e complexas, além de representar a própria razão de ser do sistema. Além disso, há uma diferença no impacto causado pelas classes de sistemas. Enquanto nos sistemas processadores de transações o impacto é sentido na eficiência das operações, nos sistemas para a tomada de decisão o impacto é sentido diretamente no resultado, ou seja, na eficácia das operações.

O autor afirma que essa classificação representa a evolução da preocupação com os sistemas nas empresas, a qual se inicia com o aperfeiçoamento dos sistemas processadores de transações, evoluindo para sistemas para a tomada de decisão e, finalmente, envolvendo os sistemas de apoio à gestão ou sistemas de informações gerenciais.

3.3.2 Sistemas de Informação Gerenciais

Ainda de acordo com Bio(1994), os Sistemas de Informações Gerenciais (SIGs) não são orientados para o processamento de transações rotineiras e sim para auxiliar o processo decisório [BIO, 1994].

Segundo Ein-Dor & Sevgev, os SIGs são aqueles sistemas que servem à administração e não às operações. Um sistema é considerado como um SIG quando é utilizado por algum gerente que o considera útil ao desempenho de seus deveres [EIN-DOR & SEVGEV, 1978] .

Um SIG é definido como um sistema para coleta, armazenamento, recuperação e processamento de informações que é usado, ou desejado, por um ou mais administradores no desempenho de seus deveres. O SIG pode ser considerado como uma *interface* dentro da organização, entre as funções de processamento de dados e de decisões administrativas.

Entende-se portanto que os SIGs têm a função de coletar dados, formatados ou não nos depósitos de dados que lhes são disponibilizados e trabalhá-los, transformando-os em informações e em conhecimento que serão utilizadas pelo gestor na sua tomada de decisão. Isso encontra-se ilustrado na Figura 3-2.

Figura 3-2: Representação simplificada para Sistemas de Informações Gerenciais (SIGs).

Segundo Guerreiro, o Sistema de Informação é impactado por definições do modelo de gestão quanto ao nível de investimentos em sistemas, caso as informações requeridas devam ser obtidas por sistemas formais ou não, conforme sejam as fases do processo decisório e os

modelos de decisão a serem atendidos, os conceitos de mensuração a serem empregados e os modelos de informação a serem configurados [GUERREIRO, 1989].

O modelo de gestão contempla três fases: *planejamento*, dividido em estratégico, tático e operacional; *execução*, que é a fase da tomada de decisão; e *controle*, traduzido em ações sobre as decisões tomadas [COSTA, 2000]. Um bom sistema de Informação deve atender o gestor em todas as fases do processo decisório.

Na fase de planejamento, o sistema de informação deve subsidiar os gestores com informações do ambiente interno e externo da organização, propiciando-lhes uma visão ampliada dos cenários futuros, que lhes permita fazer simulações e previsões de novos cenários, projetar resultados, desenvolver padrões, bem como sugerir alternativas que melhor se ajustem ao seu objetivo.

Na fase de controle, o Sistema de informação deve comparar o acontecido com o planejado, verificar as variações e os possíveis motivos dessas variações e, se possível, indicar alternativas para a correção das variações verificadas. Tudo isso com a máxima eficiência, ou seja, com benefícios maiores que os custos e na hora certa da tomada de decisão. A Figura 3-3 ilustra a integração do processo de gestão com o sistema de informação.

Figura 3-3: O processo de gestão integrado com o Sistema de Informação [CATELI, 1999].

A eficácia em um sistema de Informação pode ser avaliada pela capacidade de um sistema específico atender aos objetivos estratégicos, táticos e operacionais da empresa [MIRANDA, 1992]

Conforme observado em Horngren et all (1996), um bom sistema de informações deve contemplar os seguintes quatro fatores:

- *Controle* - O sistema deve ser capaz de controlar as operações necessárias a que se propõe, além de admitir o controle sob si mesmo;
- *Flexibilidade* - Deve ser bastante flexível, a ponto de admitir novas funções e operações;
- *Compatibilidade* - Deve ser compatível com as operações da organização, pessoal e organizacional;
- *Relação custo/benefício* - O benefício deve ser maior que o custo de aquisição, implantação e manutenção do sistema.

3.4 Tomada de Decisão

Uma decisão pode ser definida como “a escolha entre vários caminhos alternativos que levam a determinado resultado”, acrescentando como elemento básico que, para “um adequado processo decisório é necessário ter um sistema de informação eficiente”[OLIVEIRA, 1998].

Em uma outra definição, tem-se que decisão pode ser vista como “uma descrição de um futuro estado de coisas, podendo essa descrição ser verdadeira ou falsa em função dos elementos que o tomador de decisões tem em mãos e que lhe permite ter uma visão factual da situação presente e futura” [CUSTÓDIO, 1981].

Como base nas conclusões de Degui (1999), uma das principais funções de um executivo dentro de uma empresa é o de tomar decisões para que se atinjam os resultados desejados dentro de ambientes que mudam rapidamente, baseado em informações obtidas de múltiplas fontes [DEGHI, 1999]. Para tanto, esse executivo deve ter uma compreensão da empresa, seu funcionamento interno e seu relacionamento com o meio ambiente externo, utilizando-se de mecanismos que permitam identificar uma situação e seus eventuais problemas, estruturando-os, encontrando as potenciais soluções e decidindo-se por uma delas.

Uma decisão deve ser precedida por um processo de tomada de decisão que, de acordo com Russo & Schoemaker (1993), pode ser dividida em quatro elementos principais, que os autores chamam da espinha dorsal desse processo [RUSSO & SCHOEMAKER, 1993]. São eles:

- 1) Estruturar a questão;
- 2) Colher informações;
- 3) Chegar a conclusões;
- 4) Aprender com o resultado (*feedback*).

Usando outra categorização, este processo é apresentado em três fases principais [CUSTODIO, 1981]:

- 1) Descoberta e reconhecimento das situações que exigem uma tomada de decisão;
- 2) Descoberta de cursos de ação possíveis;
- 3) Escolha de um entre vários cursos de ação identificados.

Apesar de se imaginar a relação de precedência entre as fases, este ciclo é mais complexo, e “cada fase caracteriza, numa situação decisória, um complexo processo de tomada de decisão em si mesmo” [CUSTODIO, 1981]. Custodio (1981) ainda acrescenta que, portanto, um problema “gera subproblemas que, por seu turno, possuem todas as três fases, e assim por diante”.

Conforme observado em Oliveira (1998), existem alguns fatores de influência dentro do processo de decisão, entre os quais se encontram-se os seguintes:

- Complexidade evolutiva do mundo moderno, apresentando cada vez mais variáveis complexas;
- Redução do tempo disponível para a tomada de decisão pela influência de algumas variáveis, tais como a concorrência;
- Velocidade das comunicações;
- Melhoramentos nos processos de informações e com expectativa de resultados em curto prazo.

Segundo Tachizawa (1989), os sistemas de informação “como geradores de informação decisória, devem ser estabelecidos como processos de comunicação mediante os quais são fornecidos os elementos básicos para as decisões nos vários pontos da empresa” [TACHIZAWA, 1989]. Tachizawa (1989) menciona ainda que enquanto a decisão exige um fluxo de informações

de entrada, a ação conduz a um fluxo de saída que produz uma tradução em termos operacionais da decisão tomada. Poder-se-ia pensar então, segundo o autor, a informação sendo transformada em atividades, tendo a decisão o papel intermediário, terminando com o controle da realização das decisões tomadas e uma eventual correção, conforme apresentado na figura a seguir.

Figura 3-4: Relação entre decisão, atividades e controle.

É possível deduzir que a eficácia das decisões depende da informação e do modo como ela é tratada e percebida através dos sistemas de informação [DEGHI, 1999]. Isto é verdade particularmente nas chamadas decisões não programadas, onde se lidam com situações incomuns ou excepcionais, e as regras e conexões não são bem definidas [STAIR, 1996].

Outro modo de associar a informação à tomada de decisão pode ser representada graficamente conforme Figura 3-5 [OLIVEIRA, 1998].

Normalmente, deve-se levar em conta também o tipo de modelo de decisão que será adotado em uma determinada situação. Um modelo de decisão é adotado de acordo com a natureza da ação decisória. A escolha do modelo mais adequado dependerá do conjunto de variáveis envolvidas, do grau de controle sobre as variáveis, do nível de certeza associado à decisão, dos objetivos de quem decide, entre outros fatores [BEUREN, 1998].

Figura 3-5: Interação da Informação com o Processo Decisório [OLIVEIRA, 1998].

Uma descrição dos diferentes tipos de modelo de decisão é encontrada em Beuren (1998), a saber:

- **Modelos de decisão de simulação** - São modelos que permitem a formulação e avaliação de alternativas, antes da implementação de qualquer uma delas. O responsável pela decisão pode criar cenários futuros possíveis e testar alternativas;
- **Modelos de decisão de otimização** - Esses modelos são estruturados, geralmente, por relações matemáticas, para selecionar uma única alternativa ótima, tendo como orientação a função-objetivo do responsável pela decisão;
- **Modelos de decisão heurísticos** - São aqueles que, por meio de rotinas, geralmente computadorizadas, permitem encontrar uma solução satisfatória. A heurística é um conjunto de decisões que elimina alternativas inadequadas para solução de problemas complexos.

A concepção de um sistema de informações que auxilie o gestor a melhorar suas decisões não depende apenas da identificação dos modelos decisórios dos gestores e de suas necessidades informativas. Muitas vezes, faz-se necessário repensar o próprio modelo de decisão, além de utilizar informação adicional para determinar a probabilidade de ocorrência de cada estado da natureza, a fim de reduzir o problema da incerteza [BEUREN, 1998].

Para que um sistema de informações gerenciais seja eficiente, há a necessidade de que exista rapidez no fluxo de informações de determinados pontos aos centros de decisão [OLIVEIRA, 1998]. Beuren (1998) cita que uma segunda premissa diz que “conhecer a mensuração das informações é importante na determinação das características, tais como valor, custo, qualidade e validade das informações”, preocupação constante dos gestores e tomadores de decisão [BEUREN, 1998]. Tais premissas envolvem mais do que rapidez de hardware e de um planejamento eficiente. Exige-se também que, o desenvolvimento das aplicações computadorizadas, que darão sustentação a este fluxo de informações, seja feito em tempos cada vez menores, com uma taxa de erro também menor e com custos mensuráveis.

3.5 Sistemas de Informação e Estruturas de Decisões

O Modelo de Informações empresarial relaciona as informações com a sinergia necessária para gestão dos negócios e das funções empresariais. As informações são estruturadas nos níveis operacional, gerencial e estratégico, visando atender todos os requisitos funcionais estabelecidos e necessários. Cada função empresarial pode ser desmembrada ou decomposta em seus respectivos módulos. Nesse caso, conforme representado na Figura 3-6, a ênfase não está na ação e sim nas informações necessárias, relatando as Informações Estratégicas, relacionada no nível macro com o meio ambiente interno e externo, as Informações Gerenciais ou Táticas - agrupadas, sintetizadas, totais, percentuais, acumuladas, plurais etc, e as Informações Operacionais - do dia-a-dia, pontuais.

Figura 3-6: Os tipos de planejamento nas empresas.

Com apoio de uma base de dados unificada, as estruturas empresariais e respectivos níveis hierárquicos passarão a ser mais dinâmicos, eliminando barreiras e divisões que separem a alta administração do corpo gestor e do corpo técnico, provendo maior integração e envolvimento de todos, preferencialmente focados no negócio da Empresa.

Além dos procedimentos e processos de seleção e organização das informações para sua efetiva utilização, os gestores deveriam ter sistemas de informações efetivos, que processem o grande volume de dados gerado e produzam informações e conhecimentos válidos, úteis, de boa qualidade e oportunos para os negócios da organização.

As informações e o conhecimento gerados a partir dos dados históricos da empresa propiciarão a identificação de problemas e necessidades nos níveis estratégico, tático e operacional, bem como poderão fornecer subsídios para avaliar o impacto das diversas decisões a serem tomadas.

3.6 Considerações Finais

O processo de administração nas empresas utiliza a informação como apoio às decisões através de sistemas de informação. Os sistemas de informação, como geradores de informações de caráter de decisão, devem ser estabelecidos como processos de comunicação mediante os quais são fornecidos os elementos básicos para as decisões nos negócios. Ainda nesse caminho, Simcsik (1993) considera que a tomada de decisão passa pela correta modelagem de informação, definindo tomada de decisão da seguinte maneira: “o processo de organização gráfica que descreve e define o domínio do problema e o conceitua conforme normas bem definidas focalizando o mundo real na busca da formalização do conhecimento e da sistematização do modelo atual” [SIMCSIK, 1993]. Assim, segundo Simcsik (1993), “o modelo se transforma em uma ferramenta de comunicação de todos os envolvidos no trabalho, acrescentando que a árvore de decisão pode ser considerada uma modelagem da informação”.

A abordagem de sistemas de informação procura respeitar alguns princípios, dentre os quais se destacam os de que seja uma “efetiva fonte de ajuda ao tomador de decisão”, além de poder auxiliar na definição de “melhores estratégias para apoio à decisão” e que “tenha efetiva integração das fontes de dados e dos modelos, incluindo interfaces adequadas com o processamento de transações e com os sistemas de gerenciamento de base de dados”

[OLIVEIRA,1997]. Esses pontos são importantes dentro das considerações a serem feitas ao longo deste trabalho.

4 Extração de Conhecimento de Base de Dados

4.1 Considerações Iniciais

Os administradores de segurança computacional vivenciam atualmente o grande problema da tomada de decisão em tempo hábil com base numa grande quantidade de dados.

Dados em estado bruto raramente oferecem benefícios diretos para o processo de tomada de decisão. Tradicionalmente a análise destes dados está restrita a um processo manual, na qual os analistas devem estar intimamente familiarizados e, com ajuda de técnicas estatísticas, fornecem relatórios e sumários aos responsáveis pelas tomadas de decisões. O maior problema existente neste tipo de análise tradicional é o incremento constante dos dados, tornando essa atividade muitas vezes lenta e difícil. Uma comunidade de pesquisadores interessados em fazer uma “análise automática da informação” está trabalhando em uma área denominada *Extração de Conhecimento de Base de Dados* (*Knowledge Discovery in Databases – KDD*) [FELIX, 1998].

Neste capítulo será discutido, primeiramente, o que se entende por “conhecimento”, por ser a meta a ser atingida com KDD. Finalmente, serão vistos alguns dos principais problemas e conceitos encontrados no processo KDD.

4.2 O Conhecimento

Durante várias épocas da história do ser humano, o termo “conhecimento” tem sido um tema filosófico amplamente debatido. Segundo Carbonell (1987), o conhecimento é definido como a informação interpretada, categorizada, aplicada, revisada e que possui certo valor para o usuário [CARBONELL, 1987].

De uma forma geral, no processo de Aquisição de Conhecimento de Base de Dados, os dados são a matéria prima bruta. No momento em que o usuário atribui algum significado especial aos dados, estes passam a ser uma informação. Quando os especialistas do domínio do problema elaboram uma norma ou regra, a interpretação de confrontação entre um dado fato (informação) e essa regra constitui um conhecimento. Uma hierarquia entre os dados, a informação e o conhecimento existente em uma base de dados, observando seu volume e o valor

que os responsáveis pelas tomadas de decisões dão a essa hierarquia, pode ser visto na Figura 4-1.

Certamente, o conhecimento pode apresentar diversas e complexas formas de representação, dependendo, na maioria das vezes, da forma como ele é adquirido, sendo isto um dos principais problemas relacionados com desenvolvimento de sistemas inteligentes de um modo geral.

O processo de Aquisição de Conhecimento (AC) envolve a extração, interpretação e representação do conhecimento de um dado domínio e é considerado muito difícil. A AC envolve um consumo de tempo considerável, o que a torna um componente extremamente caro no desenvolvimento de Sistemas Inteligentes [FELIX, 1998].

Figura 4-1: Pirâmide do Processo de Conhecimento

As dificuldades na AC se originam, em parte, pela falta de uma boa comunicação com especialistas do domínio, falta de tempo das pessoas envolvidas no processo de AC, falta de habilidade da equipe de engenheiros do conhecimento para entender o especialista do domínio, dificuldades quanto às terminologias empregadas e também falta de habilidade para mapear um domínio de conhecimento para um esquema de representação apropriado para o computador. Com o propósito de solucionar algumas dessas dificuldades, pesquisadores têm sugerido que a delimitação, aquisição e, em alguns casos, a representação do conhecimento se realizem de uma forma mais automática.

Vários esforços estão sendo feitos para automatizar o processo de AC, entre eles destacam-se os seguintes: editores inteligentes, uso de processamento de linguagem natural para

comunicação direta com o sistema e aplicações de aprendizado de máquina para apoiar a aquisição de conhecimento baseada em exemplos passados.

A Extração de Conhecimento de Base de Dados pode cooperar na solução de alguns dos problemas relacionados com a AC, procurando padrões interessantes em base de dados de uma forma mais automática, obtendo vantagens como o refinamento de tipos específicos de conhecimento, redução de custos (tempo e dinheiro) e de recursos humanos envolvidos no desenvolvimento desses sistemas. Podem, ainda, ajudar na padronização de alguns dos processos de AC.

Um dos principais objetivos do KDD é apoiar os especialistas do domínio na obtenção de conhecimento de base de dados, envolvendo diferentes áreas, tais como Estatística, Base de Dados, Inteligência Artificial e Computação Gráfica. Para poder atingir tais objetivos, o processo KDD é constituído de várias etapas e elementos de apoio que serão apresentados a seguir.

4.3 Processo de Extração de Conhecimento de Base de Dados

Segundo Fayyad (1996a), o processo KDD é definido como um processo não trivial de identificação válida, recente, potencialmente útil de padrões compreensíveis embutidos nos dados [FAYYAD, 1996a].

Dada a definição anterior de KDD, o “conhecimento” é definido em termos dependentes do domínio relacionados fortemente em medidas de utilidade, originalidade e compreensão. O termo “padrões” denota os conjuntos de modelos ou padrões que representam alguma abstração de um subconjunto dos dados em alguma linguagem. Um outro termo importante na definição anterior é o “processo” que envolve as etapas de análise, experimentação, iteração, interação com o usuário, normalização, padronização e avaliação, que juntas formam todas as etapas do processo KDD que serão discutidas a seguir [FAYYAD, 1996b] [FAYYAD, 1996C].

4.3.1 Etapas do Processo de Extração de Conhecimento de Base de Dados

O processo KDD é composto por várias etapas, que vão desde a definição e compreensão do domínio, seleção e amostragem dos dados, limpeza, enriquecimento e preparação dos mesmos, *Data Mining*, até uma etapa na qual os resultados são interpretados e avaliados pelos especialistas do domínio, a saber, o usuário final ou responsável pela base de dados.

Baseado na definição de Fayyad (1996b), *Data Mining* pode ser entendido como uma etapa do processo KDD, que envolve a aplicação de ferramentas de busca para encontrar padrões em conjuntos de dados. Uma boa definição e compreensão do domínio, definindo os objetivos a atingir, são de fundamental importância para o êxito da aplicação o KDD.

Devido ao fato de existir uma imensa variedade de problemas e diferentes tipos de base de dados é praticamente impossível definir uma metodologia única para a Extração de Conhecimento de Base de Dados. Dependendo do problema, existe em algumas situações a necessidade de se criar “subetapas” dentro de cada etapa. A seguir serão discutidas, de uma forma geral, todas as etapas do processo KDD, com base no trabalho de Felix (1998):

1. **Definição e Compreensão do Domínio** - A definição dos objetivos a atingir é um dos aspectos fundamentais a serem considerados para o êxito do processo de Extração de Conhecimento de Base de Dados. Essa definição é geralmente realizada pelos especialistas do domínio ou proprietários da base de dados, com apoio de especialista do processo KDD (engenheiro de conhecimento do processo de AC), a fim de definir o domínio da aplicação (região limitada e definida de uma aplicação), o conhecimento prévio relevante, a viabilidade e custos de aplicação, duração do projeto, resultados esperados, entre outros. Uma análise cuidadosa do problema é requerida nessa etapa para uma melhor compreensão do domínio;
2. **Seleção e Criação das Bases de Dados** - Esta etapa consiste em selecionar ou dependendo do caso, criar uma nova base de dados usando conjuntos de elementos de várias fontes de dados. Isso envolve considerações sobre a homogeneidade dos dados bem como a identificação das fontes desses dados, aos quais podem ser internas (por exemplo, base de dados do departamento de produção, de finanças, etc) ou externas (por exemplo, Internet, livros, etc.). Nessa etapa consegue-se uma melhor identificação dos gargalos do domínio, considerando, entre outros aspectos, o seguinte: viabilidade do projeto, tempo de execução, possíveis resultados esperados etc;
3. **Compreensão dos Dados** - Em muitas aplicações é importante interpretar os dados para um melhor entendimento do domínio. Possíveis soluções incluem a seguinte: consultas usando a linguagem SQL (*Structured Query Language*), ferramentas OLAP (*On-Line Analytical Processing*), representações gráficas, visualização dos

dados, cálculos estatísticos etc. Vale ressaltar que a visualização tem um papel importante nessa etapa, já que permite que sejam incorporadas diretamente a capacidade de percepção visual e entendimento, as capacidades de cálculo e associações de uma forma mais compreensível;

4. **Seleção das amostras mais representativas** - A extração direta de conhecimento a partir de grandes bases de dados pode se tornar uma tarefa inviável, principalmente pela limitação do número de registros que os algoritmos de Aprendizado de Máquina podem manipular. Esse grande volume de dados pode gerar um espaço de busca de padrões combinatorialmente imenso. Além disso, a busca de conhecimento em grandes bases de dados pode ocasionar, na maioria das vezes, um aumento na chance de encontrar padrões pouco significativos e até mesmo espúrios. Segundo Mannila (1997), a seleção das amostras mais representativas consome cerca de 80% de todo o tempo do processo KDD [MANNILA, 1997]. A escolha de uma amostra que possa refletir com maior fidelidade possível a base de dados é de suma importância para as demais etapas do processo KDD. Seleções e amostras pouco significativas podem resultar em padrões imprecisos ou sem valia;
5. **Enriquecimento do conjunto de dados** - É necessário, em certas ocasiões, agregar dados externos quando o conjunto de dados selecionados necessita deles para poder atingir metas determinadas no início do processo. Por exemplo, nas pesquisas de mercado, é importante agregar o CEP ou sexo das pessoas para saber de certa forma o público alvo a atingir e evitar, por exemplo, que propaganda de absorventes chegue pelo correio com o nome de uma pessoa do sexo masculino.
6. **Limpeza do conjunto de dados** - Essa etapa inclui, principalmente, a padronização e eliminação de ruídos gerados de diversas formas nos conjuntos de dados. A geração de ruídos é devida a migrações de um sistema para outro, quedas de tensão na hora do processamento, desligamento do computador tendo arquivos abertos etc;
7. **Preparação do Conjunto de dados** - Em algumas ocasiões, é necessário fazer certas adequações no conjunto de dados de acordo com a técnica de *Data Mining* a ser usada;
8. **Data Mining**: É importante considerar previamente que os algoritmos de Aprendizado de Máquina usados por *Data Mining* necessitam que os conjuntos de dados estejam em um determinado formato para poderem trabalhar. Devido a sua

complexidade e importância, a etapa de *Data Mining* pode ser dividida em três subetapas: redução de instâncias e atributos (*features*), descoberta de padrões e pré-avaliação do conhecimento obtido por parte do especialista do KDD;

9. **Avaliação do Conhecimento Descoberto** - O processo KDD não termina quando os padrões nos dados de entrada são descobertos. É preciso que o especialista do domínio entenda e possa julgar a utilidade do conhecimento extraído. A avaliação do modelo é uma tarefa bastante difícil que envolve, entre outras coisas, a utilização de técnicas de visualização para auxiliar o especialista de domínio a decidir a importância e utilidade do conhecimento extraído, bem como na remoção de padrões redundantes e irrelevantes. Para verificar o produto final do processo KDD – o conhecimento – a interatividade do especialista do KDD com o especialista do domínio é bastante acentuada nessa etapa. Portanto, os resultados obtidos podem acarretar mudanças a quaisquer das fases anteriores ou, ainda, o recomeço de todo o processo KDD;
10. **Consolidação e Utilização do Conhecimento Extraído** - A consolidação do conhecimento extraído pressupõe a verificação e solução de potenciais conflitos com o conhecimento existente antes de o processo KDD ser iniciado. O conhecimento pode ser organizado pelo especialista KDD dentro de um modelo existente na aplicação ou simplesmente documentação e informando ao especialista do domínio, uma vez que é considerado útil nas tomadas de decisões. É importante destacar que as bases de dados são dinâmicas, sofrendo mudanças constantes ao longo do tempo e conseqüentemente alternando também o conhecimento. Deste modo, o processo KDD é também dinâmico, sendo convenientemente executá-lo periodicamente;

4.3.2 Elementos de Apoio ao Processo de Extração de Conhecimento de Base de Dados

Nesta seção serão abordados três dos principais elementos de apoio ao processo KDD: *Data Warehouse*, Técnicas Estatísticas e Visualização de Dados, além do Data Mining. Esses elementos podem ser considerados como ferramentas de auxílio neste processo, devido ao fato de que, em muitas ocasiões, seu uso faz com que o especialista do KDD encontre menos dificuldade no decorrer do processo.

Embora não seja estritamente necessário usar *Data Warehouse* dentro do processo KDD, na prática, é conveniente seu uso, principalmente em base de dados de grande porte, para qual se necessitam de acesso rápido aos dados e, sobretudo, de uma normalização dos mesmos para facilitar o trabalho do especialista do processo KDD. Por outro lado, as técnicas estatísticas têm um papel importante de apoio às etapas do processo KDD, principalmente na compreensão do domínio, seleção de amostras e redução de atributos, ao se procurar correlações entre eles. O terceiro elemento que será abordado é a visualização dos dados que praticamente dá apoio a todas as etapas do processo KDD, mostrando de maneiras mais compreensíveis os resultados gerados em cada uma das etapas do processo. Uma melhor explicação desses três elementos será vista a seguir.

4.3.2.1 Data Warehouse

O conceito original de *Data Warehouse (DW)* ou Repositório de dados foi apresentado por William H. Inmon (1997) e popularizado pela IBM com o termo *Information Warehousing*. Nessa definição, o *Data Warehouse* é apresentado como um banco de dados “orientado a assunto, integrado, passível de variação conforme o tempo, uma coleção não volátil de dados com suporte a processos de gerenciamento de tomada de decisões”. Seu uso como modelo de infra-estrutura para o suporte à tomada de decisão tem quatro objetivos fundamentais:

- Proteger os sistemas de produção de dados e informação do acesso indiscriminado de usuários, que poderiam afetar o desempenho desses sistemas;
- Prover um ambiente de informação protegido e bem administrado para auxiliar o processo de tomada de decisões, já que representam um ativo importante para a empresa;
- Construir um modelo de dados corporativo que permita uma padronização na manipulação da informação, tanto nos sistemas de produção, como nos sistemas para o suporte à tomada de decisão;
- Manter independência entre os processos dos usuários e os da administração da informação, definindo-os como problemas independentes.

Estes objetivos marcaram o ponto de partida para que se desenvolvessem, de uma maneira prática e comercial, as diversas estratégias de implementação desse tipo de ambiente.

Data Warehouse é uma base de dados voltada ao suporte na tomada de decisão de usuários finais, derivado de outras diversas bases de dados operacionais, segregado de um ambiente transacional (*On-Line Transaction Processing - OLTP*) [AMARAL, 1997]. Um *Data Warehouse* pode ser visto como um conjunto de diversas tecnologias, tais como, plataformas de hardware, ferramentas de extração e conversão de dados, base de dados voltadas para consultas complexas, ferramentas inteligentes de prospecção e análise de dados e ferramentas de administração e gerenciamento de base de dados.

Embora as tecnologias incorporadas em um ambiente de *Data Warehouse* não sejam novas, as que mais evoluíram na última década foram as seguintes:

- Sistemas gerenciadores de bases de dados distribuídas que suportam processamento paralelo;
- Produtos de conversão de dados operacionais;
- Tecnologias cliente/servidor que permitem acesso a dados distribuídos em múltiplas plataformas;
- Integração de ferramentas de análise e relatório em ambiente de escritório (*desktop*).

Criar um *Data Warehouse* não é uma simples questão de tecnologia de base de dados ou processadores paralelos. Criar um *Data Warehouse* envolve planejamento e modelagem (que são aspectos muitas vezes deixados em segundo plano, mas que garantem a qualidade dos dados, que é um fator crítico para o sucesso), integração de diferentes produtos de software e uma contínua atualização e refinamento.

Uma solução bem projetada de *Data Warehouse* objetiva satisfazer as necessidades de análise de informações dos usuários, como monitorar e comparar as operações atuais com as passadas, além de prever situações futuras. Ao transformar, consolidar e racionalizar as informações dispersas em diferentes bases de dados e plataformas, um *Data Warehouse* permite que sejam realizadas análises estratégicas bastante eficazes em informações antes inacessíveis ou subaproveitadas.

A comunidade de base de dados desenvolveu ferramentas para análise de *Data Warehouse*, chamadas de Processamento Analítico em Linha (*On-line Analytical Processing – OLAP*), para obter informações destinadas à tomada de decisões táticas diárias da organização. As ferramentas OLAP enfocam a análise multidimensional de dados de modo superior aos

mecanismos de “resumo” (*summary*) e “lotes encaixantes” (quebra ou *break-down*) entre dimensões oferecidas pelas ferramentas tradicionais. A partir de todos estes elementos envolvidos no *Data Warehouse*, o especialista KDD aproveita essas bases de dados normalizadas, sem ruídos e nos quais foram feitos diversos tipos de consulta, pode selecionar só os atributos necessários baseados nas considerações do especialista do domínio.

Os sistemas clássicos de Banco de Dados, que operam em nível de transação - OLTP (*On-line transaction processing* – processamento de transação *on-line*), são modelados e organizados em torno das aplicações da empresa. No caso do *Data Warehouse*, os dados operacionais são considerados dados primitivos que precisam ser primeiramente tratados para depois gerar informações úteis para determinados assuntos de interesse para os negócios da empresa, tal como o nível de influência de marketing para uma determinada classe consumidora de um determinado produto. Este tratamento dos dados pode se dar através de agregação, somatória, mediana, etc.

A integridade dos dados pode ser considerada a característica mais importante do *Data Warehouse*. A fase de verificação de integridade ocorre quando os dados passam do nível operacional para o *Data Warehouse*. O processo de inserção dos dados no *Data Warehouse* é conduzido sempre tendo em vista a preocupação de se eliminar muitas inconsistências das aplicações no que se refere a codificação, convenções de atribuição de nome, atributos físicos, unidades de medida etc. Ao proceder a codificação para o *Data Warehouse*, deve-se assegurar que ela seja feita de forma consistente e independente da aplicação de origem [HIROSE, 2000].

Dentro do *Data Warehouse* os dados armazenados são não voláteis. Numa base operacional, os dados primitivos são acessados com regularidade e tratados com um registro cada vez e podem sofrer atualizações no decorrer de períodos. Porém, os dados existentes no *Data Warehouse* possuem características diferentes. São carregados e armazenados em grande quantidade, e depois acessados; porém, a sua atualização não é feita dentro do ambiente de *Data Warehouse*.

Outra característica do *Data Warehouse* é que seus dados são variáveis em relação ao tempo. Se uma empresa tivesse dados a respeito de um cliente e este tivesse mudado de endereço, em sua base operacional (OLTP) estariam representados os últimos dados atualizados a seu respeito. Porém, em um ambiente de *Data Warehouse*, os dados antigos do endereço seriam mantidos e não haveria atualização dos mesmos, o que há é a inclusão de novos dados a respeito desse cliente, com o tempo associado às informações, mantendo-se assim um histórico

das informações a seu respeito dentro da empresa, o que será útil para se levantar algum interesse de negócio da empresa.

Data Mining

Data Mining, ou mineração de dados, é outra tecnologia que compõe a tecnologia de Data Warehousing. O *Data Mining* surgiu através dos conceitos da inteligência artificial, juntamente com o conceito de extração de conhecimento em banco de dados ou *KDD*.

O *Data Mining* pode ser definido como “o processo de extrair informação válida, previamente desconhecida e de máxima abrangência, a partir de grandes base de dados, usando-as para efetuar decisões cruciais” [CHEN et al, 1997]. Segundo esses autores, a tecnologia *Data Mining* vai muito além da simples consulta e descobrimento de relacionamentos em um banco de dados. Na realidade, o *Data Mining* busca a descoberta de padrões e anomalias em bases complexas de dados.

O principal objetivo do *Data Mining* é a descoberta de informações e conhecimento, através do reconhecimento de novos fatos e das relações em uma base de dados. O papel mais importante do *Data Mining* é saber onde utilizar as informações descobertas no processo de busca, ou seja, saber o objetivo da análise dos dados [CHEN et al, 1997].

O *Data Mining* pode ser utilizado com os seguintes objetivos:

- *Objetivo explicatório*: explicar algum evento ou medida observada;
- *Objetivo confirmatório*: confirmar uma hipótese; e
- *Objetivo exploratório*: analisar os dados, buscando relacionamentos novos e não previstos.

Na busca de novas informações, o *Data Mining* realiza, na ordem em que for necessário, as seguintes tarefas:

- *Associação*: a ferramenta tenta encontrar relacionamentos entre os dados;
- *Agrupamento*: as informações são segmentadas em grupos homogêneos, com base em algumas características;
- *Classificação e regressão*: os dados são classificados através de modelos de comportamento;
- *Padrões sequenciais*: a ferramenta tenta descobrir eventos relacionados que ocorreram ao longo de um período de tempo;

- *Séries temporais similares*: tenta identificar séries similares ao longo de um período de tempo.

O sucesso do processo depende da adequação de *Data Mining* com o tipo de problema que se quer solucionar. Para que o *Data Mining* possa executar suas tarefas, é necessária a utilização de algumas técnicas, das quais destacam-se as seguintes:

- Raciocínio baseada em casos;
- Modelagem de dependência;
- Descoberta de regras;
- Pontuação;
- Detecção de desvios;
- Processamento de sinais;
- Fractais; e
- Redes neurais.

Essas técnicas podem ser usadas em conjunto ou separadamente, dependendo do problema que a ferramenta vai resolver.

Atualmente a técnica de mineração de dados é aplicada em várias ciências, tais como economia, administração (marketing e finanças), medicina etc.

O resultado da análise é divulgado por meio de relatórios, gráficos ou meios alternativos de visualização, que é a técnica utilizada para se analisar os dados de forma gráfica.

4.3.2.2 Métodos Estatísticos no Tratamento dos Dados

A Estatística é a área de matemática que estuda a coleta, organização e interpretação de dados numéricos, especialmente a análise de características da população por inferências a partir de amostras [GLYMOUR, 1997].

As ferramentas estatísticas de hoje trabalham com um rico conteúdo de pesquisa teóricas e metodológicas, onde alguns são mostrados na Tabela 4-1 [GLYMOUR, 1997]. Os estatísticos têm desenvolvido uma infra-estrutura teórica para suportar seus métodos e linguagens para descrever uma aproximação dos modelos, quantificando as incertezas associadas às inferências a partir dos dados.

Tabela 4-1: Áreas de Trabalho da Estatística

Área Estatística	Descrição de Atividades
Desenho de experimentos e amostragem	Como selecionar casos onde se tem a liberdade de escolha
Análise exploratória de dados	Geração de hipótese antes do teste de hipótese
Estatística gráfica	Visualização de dados
Modelagem Estatística	Técnicas de classificação e regressão
Inferência estatística	Técnicas de estimativa e previsão

4.3.3.3 Visualização dos Dados

As ferramentas de visualização de dados estão se tornando cada vez mais importantes no processo KDD, pois permitem aumento na capacidade de análise e da interpretação dos resultados obtidos [REZENDE, 1998]. Existem certas abordagens que tentam unir visualização com a etapa de *Data Mining*, como a de Peter Brooks [BROOKS, 1997], que diz o seguinte: “a visualização dos dados por si só pode ser uma forma completa de aplicação de *Data Mining*”.

Por outro lado, na maioria dos casos a visualização de dados pode ser usada como uma ferramenta exploratória na análise de dados. Um especialista em visualização pode construir diferentes exibições de dados para determinar os gráficos mais significativos. O número e tipo de exibições de dados que estão sendo gerados dependem da capacidade ou discernimento do especialista em visualização.

A visualização dos dados permite que sejam incorporadas informações diretamente à capacidade de percepção do especialista do domínio. Existem algumas restrições de visualização, a saber: muitas pessoas não têm orientação espacial, principalmente em gráficos 3D ou 4D; pessoas daltônicas que não conseguem distinguir as partes que compõem um gráfico quando são diferenciadas por cores; aspectos de hardware como resoluções dos monitores, suporte de cores e desempenho do computador podem restringir e limitar a visualização desejada.

4.4 Considerações Finais

Neste capítulo foi apresentada uma visão geral do processo KDD. Este processo é composto por várias etapas, nas quais cada uma delas é extremamente importante para se obter

um conhecimento com alto grau de confiança. Além disso, é importante ressaltar que dentro de cada etapa do processo podem existir outras subetapas.

Existe uma confusão entre os pesquisadores acerca do significado exato dos termos *Data Mining* e KDD devido a que alguns deles o consideram como sinônimos. Conforme apresentado por Felix (1998), foi proposto na Primeira Conferência Internacional sobre Descoberta de Conhecimento e *Data Mining* realizada em Montreal, Canadá em 1995, que o termo KDD seja usado para descrever o processo total de extração de conhecimento a partir dos dados [FELIX, 1998]. Por outro lado, o termo *Data Mining* deve ser usado exclusivamente para o estado de descoberta de padrões dentro desse processo.

Vale ressaltar que KDD não é uma tecnologia nova. É um campo multidisciplinar de pesquisa, no qual Aprendizado de Máquina, Estatística, Tecnologias de Base de Dados, Sistemas Inteligentes e Ferramentas de Visualização contribuem no seu processo, como é apresentado na Figura 4-2.

Figura 4-2: Áreas de Apoio ao KDD

5 Necessidade de um Modelo para Governança da Segurança da Informação

5.1 Considerações Iniciais

Os capítulos anteriores apresentaram uma revisão de literatura para o termo Segurança Computacional, apontando as dificuldades encontradas no cenário atual, para Sistemas de Informação e para o processo de extração de conhecimento de bases de dados. Foi apresentado também como as organizações vêm utilizando os Sistemas de Informações Gerenciais e sua estrutura de decisão dividida em nível operacional, nível tático e nível estratégico. Com base nas informações apresentadas, este trabalho propõe que as tarefas relacionadas com gerenciamento de segurança computacional utilizem as experiências do processo decisório no enfoque de negócios, uma vez que os dois processos apresentam características similares.

Este trabalho identificou que, nos dois casos, torna-se imprescindível que o gestor possa e saiba decidir com certo grau de segurança assertiva em um tempo cada vez menor e com base em uma quantidade de dados cada vez maior.

Seja de forma sistêmica e prática ou de forma científica, o gestor deve sempre buscar a melhor das alternativas para suas decisões. De forma sistêmica, o gestor usa a experiência acumulada e as observações do ambiente para fazer seu cenário decisório ou modelo decisório. Este trabalho considera que isso é válido não somente para o processo decisório no enfoque organizacional, mas também para o gerenciamento de segurança computacional. Entretanto, em função do grande número de dados provenientes das mais diversas fontes no cenário atual, boa parte das decisões precisa ser tomada de forma estruturada e científica e não mais de forma sistêmica. Isso é válido tanto para as questões de segurança computacional quanto para o processo de tomada de decisões estratégicas nas organizações.

No enfoque organizacional, de forma científica o gestor pode utilizar modelos de Governança Organizacional apoiados por ferramentas disponíveis na *teoria da decisão*, que por sua vez utiliza ferramental de outras ciências, tais como: matemática, estatística, filosofia, administração etc.

Considerando a dependência atual das organizações do correto funcionamento de sua área de Tecnologia da Informação e Comunicação (TIC) para a realização de sua missão, as ações relacionadas com a Segurança Computacional estão deixando cada vez mais de serem tratadas apenas como uma responsabilidade da área de TIC e estão sendo vistas como um desafio para os gestores das organizações. Os gestores atuais estão cada vez mais necessitados de incorporar as responsabilidades relacionadas com a Segurança Computacional em seu processo de tomada de decisão.

Apesar de a literatura apresentar vários guias e recomendações para o gerenciamento de segurança, partindo de um bom detalhamento técnico e alcançando até princípios gerenciais, não foi encontrado um modelo que alcance todos os níveis organizacionais e que ajude a determinar o que deva ser feito e quem é responsável por fazê-lo. A ausência desse modelo implica que os gestores não são abastecidos com o conhecimento desejável no momento do planejamento estratégico da organização, para alocar recursos para a segurança da informação e, ainda, para medir o retorno do investimento feito nessa área.

Como será visto neste capítulo, neste trabalho propõe-se um modelo de Governança da Segurança da Informação baseado na utilização dos conceitos da estrutura de decisão de sistemas de informação e em modelos de Governança de Tecnologia da Informação e Comunicação. O modelo proposto neste trabalho irá prover aos gestores uma abordagem para que possam, de forma estruturada, ter a área de segurança computacional alinhada com o negócio da organização. De forma estruturada, o modelo permitirá que se consiga correlacionar os dados para obter informações e, a seguir, gerar o conhecimento que possibilite aos gestores planejar e programar a tomada de decisão com a eficiência e a eficácia exigidas pela competitividade e pelos acordos de nível de serviço necessários no cenário atual.

5.2 Governança de Tecnologia da Informação e Comunicação

A informação é reconhecida pelas organizações nos últimos anos como sendo o mais importante recurso estratégico que necessita ser gerenciado [WEILL&ROSS, 2004]. Os sistemas e os serviços de Tecnologia da Informação e Comunicação 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 TIC é crucial, estratégica e um importante recurso que precisa de investimento e gerenciamento apropriados.

Esse cenário motivou o surgimento do conceito de Governança Tecnológica, do termo inglês *IT Governance*, através da qual se procura o alinhamento de TIC com os objetivos da organização. Governança tecnológica define que TIC é um fator essencial para a gestão financeira e estratégica de uma organização e não apenas um suporte aos mesmos.

Governança de Tecnologia da Informação e Comunicação pode ser definida da seguinte forma:

- 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 TIC e seus processos [ITGI, 2001];
- Capacidade organizacional exercida pela mesa diretora, gerente executivo e o gerente de TIC de controlar o planejamento e implementação das estratégias de TIC e dessa forma, permitir a fusão de TIC ao negócio [Van Grembergen, 2003];
- Especificação das decisões corretas em um modelo que encoraje o comportamento desejável no uso de TIC nas organizações [WEILL&ROSS, 2004].

A governança envolve direcionamento de TIC e controle da Gestão, verificação do retorno do investimento e do controle dos riscos, análise do desempenho e das mudanças na TIC, e alinhamento com as demandas futuras da atividade fim - foco interno - e com a atividade fim de seus clientes - foco externo. Essa abrangência é ilustrada na Figura 5-1. A gestão preocupa-se com o planejamento, a organização, a implementação, a implantação e a manutenção da infraestrutura de TIC, e com o gerenciamento dos processos com foco no suporte e no fornecimento dos serviços [Van Grembergen, 2003].

Figura 5-1: Abrangência da Governança e da Gestão de TI [Van Grembergen, 2003].

Para alcançar a Governança da Tecnologia da Informação e Comunicação as organizações utilizam modelos que definem as “melhores práticas” para a gestão de TIC. Entre esses modelos, os de maiores aceitação são os dois seguintes: COBIT [ITGI, 2000] e ITIL [OGC, 2002].

5.3 Governança da Segurança da Informação

A proposta de um modelo para Governança da Segurança da Informação é apresentada neste trabalho para se tornar um subconjunto da Governança de TIC e, conseqüentemente, da Governança Organizacional. Esse modelo será responsável pelo alinhamento das questões de segurança computacional com o plano estratégico da organização.

Ao descrever o cenário atual para o gerenciamento de segurança computacional, muitas fontes da 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 Computacional 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 [IAA, 2001].

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 observar um cenário onde as questões de segurança computacional não são tratadas em um nível de gestão da organização, tendo como consequência a falta de recursos para minimizar os riscos existentes ao nível exigido pela estratégia organizacional. A responsabilidade pelo nível correto de segurança computacional 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 computacional 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 [BSA, 2003]. Esse trabalho sugere 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 com as pessoas, processos e tecnologia.

Para que as organizações obtenham sucesso na segurança de sua informação, os gestores precisam tornar a segurança computacional uma parte integrante da operação do negócio da organização [ENTRUST, 2004]. 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, segurança computacional deixaria de ser tratada apenas como uma questão técnica, passando a ser um desafio administrativo e estratégico.

Este trabalho propõe que um modelo de Governança da Segurança da Informação deva 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 computacional.

5.4 Requisitos para um Modelo de Governança de Segurança da Informação

Uma vez que as organizações possuem necessidades distintas, elas irão apresentar abordagens diversas para tratar as questões relacionadas com a segurança da informação. Dessa forma, um conjunto principal de requisitos deve ser definido para guiar os mais diversos esforços. Identificados esses requisitos, deve-se correlacioná-los em um Modelo de Governança da Segurança da Informação.

Na busca por um modelo de Governança da Segurança da Informação, nesse trabalho propõem-se os seguintes requisitos:

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;
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;
3. Organizações devem conduzir periodicamente uma avaliação de risco relacionada com a informação como parte do programa de gerenciamento de riscos;
4. Organizações precisam desenvolver e adotar políticas e procedimentos de segurança baseados na análise de risco para garantir a segurança da informação;
5. Organizações precisam estabelecer uma estrutura de gerenciamento da segurança para definir explicitamente o que se espera de cada indivíduo em termos de 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, conscientizando e educando os indivíduos;
9. Organizações precisam conduzir testes periódicos e avaliar a eficiência das políticas e procedimentos relacionados com 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 com a segurança computacional, como a ISO 17799 [ISO, 2000], para medir a performance da 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 nos três níveis, a saber: Operacional, Tático e Estratégico. A organização nesses níveis irá permitir a evolução de dados do nível operacional em informação do nível tático e posteriormente, em conhecimento do nível estratégico, que possa ser útil aos gestores no planejamento estratégico das organizações.

O modelo proposto neste trabalho será estruturado para prover 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 deverá ainda ser 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:

- O que se espera de cada indivíduo: o que deve e o que não deve ser feito;
- Como cada indivíduo poderá verificar se está cumprindo o que é esperado: indicadores de produtividade;
- Quais métricas devem ser utilizadas para medir a eficiência dos processos executados e para apontar ajustes que necessitem ser aplicados.

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

Uma revisão de literatura sobre práticas de gerenciamento de segurança computacional aponta pelo menos quatro pontos-chaves a serem considerados na definição de um modelo, a saber:

- Necessidade de uma avaliação de risco. Os riscos precisam ser conhecidos e as medidas de segurança correspondentes devem ser identificadas;
- Necessidade de uma estrutura organizacional de segurança computacional. Segurança computacional deve ser tratada em todos os níveis da organização;
- Necessidade de criar, endossar, implementar, comunicar e monitorar uma política de segurança por toda a organização, com comprometimento e apoio visível dos gestores;
- Necessidade de fazer com que cada indivíduo da organização conheça a importância da segurança computacional e treiná-los para que possam utilizar as melhores práticas neste sentido.

Embora esses quatro pontos-chaves sejam os mais comuns apontados pela literatura, os seguintes pontos são citados com frequência:

- Necessidade de monitorar, auditar e revisar as atividades de forma rotineira;
- Necessidade de estabelecer um plano de continuidade de negócio que possa ser testado regularmente.

Apesar da importância e da necessidade dos requisitos apresentados nesta seção, um dos pontos fortes do Modelo para Governança da Segurança da Informação proposto neste trabalho está relacionado com a forma como estes requisitos se correlacionam e em quais níveis de gerenciamento os mesmos devem ser incluídos.

5.5 Processos e Controles para um Modelo de Governança da Segurança da Informação

Para atender a todos os requisitos necessários a um modelo de Governança da Segurança da Informação, 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.

A Norma ISO 17799 e os modelos COBIT e ITIL são descritos com maiores detalhes a seguir.

5.5.1 Código de Prática para a Gestão da Segurança da Informação – ISO 17799

Para atender os anseios de grandes empresas, de agências governamentais e de instituições internacionais em relação ao estabelecimento de padrões e normas que refletisse as melhores práticas de mercado relacionadas com a segurança dos sistemas e informações, o *British Standards Institute* (BSI) criou uma das primeiras normas sobre o assunto. Denominada BS 7799 - *Code of Practice for Information Security Management*, ela foi oficialmente apresentada em primeiro de dezembro de 2000, após um trabalho intenso de consulta pública e internacionalização. A BS 7799 foi aceita como padrão internacional pelos países membros da *International Standards Organization* (ISO), sendo então denominada ISO/IEC 17799:2000 [ISO, 2000]. No ano 2001 a norma foi traduzida e adotada pela Associação Brasileira de Normas Técnicas (ABNT) como NBR 17799 - Código de Prática para a Gestão da Segurança da Informação [ABNT, 2001].

A norma ISO/IEC 17799, baseada na parte um da BS 7799, fornece recomendações para gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações. Tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre organizações [ISO, 2000].

A norma define 127 objetivos de controles que serão utilizadas neste trabalho para indicar o que deve ser abordado no Modelo de Governança da Segurança da Informação proposto, enfocando o processo sob o ponto de vista do negócio da empresa. A norma trata, dentre outros, dos seguintes aspectos: Política de Segurança, Plano de Continuidade do Negócio, Organização da Segurança, Segurança Física e Ambiental, Controle de Acesso e Legislação.

Essa norma considera a informação como um patrimônio que, como qualquer importante patrimônio da organização, tem um valor e consequentemente, precisa ser adequadamente

protegido. A conformidade dos processos corporativos com a norma ISO 17799 pode ser utilizada pelas empresas para demonstrar aos seus parceiros de negócio e clientes o seu comprometimento com as informações por ela manipuladas em relação aos seguintes conceitos básicos da segurança da informação:

- **Confidencialidade:** Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Integridade:** Salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- **disponibilidade:** Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Nesse contexto, a segurança da informação está relacionada com a proteção da informação contra uma grande variedade de ameaças, para permitir a continuidade do negócio, minimizar perdas, maximizar o retorno de investimentos e capitalizar oportunidades.

Para a seleção dos objetivos de controles apropriados para a organização, a norma recomenda que seja realizada uma Análise de Risco, que irá determinar a necessidade, a viabilidade e a melhor relação custo/benefício para a implantação desses controles.

5.5.2 Modelo COBIT

A missão maior relacionada com desenvolvimento do modelo COBIT (*Control Objectives for Information and Related Technology*) é pesquisar, desenvolver, publicar e promover um conjunto atualizado de padrões internacionais e de melhores práticas referentes ao uso corporativo de TIC para os gerentes e auditores de tecnologia [ITGI, 2000].

Desenvolvido e difundido pelo ISACA (*Information System Audit and Control*) e pelo *IT Governance Institute* (apenas a terceira edição do modelo), o COBIT é um modelo considerado por muitos como sendo a base da governança tecnológica. O COBIT funciona como uma entidade de padronização e estabelece métodos formalizados para guiar a área de tecnologia das empresas, incluindo qualidade, níveis de maturidade e segurança da informação.

O COBIT está estruturado em quatro domínios para que possa refletir um modelo para os processos de TIC. Esses domínios podem ser caracterizado pelos seus processos e pelas

atividades executadas em cada fase de implementação da Governança Tecnológica. Os domínios do COBIT são os seguintes:

- a) Planejamento e Organização:** Esse domínio possui 11 objetivos de controle que dizem respeito às questões estratégicas associadas a como a TIC pode contribuir da melhor forma possível para alcançar os objetivos da organização;
- b) Aquisição e Implementação:** Possui 6 objetivos de controle que definem as questões de identificação, desenvolvimento e aquisição da infra-estrutura de TIC conforme as diretrizes estratégicas e de projeto predefinidos no Plano Estratégico de Informática da empresa, também conhecido como PDI (Plano Diretor de Informática);
- c) Entrega e Suporte:** Esse domínio, com 13 objetivos de controle, define as questões ligadas ao uso da TIC para atendimento dos serviços oferecidos para os clientes, a manutenção e as garantias ligadas a estes serviços.
- d) Monitoração:** Com 4 objetivos de controle, esse domínio define as questões de auditoria e acompanhamento dos serviços de TIC, sob o ponto de vista de validação da eficiência dos processos e evolução dos mesmos em termos de desempenho e automação.

O modelo COBIT define objetivos de controle como sendo declarações de resultado desejado, ou propósito a ser atingido, pela implementação de procedimentos de controle numa atividade de TI em particular.

A Figura 5-2 ilustra os quatro domínios do COBIT, os objetivos de controle para cada domínio e seus inter-relacionamentos.

Além dos quatro domínios principais que guiam o bom uso da tecnologia da informação na organização, existe também a questão de auditoria, que permite verificar, através de relatórios de avaliação, o nível de maturidade dos processos da organização. O método de auditoria segue o modelo do CMMS (*Capability Maturity Model for Software*) [PAULK et al, 1993] e estabelece os seguintes níveis:

- 0) Inexistente:** Significa que nenhum processo de gerenciamento foi implementado;
- 1) Inicial:** O processo implementado é realizado sem organização, de modo não planejado;
- 2) Repetível:** O processo implementado é repetido de modo intuitivo, isto é, depende mais das pessoas do que de um método estabelecido;

- 3) **Definido:** O processo implementado é realizado, documentado e comunicado na organização;
- 4) **Gerenciado:** Existem métricas de desempenho das atividades, de modo que o processo implementado é monitorado e constantemente avaliado;
- 5) **Otimizado:** As melhores práticas de mercado e automação são utilizadas para a melhoria contínua dos processos envolvidos.

Figura 5-2- Os domínios de processo do COBIT [ITGI, 2000].

O resultado da auditoria da metodologia COBIT para a avaliação do nível de maturidade ajuda a área de TIC a identificar o nível atual e como evoluir para melhorar os processos da organização, permitindo a evolução gradativa desses.

O resultado da auditoria permite identificar o nível de evolução dos processos na organização, de modo concreto, com base em relatórios confiáveis de auditoria e parâmetros de mercado. O sumário executivo do relatório gerado pela auditoria traz as seguintes informações: se existe um método estabelecido para o processo; como o método é definido e estabelecido; quais os controles mínimos para a verificação do desempenho do método; como pode ser feita a auditoria no método; quais as ferramentas utilizadas no método e o que avaliar no método para sua melhoria. A partir desse ponto, a organização define os objetivos de controle a serem atingidos.

5.5.3 Modelo ITIL

O modelo ITIL (*Information Technology Infrastructure Library*) foi desenvolvido pelo governo britânico no final da década de 1980 e tem como foco principal a operação e a gestão da infra-estrutura de TIC na organização, incluindo todos os pontos importantes no fornecimento e manutenção dos serviços de TIC [OGC, 2000]. O ITIL, composto por um conjunto das melhores práticas para auxiliar a Governança de TIC, vem sendo um dos modelos mais amplamente utilizados atualmente [RUDD, 2004].

O princípio básico do ITIL é o objeto de seu gerenciamento: a infra-estrutura de TIC. O ITIL descreve os processos que são necessários para dar suporte à utilização e ao gerenciamento da infra-estrutura de TIC. Outro princípio fundamental do ITIL é o fornecimento de qualidade de serviço aos clientes de TIC a custos justificáveis, isto é, relacionar os custos dos serviços de tecnologia de forma que se possa perceber como estes trazem valor estratégico ao negócio. Através de processos padronizados de gerenciamento do ambiente de TIC é possível obter uma relação adequada entre custos e níveis de serviços prestados pela área de TIC.

O ITIL consiste em um conjunto de melhores práticas que são inter-relacionadas para minimizar o custo, ao mesmo tempo em que aumenta a qualidade dos serviços de TIC entregue aos usuários. Como destacado na Figura 5-3, o ITIL é organizado em 5 módulos principais, a saber: A Perspectiva de Negócios, Gerenciamento de Aplicações, Entrega de Serviços, Suporte a Serviços e Gerenciamento de Infra-estrutura. Embora o modelo ITIL não tenha um módulo dedicado ao Gerenciamento de Segurança Computacional, ele faz referência a esse tema

descrevendo em um documento como o mesmo poderia ser incorporado através dos processos descritos nos módulos de Suporte a Serviços e Entrega de Serviços.

Dentre os 5 módulos citados, os mais utilizados são o *Suporte a Serviços* e *Entrega de Serviços*.

Apesar de o modelo ITIL possuir processos bem definidos para auxiliar na Governança da Tecnologia da Informação e Comunicação, nesse trabalho identifica-se a necessidade de algumas adaptações para que ele possa ser utilizado para implementar todos os requisitos de um modelo de Governança de Segurança da Informação. Essas adaptações estão relacionadas principalmente com forma de como tratar incidentes de segurança computacional.

No capítulo 7 será apresentada a proposta deste trabalho para expansão do modelo ITIL.

Figura 5-3: Modelo para Gerenciamento de Serviços ITIL [OGC, 2000].

Considerando a estrutura de tomada de decisão em sistemas de informação, este trabalho propõe ainda um mapeamento dos módulos *Suporte a Serviços* e *Entrega de Serviços* do modelo ITIL no nível operacional e no nível tático, conforme descrito a seguir.

5.5.3.1 Suporte a Serviços: Processos do ITIL para o Nível Operacional

O módulo de Suporte a Serviços descreve 5 processos e a organização de um *Service Desk* que ajudam a manter a entrega de serviços ao se concentrarem nas atividades diárias e no suporte de serviços de TIC. Uma descrição sucinta de cada um deles é apresentada a seguir:

- **Service Desk** - Provê um ponto único de contato para todos os usuários de TIC dentro da organização, manipulando todos os incidentes, consultas e requisições. O *Service Desk* provê ainda a interface para todos os processos contidos no domínio de Suporte a Serviços.
- **Gerenciamento de Configuração** - É o processo de administração de informação sobre todos os itens de configuração (*CI-Configuration Item*), ou seja, hardware, software e documentação relacionada, em uma infra-estrutura de TI, bem como os relacionamentos entre esses itens de configuração. Todas essas informações sobre os CIs serão armazenadas em um Banco de Dados de Gerenciamento de Configuração (*CMDB-Configuration Managment Data Base*);
- **Gerenciamento de Incidentes** - Diz respeito à habilidade e rapidez em contornar incidentes relatados ao *Service Desk*, tais como erros, interrupções ou pedidos de serviços. Gerenciamento de Incidentes implica em registro e monitoramento de incidentes, verificação de *status* de recursos de sistemas, preenchimento de pedidos de serviço padrão e gerenciamento de conhecimento;
- **Gerenciamento de Problemas** – É o processo que procura descobrir a causa raiz dos incidentes reportados e, em seguida, determinar a mudança adequada à infra-estrutura de TI para evitar a sua recorrência. Ao contrário do Gerenciamento de Incidentes, o Gerenciamento de Problemas enfatiza as soluções a longo prazo, e não incidentes. A automação para Gerenciamento de Problemas inclui análise de dados históricos, registro e monitoramento de problema, diagnóstico de problema e identificação da causa raiz dos acidentes;
- **Gerenciamento de Mudanças** - É o processo de verificação e aprovação de pedidos de mudança, bem como de coordenação de mudanças aprovadas a serem implementadas. As

ferramentas utilizadas para dar suporte ao Gerenciamento de Mudanças incluem monitoramento de aprovação de mudanças e análise de impacto de mudanças;

- **Gerenciamento de Versões** - Diz respeito à construção, teste e implementação de uma versão, geralmente com diversas mudanças aprovadas.

O relacionamento entre os processos contidos no módulo de Suporte a Serviços é apresentado na figura 5-4.

Figura 5-4: ITIL – Processos a serem utilizados no Nível Operacional.

5.5.3.2 Entrega de Serviços: Processos do ITIL para o Nível Tático

O módulo de Entrega de Serviços descreve 5 processos que cuidam do gerenciamento da entrega de serviços de TIC para o usuário final, com ênfase em planejamento a longo prazo e melhoria contínua desses serviços. Uma descrição sucinta desses processos é apresentada a seguir:

- **Gerenciamento de Nível de Serviço** - Estabelece e mantém acordos de nível de serviços (SLA) e garante que esses níveis de serviços sejam mantidos;
- **Gerenciamento de Capacidade** - É o processo proativo que garante capacidade suficiente para a infra-estrutura de TIC de maneira rentável;
- **Gerenciamento de Disponibilidade** - Garante que os serviços de TIC estejam ativos e disponíveis. O que significa compreender os requisitos de cliente quanto

à disponibilidade, avaliando os recursos de infra-estrutura de TIC para apresentar esses níveis de disponibilidade e procurando melhorar a disponibilidade;

- **Gerenciamento de Continuidade** - Gerenciamento de Continuidade de Serviços de TIC é o processo de planejamento para recuperação de interrupções de serviços de TIC;
- **Gerenciamento Financeiro** - Gerenciamento Financeiro para Serviços de TIC é a administração financeira do fornecimento de ativos e serviços de TIC.

O relacionamento entre os processos contidos no módulo de Entrega de Serviços é apresentado na Figura 5-5.

Figura 5-5: ITIL – Processos a serem utilizados no Nível Tático.

5.6 Relação dos processos entre os modelos ITIL e COBIT e a norma ISO 17799

Para consubstanciar o uso integrado do modelo COBIT, do modelo ITIL e da norma ISO 17799 em um Modelo de Governança da Segurança da Informação, apresenta-se na tabela 5-1 uma correlação entre os objetivos de controle apresentados no modelo COBIT e os apresentados na norma ISO 17799. Ainda nessa tabela, são apresentados quais objetivos de controle são referenciados pelos processos descritos no modelo ITIL, em especial pelos módulos de *Suporte a Serviços* e *Entrega de Serviços*.

A Tabela 5-1 apresenta também a proposta deste trabalho para estruturação dos objetivos de controle em níveis organizacional, tático e estratégico.

Tabela 5-1: Relacionamento de Processos entre os modelos ITIL e COBIT e a norma ISO 17799.

	Objetivos de Controle do COBIT	Objetivos de Controle ISO 17799	Referência 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		
	M – Monitoramento		
	M1-Monitorar os Processos	X	
	M2-Avaliar a Adequação do Controle Interno	X	
	M3-Obter certificação Independente		
	M4-Providenciar Auditoria Independente		
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

Comparado ao modelo COBIT, o modelo ITIL descreve de forma detalhada os processos relativos ao suporte e entrega de serviços (domínio DS na Tabela 5-1), mas não cobre todos os requisitos de controle relacionados com o gerenciamento de TIC descritos pelo COBIT para esse 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 TIC. Seus processos estão estruturados e detalhados para indicar *como implementar e quem faz o quê, ou seja, delimitar papéis e responsabilidades*.

Após uma avaliação de cada objetivo de controle descrito no modelo COBIT, propõe-se uma categorização nos níveis operacional, tático e estratégico, conforme ilustrado na Tabela 5-1.

5.7 Identificação de Requisitos de Segurança a Partir de uma Análise de Risco

Um modelo de Governança de Segurança da Informação deverá prover mecanismos para a identificação dos requisitos de segurança adequados a uma organização. A ISO/IEC 17799:2000 [ISO, 2000] aponta três fontes principais para essa identificação:

- Através da análise de risco dos ativos da organização são identificadas as ameaças aos ativos, as vulnerabilidades e suas respectivas probabilidades de ocorrência são avaliadas, bem como o impacto potencial é estimado;
- A legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender;
- O conjunto particular de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

Os requisitos de segurança são identificados através de uma avaliação sistemática dos riscos de segurança. Os gastos com os requisitos de controles necessitam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança. As técnicas de avaliação de risco podem ser aplicadas em toda a organização ou apenas em parte

dela, assim como em um sistema de informação individual, componentes de um sistema específico ou serviços, quando for viável, prático e útil.

A avaliação de risco é uma consideração sistemática a respeito de seguinte:

- Do impacto nos negócios como resultado de uma falha de segurança, levando-se em conta as potenciais consequências da perda de confidencialidade, integridade ou disponibilidade da informação ou de outros ativos;
- Da probabilidade de tal falha realmente ocorrer à luz das ameaças e vulnerabilidades mais frequentes e nos controles atualmente implementados.

Os resultados da avaliação de risco ajudarão a direcionar e determinar ações gerenciais e prioridades mais adequadas para um gerenciamento dos riscos da segurança da informação e a selecionar os objetivos de controles a serem implementados para a proteção contra esses riscos.

É necessário realizar análises críticas periódicas dos riscos de segurança e dos controles implementados para o seguinte fim:

- Considerar as mudanças nos requisitos de negócio e suas prioridades;
- Considerar novas ameaças e vulnerabilidades;
- Confirmar que os controles permanecem eficientes e adequados.

Convém que as análises críticas sejam executadas em diferentes níveis de profundidade, dependendo dos resultados das avaliações de risco feitas anteriormente e das mudanças nos níveis de riscos que a direção considera aceitável para os negócios. As avaliações de risco são sempre realizadas em nível amplo primeiramente, como uma forma de priorizar recursos em áreas de alto risco, e então em um nível mais detalhado, para solucionar riscos específicos.

Para a identificação dos requisitos de segurança de uma organização, neste trabalho propõe-se a utilização das avaliações e diagnósticos apresentados pelo modelo COBIT.

5.8 Considerações finais

Neste capítulo apresenta-se a necessidade de um modelo para Governança da Segurança da Informação e os requisitos necessários para o mesmo. Para atender todos os requisitos

necessários a um modelo de Governança da Segurança da Informação, neste trabalho propõe-se a utilização integrada dos modelos COBIT e ITIL e da norma ISO 17799.

O modelo COBIT e a norma ISO 17799 irão fornecer os objetivos de controle necessários para atender aos requisitos apresentados. Os processos descritos no modelo ITIL serão utilizados para guiar a implementação desses objetivos de controle.

Através de uma correlação dos objetivos de controle presentes no modelo COBIT e na norma ISO 17799 com os processos descritos no modelo ITIL, neste trabalho identificou-se que os módulos de *Suporte a Serviços* e *Entrega de Serviços* do modelo ITIL não estão estruturados para implementar todos os objetivos de controle apresentados para o nível Operacional e Tático.

Para que o modelo ITIL seja capaz de implementar todos os objetivos de controle apresentados pela norma ISO 17799 e pelo modelo COBIT para os níveis operacional e tático, este trabalho irá propor no capítulo 6 uma expansão de seus processos.

6 Extensão do Modelo ITIL com a Estratégia de CSIRTs

6.1 Considerações Iniciais

Conforme apresentado no capítulo anterior, uma expansão do modelo ITIL e o seu mapeamento nos níveis operacional e tático são propostos neste trabalho para se obter parte de um modelo de Governança para Segurança da Informação apoiado nos conceitos de Sistemas de Informação e Governança de TIC.

Neste capítulo apresenta-se a proposta a partir da adaptação dos processos ITIL de ‘Gerenciamento de Incidentes’, ‘Gerenciamento de Problemas’ e ‘Gerenciamento de Mudanças’ para que esses processos permitam a reação aos incidentes de segurança computacional no nível operacional. Neste trabalho propõe-se também a inserção de um processo novo chamado de ‘Gerenciamento de Comportamento’, no nível tático.

Apesar de o modelo ITIL ter a capacidade de tratar incidentes de forma reativa (Gerenciamento de Incidentes) e de forma proativa (Gerenciamento de Problemas e Gerenciamento de Mudanças), ambos no nível operacional, torna-se necessário essa expansão tendo em vista as particularidades de um incidente de segurança computacional e a necessidade de implementar os objetivos de controle previstos no modelo COBIT e na norma ISO 17799.

As adaptações propostas neste trabalho para o Modelo ITIL serão fundamentadas com base em trabalhos que apresentam a experiência de centros especializados em pesquisas relacionadas com o Gerenciamento de Atividades de Resposta a Incidentes, principalmente aqueles que podem ser classificados como CSIRTs – *Computer Security Incident Response Teams* [WEST-BROWN et al, 1998].

6.2 Gerenciamento de Incidentes de Segurança Computacional

Como ponto de partida para a expansão do processo de gerenciamento de incidentes do modelo ITIL, primeiramente torna-se necessário definir *gerenciamento de incidentes*.

A literatura apresenta diversas definições para gerenciamento de incidentes, de forma que é difícil obter uma definição precisa. Esse termo tem significados diferentes para comunidades diferentes. Parte da dificuldade de uma definição única para ‘gerenciamento de incidentes’ está

relacionado com o entendimento para o termo incidente, o qual é frequentemente definido com base nas especificações e necessidades de cada organização.

A RFC 2350 define que um incidente de segurança computacional é “um evento adverso que compromete algum aspecto da segurança do computador ou da rede” [BROWNLEE, 1998]. Uma definição de ‘evento’ pode ser obtido a partir da RFC 2828: “uma ocorrência em um sistema que é relevante para a segurança desse sistema... O termo inclui eventos que são incidentes de segurança e aqueles que não são” [SHIREY, 2000]. O termo evento ainda é utilizado para descrever uma atividade que é relacionada com a segurança computacional, mas que ainda não foi identificada como um incidente ou uma vulnerabilidade [ALBERTS, 2004]. Como exemplo para essa última definição, pode-se considerar um aumento de tráfego não perceptível aos usuários em uma rede e que é decorrente do primeiro ataque de um *worm* recém desenvolvido e que ainda é desconhecido. Neste exemplo, observa-se um evento que ainda não foi registrado ou reconhecido como um incidente de segurança computacional.

Um incidente também pode ser definido como um evento adverso, real ou suspeito, relacionado com a segurança de sistemas ou redes e também com o ato de violar uma política de segurança implícita ou explícita [ALLEN, 2004]. Exemplos para esta definição incluem o seguinte: uma tentativa ou o sucesso em ganhar acesso não autorizado a um sistema ou a seus dados; ações que causam a falha de um serviço (*denial of service*); o uso não autorizado de um sistema para processamento ou armazenamento de dados; mudanças no sistema sem o consentimento do proprietário; a ocorrência de um vírus de computador; busca de vulnerabilidades em sistemas computacionais através de uma rede (*probes* ou *scans*).

Para Alberts (2004), o gerenciamento de incidentes diz respeito à prevenção e tratamento dos incidentes de segurança computacional. Essa definição inclui identificar e minimizar o impacto de vulnerabilidades técnicas em software ou hardware que podem expor a infraestrutura computacional a ataques ou comprometimentos e, dessa forma, causar incidentes. Nesse caso é possível dizer que o gerenciamento de incidentes de segurança computacional exige um conjunto de ações proativas.

Segundo o modelo ITIL, um incidente é qualquer evento que não faz parte da operação padrão de um serviço e que causa, ou pode causar, uma interrupção do serviço ou uma redução da sua qualidade [OGC, 2000]. Assim, o gerenciamento de incidentes diz respeito à habilidade e

rapidez em contornar incidentes – tais como erros, interrupções ou pedidos de serviços – relatados ao *Service Desk*. No modelo ITIL, o Gerenciamento de Incidentes tem como principal objetivo restaurar o serviço o mais rápido possível para o usuário, minimizando impactos na operação do negócio dentro dos níveis de serviço acordados (*SLA-Service Level Agreement*) [OGC, 2000].

A meta do gerenciamento de incidentes do modelo ITIL é restaurar a operação normal do serviço o mais rapidamente possível e minimizar o impacto adverso para o negócio, assegurando dessa forma que os melhores níveis possíveis de qualidade e disponibilidade sejam mantidos. ‘Operação normal do serviço’ é definido como a operação do serviço dentro do Acordo de Nível de Serviço (*Service Level Agreement –SLA*) [OGC, 2000]. Dessa forma, observa-se que o processo de Gerenciamento de Incidentes no modelo ITIL comporta-se de forma reativa, sendo que não é previsto o tratamento de ameaças ou vulnerabilidades que podem levar a um incidente. Apesar de o modelo ITIL prever atividades proativas no processo de Gerenciamento de Problemas, esta proatividade só ocorre após a correlação de causas não conhecidas para incidentes de mesma natureza ou a consumação de um incidente de grande impacto.

Com base nas definições apresentadas, verifica-se que o incidente de segurança computacional apresenta características particulares quando comparado ao conceito de incidentes descrito no modelo ITIL, necessitando ser tratado de uma forma diferenciada. Com isso, torna-se necessário uma expansão no modelo ITIL para permitir um tratamento dos incidentes de segurança computacional de acordo com os requisitos de um modelo de Governança da Segurança da Informação.

Como uma forma de tratar incidentes de segurança computacional de forma rápida e efetiva, muitas organizações incluem em sua estratégia a criação de um *Computer Security Incident Response Team-CSIRT* (Grupos de Resposta a Incidentes de Segurança Computacional) [WEST-BROWN et al, 1998] [MANDIA, 2001] [SHULTS & SHUMWAY, 2002].

6.3 Computer Security Incident Response Team - CSIRT

Um *CSIRT*, ou Grupo de Resposta a Incidentes de Segurança Computacional, é uma organização ou grupo responsável por receber, analisar e responder as notificações e atividades

relacionadas com incidentes de segurança computacional, entre tantas outras atividades possíveis.

Normalmente, um CSIRT presta serviços para uma comunidade bem definida, que pode ser a entidade que o mantém, como uma empresa, um órgão governamental ou uma organização acadêmica. Um CSIRT também pode prestar serviços para uma comunidade maior, como um país, uma rede de pesquisa ou clientes que pagam por seus serviços.

A Tabela 6.1 apresenta os objetivos de alguns tipos de CSIRTs baseados nos diferentes tipos de grupos com diferentes missões. Essa tabela não considera todos os tipos possíveis para CSIRTs.

O CSIRT pode ser um grupo formal ou um grupo "*ad hoc*". Um grupo formal tem no trabalho de resposta a incidentes a sua principal função. Um grupo "*ad hoc*" é reunido quando há um incidente de segurança em andamento ou quando é necessário responder a um incidente.

No momento de se criar um CSIRT, deve-se ter muito bem definido quais atividades o mesmo irá exercer. O CSIRT poderá oferecer uma série de atividades proativas e reativas em relação ao conceito de segurança computacional. Entretanto, a atividade de Resposta a Incidente torna-se indispensável para que um grupo possa ser chamado de CSIRT.

Em ambientes onde é freqüente a ocorrência de incidentes de segurança, torna-se vital a existência de um ponto de contato único e de procedimentos eficientes e eficazes de resposta a incidentes. Este ponto de contato único pode receber diversos nomes, sendo o *Computer Security Incident Response Team - CSIRT* o mais comumente empregado [WEST-BROWN, 2002][MANDIA, 2001] [SCHULTZ, 2002]. Em função do tamanho desse ambiente, as atividades podem ser exercidas por uma pessoa ou por um grupo.

Uma vez estabelecidos, muitos CSIRTs tem falhado atualmente por não terem claramente definidas suas atividades, os procedimentos para executar as mesmas e ainda, pela falta de comunicação e inter-relacionamento entre essas atividades [ALBERTS et al, 2004]. Outro ponto falho observado tem relação com a organização da grande quantidade de dados gerados pelos incidentes. Esses dados, quando bem trabalhados, fornecem informações essenciais para que se consiga incrementar o grau de segurança do ambiente a ser protegido.

Tabela 6-1: Variedade de Objetivos possíveis para o Serviço de Gerenciamento de Incidentes de Segurança Computacional com base alguns tipos de CSIRTs (Adaptado de [WEST-BROWN-2002]).

Tipo de CSIRT	Natureza ou Missão	Objetivos possíveis para o Serviço
Centros de Coordenação Internacional (ex.: CERT/CC, FIRST e AusCERT)	Obter uma base de informações com perspectiva global das ameaças de segurança computacional através da coordenação de outros CSIRTs	<ul style="list-style-type: none"> • Provê suporte técnico em resposta a incidentes de segurança computacional através da coordenação de diversos outros CSIRTs espalhados pelo mundo; • Através das atividades de manipulação de incidentes, identificar e documentar detalhes técnicos das potenciais ameaças de intrusão na atualidade; • Criar e publicar informações sobre detecção, prevenção e recuperação contra ameaças de intrusão.
Times Nacionais (ex. NBSO Brasil)	Manter um ponto de contato nacional para ameaças de segurança e reduzir o número de invasões realizadas contra ou proveniente de um sistema no país.	<ul style="list-style-type: none"> • Provê suporte técnico em resposta a incidentes de segurança computacional na língua nacional e no horário nacional; • Provê informações para detectar, prevenir e recuperar vulnerabilidades; • Agir em parceria com os órgãos jurídicos nacionais.
Network Service Provider Team (CSIRT implementado através deste trabalho no Centro de Computação Eletrônica da USP)	Provê um ambiente seguro para a conectividade de seus clientes. Provê uma resposta eficiente para seus clientes para incidentes de segurança computacional.	<ul style="list-style-type: none"> • Provê suporte técnico em resposta a incidentes de segurança computacional; • Provê informações técnicas para detectar, prevenir e recuperar vulnerabilidades; • Agir em parceria com os órgãos Jurídicos nacionais; • Agir em parceria com o CSIRT Nacional; • Servir como ponto de contato para assuntos relacionados aos incidentes de segurança envolvendo seus clientes; • Avaliar a política de segurança proposta para a organização; • Notificar seus clientes e aplicar sanções quando necessárias.
Empresas Fornecedoras de TI (Ex. CSIRT Microsoft)	Melhorar a segurança de seus produtos	<ul style="list-style-type: none"> • Prover suporte técnico em resposta às vulnerabilidades. Cooperar com CSIRTs para analisar a fonte básica do incidente; • Criar e divulgar alertas sobre novos <i>patches</i> e boas práticas a serem seguidas;
Time corporativo (ex. CSIRT proposto para o Centro de Computação Eletrônica da USP prestando serviço para o próprio Centro)	Melhorar a infra-estrutura da segurança da informação da organização e minimizar as ameaças de estrago resultantes de ataques e intrusões	<ul style="list-style-type: none"> • Provê um centro de excelência para suporte à manipulação de incidentes para administradores e usuários de sistemas e redes na organização; • Provê um suporte técnico local para incidentes contra os sistemas e a rede, ajudando a isolar e recuperar serviços diante de ameaças de intrusão e ataques;

Para auxiliar os CSIRTs na tarefa de organização dos dados gerados pelos diversos incidentes de segurança computacional, foi desenvolvido uma ferramenta denominado *SiRI-Sistema para Resposta a Incidentes* [BERNARDES et al., 2003]. Essa ferramenta, apresentada no Apêndice A deste trabalho, auxilia as organizações a reduzir os efeitos dos incidentes de segurança, fornecendo subsídios para reduzir o tempo de sua detecção e relato e organizar os dados para fornecer informações importantes para a prevenção de incidentes. Atualmente, ela está sendo utilizada no Centro de Computação Eletrônica da Universidade de São Paulo, ambiente onde será validado o resultado deste trabalho.

6.4 Gerenciamento de Incidentes

Antes de propor neste trabalho a expansão do modelo ITIL com as funcionalidades de um CSIRT, torna-se necessário uma revisão de literatura sobre as várias publicações relacionadas ao gerenciamento de incidentes de segurança computacional. Nos últimos anos, vários livros e artigos foram escritos sobre gerenciamento de incidentes de segurança computacional e atividades de resposta ao incidentes de segurança computacional [ALBERTS et al, 2004].

Na literatura é comum encontrar o termo ‘resposta a incidentes’ sendo empregado como o processo de gerenciamento de incidentes de segurança computacional. O termo ‘resposta a incidentes’ é comumente empregado nos trabalhos que descrevem atividades de um CSIRT, enquanto que o termo ‘Gerenciamento de Incidentes’ é observado em trabalhos que descrevem modelos para ‘Governança de TI’. Em seu trabalho, Killcrece et al. (2003) detalha o conjunto de atividades básicas ou tarefas descritas por diversos autores que apresentaram metodologias para o gerenciamento de incidentes [KILLCRECE et al, 2003]. Alguns dados desta revisão de literatura são apresentados na Tabela 6.2. Estes dados irão fornecer a base necessária para as adaptações propostas neste trabalho para que o modelo ITIL possa ser utilizado para implementar os objetivos de controle necessários a um modelo de Governança de Segurança Computacional.

Tabela 6-2: Revisão do Processo de Gerenciamento de Incidentes de Segurança Computacional com base em diversos autores [ALBERTS, 2004].

Título da Publicação	Autor(es)	Processos ou atividades
<i>Computer Forensics, Incident Response Essentials</i>	Warren G. Kruse II and Jay G. Heiser [KRUSE, 2002]	Descoberta e Notificação Confirmação do Incidente Investigação Recuperação Aprendizado/Recomendação
<i>Incident Response</i>	Kenneth R. van Wyk and Richard Forno [van WYK, 2001]	Identificação Coordenação Reação Investigação Educação
<i>Incident Response: A Strategic Guide to Handling System and Network Security Breaches</i>	Eugene Shultz and Russel Shumway [SHULTZ, 2002]	Preparação Detecção Contenção Erradicação Recuperação Continuação
<i>Incident Response: Investigating Computer Crime</i>	Kevin Mandia and Chris Prosise [MANDIA, 2001]	Preparação Pré-Incidente Detecção Resposta Inicial Formulação de uma estratégia de Resposta Duplicação (backup para <i>forensis</i>) Investigação Implementação de medidas de Segurança Monitoração da Rede Recuperação Anúncio Continuidade
<i>Advance Planning for Incident Response</i>	Symantec Corp. [SYMANTEC, 2001]	Identificar equipamentos vitais Contratar equipe experiente Proteger <i>hosts</i> individuais Proteger a rede Monitorar dispositivos Estabelecer uma estratégia de resposta Estabelecer políticas e procedimentos
<i>Computer Security Incident Handling Step by Step</i>	The SANS Institute [SANS, 2003]	Preparação Identificação Contenção Erradicação Recuperação Continuidade

Tabela 6.2: Revisão do Processo de Gerenciamento de Incidentes de Segurança Computacional com base em diversos autores [ALBERTS, 2004]. [continuação...]

Título da Publicação	Autor(es)	Processos ou atividades
<i>Security Architecture and Incident Management for E-business</i>	Internet Security Systems - Marc Sokol and David A. Curry [SOKOL, 2000]	Estar preparado para o Incidente Alertar Anunciar e notificar Investigação Preliminar Decisão e Alocação de Recursos Resposta Recuperação Aprendizado
<i>Computer Security Incident Response Planning</i>	Internet Security Systems [ISS, 2001]	Alerta Triagem Resposta Recuperação Manter
<i>Responding to Computer Security Incidents: Guidelines for Incident Handling</i>	E. Eugene Schultz, Jr., David S. Brown, Thomas A. Longstaff [SCHULTZ, 1990]	Proteção Identificação Conter Erradicação Recuperação Continuidade
<i>State of Vermont Incident Handling Procedure</i>	State of Vermont [VERMONT, 2001]	Proteger Identificar Conter Erradicar Recuperar Continuidade
<i>RFC 2196 Site Security Handbook</i>	Barbara Fraser, Editor [FRASER, 1997]	Notificação e troca de informação Proteção de evidências e atividades de log Conterção Erradicação Recuperação Continuidade
<i>Computer Incident Response Guidebook</i>	Naval Command, Control and Ocean Surveillance Center [NAVY, 1996]	Preparação Identificação Conterção Erradicação Recuperação Continuidade

Para ser considerado um CSIRT, é necessário que seja previsto o gerenciamento de incidentes onde se tenha a análise do incidente e pelo menos uma atividade dentre as seguintes: a resposta a incidentes locais, suporte a resposta a incidentes ou coordenação da resposta a incidentes. [WEST-BROWN, 2002].

6.5 Categorização dos Serviços em um CSIRT

Com base na Tabela 6.2, verifica-se que um CSIRT pode ser estruturado para oferecer uma série de serviços, que podem ser agrupados em três categorias:

- **Serviços Proativos** - Serviços que provêem assistência ou informação que ajudam a preparar e proteger sistemas, antecipando-se a ataques, problemas ou eventos. Executando essas atividades, este serviço irá reduzir a possibilidade da ocorrência de incidentes no futuro;
- **Serviços Reativos** - Serviços que são disparados por um evento ou uma requisição, como o relato de um *host* comprometido, a distribuição mundial de um código malicioso, vulnerabilidade de um software, algo que foi identificado por um sistema de detecção de intrusão ou um sistema de análise de log. Serviços Reativos constituem o componente principal do trabalho de um CSIRT;
- **Serviço de gerenciamento da qualidade de segurança** - Este serviço incrementa procedimentos existentes e bem estabelecidos e que são independentes do gerenciamento de incidentes e tradicionalmente são executados por outras áreas dentro da organização, como a auditoria. Se o CSIRT executar ou auxiliar esse serviço, o ponto de vista do CSIRT e a experiência poderão prover idéias para ajudar a melhorar a segurança global da organização e identificar riscos, ameaças, e fraquezas no sistema. Estes serviços são geralmente proativos e podem contribuir indiretamente para a redução do número de incidentes.

É importante observar que alguns serviços possuem ao mesmo tempo atividades reativas e atividades proativas. Por exemplo, o tratamento de vulnerabilidades pode ser feito em resposta à descoberta de uma vulnerabilidade em um software que está sendo explorada em um determinado momento. Mas também pode ser proativo ao revisar e testar o código para determinar se existem vulnerabilidades, sendo que o problema poderá ser resolvido antes que seja amplamente conhecido ou explorado.

Tabela 6-3: Correlação das atividades de gerenciamento de segurança computacional previstas no modelo ITIL e pelos CSIRTs.

Nível Operacional			Nível Tático			Nível Estratégico		
Serviços Reativos			Serviços Proativos			Serviços de Gerenciamento da qualidade da Segurança		
	CSIRT	ITIL		CSIRT	ITIL		CSIRT	ITIL
Alertas e Warnings	X		Anúncios	X		Análise de Risco	X	
Tratamento ao Incidente	X	X	Assistência Tecnológica	X	X	Consultoria em Segurança	X	
Registro e Alerta	X	X	Continuidade do Negócio e Plano de Recuperação de desastre	X	X	Construir um Mapa de Desinformação	X	
Suporte Inicial e Classificação	X	X	Configuração & Manutenção de Ferramentas de Segurança e Infra-estrutura	X		Educação/Treinamento	X	
Análise do Incidente (Investigação e Diagnóstico)	X	X	Desenvolvimento de ferramentas de segurança	X		Avaliação e Certificação de Produto	X	
Resposta local ao Incidente	X	X	Serviço de Detecção de Intrusão	X		Código de Conduta	X	
Suporte à resposta ao Incidente	X	X	Disseminação da informação relacionada à segurança	X	X	Gerenciamento de Segurança	X	
Coordenação da resposta ao incidente	X	X				Auditoria de Segurança	X	
Tratamento da Vulnerabilidade	X	X						
Análise da Vulnerabilidade	X							
Resposta à Vulnerabilidade	X	X						
Coordenação da resposta à vulnerabilidade	X	X						
Tratamento de artefatos	X							
Análise de artefatos	X							
Resposta ao Artefato	X	X						
Coordenação da resposta ao Artefato	X	X						
Identificação de equipamentos relacionados ao incidente		X						
Correlação de Incidentes de mesma natureza		X						
Base de Dados de Erros conhecidos		X						
Gerenciamento das Mudanças		X						

Outra observação importante diz respeito à proatividade no gerenciamento de incidentes, eliminando a possibilidade que eles aconteçam. Por exemplo, a disseminação de alertas para correção de vulnerabilidades antes que estas possam ser exploradas. Caso não haja nenhum incidente de segurança computacional identificado, as correções poderão ser feitas antes que os mesmos ocorram. Mesmo que não haja nenhum incidente registrado relacionado com uma

vulnerabilidade recém descoberta, a divulgação dos alertas irá reduzir o tempo de correção da vulnerabilidade e a possibilidade de correção ou eliminação da mesma antes que haja incidentes.

Com base nas observações apresentadas anteriormente, conclui-se que o Gerenciamento de Incidentes de Segurança Computacional exige um trabalho significativo antes que ocorra um incidente, independentemente se houve ou não a ocorrência de algum incidente de mesma natureza. A característica de proatividade no gerenciamento de incidentes de segurança computacional vai além da correlação de incidentes de mesma natureza, conforme previsto no processo de gerenciamento de problemas no modelo ITIL.

Para que seja possível identificar quais as atividades de um CSIRT que devem ser incorporadas aos processos descritos no modelo ITIL, neste trabalho propõe-se a Tabela 6.3. Nessa tabela é possível correlacionar as atividades previstas para o gerenciamento de segurança computacional no modelo ITIL e nos modelos comuns aos CSIRTs. A tabela propõe ainda uma classificação dessas atividades em nível operacional, nível tático e nível estratégico.

6.6 Gerenciamento de Incidentes

As atividades da gerência de Incidentes em um CSIRT podem ser organizadas em quatro funções principais: “Triagem”, “Análise do Incidente”, “Retorno ao reclamante (Feedback)” e “Divulgação dos resultados” [WEST-BROWN, 2002].

Essas quatro funções são totalmente inter-relacionadas, podendo ser representadas conforme a Figura 6-1.

Figura 6-1: As principais funções do serviço de Resposta a Incidentes e suas relações [WEST-BROWN, 2002]

O modelo ITIL trata um incidente de segurança computacional da mesma forma que os demais tipos de incidentes, sendo que atividades proativas são realizadas apenas no nível de gerenciamento de Problemas. A Figura 6-2 apresenta o relacionamento do processo de gerenciamento de Incidentes do modelo ITIL com a infra-estrutura de TIC e demais processos do modelo.

Figura 6-2: Processo de Gerenciamento de Incidentes no modelo ITIL [OGC, 2000]

Apesar dos modelos previstos para CSIRTs descritos em West-Brown(2002) apresentarem uma estrutura muito similar ao processo de Gerenciamento de Incidentes do modelo ITIL, os CSIRTs apresentam características específicas para o tratamento de incidentes de segurança computacional.

6.6.1 Função de Triagem em um CSIRT

A função de triagem fornece um ponto único de contato e é o local responsável por receber, coletar, ordenar, identificar os pontos envolvidos com o incidente, encaminhar o incidente para os pontos responsáveis ou para um grupo de especialistas, receber as respostas e divulgá-las. Esta função requer diversos canais de comunicação, tais como: e-mail, telefone, fax etc. Outra importante atividade desta função é priorizar o incidente e associar um identificador a cada incidente, de forma a estabelecer uma referência para o mesmo ao longo do tempo e através das demais funções do serviço de resposta a incidentes. Como parte do serviço de triagem, ações

adicionais podem ser realizadas para facilitar a atividade seguinte. Por exemplo, fazer a conversão de horas (*time zone*), conversão de mídia, organização dos *logs* e correlação com alertas registrados.

6.6.2 Função de Análise do Incidente em um CSIRT

Essa função fornece apoio aos pontos relacionados com o incidente. Essas atividades vão desde a divulgação de conhecimento adquirido com casos semelhantes ocorridos no CSIRT até o compartilhamento de informações recebidas de outras fontes e contatos com centros especializados.

6.6.3 Função de Divulgação dos Resultados em um CSIRT

Essa função é responsável por tratar e divulgar os dados relativos ao incidente. Entre suas atribuições está o acompanhamento do ciclo de vida de cada incidente, cuidar para que o mesmo tenha um encerramento e que informações correspondentes sejam encaminhadas ao reclamante.

Os dados recebidos nessa função, quando bem trabalhados, irão gerar informações vitais para a redefinição dos requisitos de controle da política de segurança em vigor na organização e, conseqüentemente, contribuir para a redução do número de incidentes.

6.6.4 Função de *Feedback* em um CSIRT

A função de *feedback* fornece suporte para uma resposta a elementos que não estão diretamente relacionados com um incidente. Esta é uma função extremamente importante no momento de lidar com contatos externos e a mídia e ainda, para fornecer um mecanismo de segurança frente a exploração das técnicas de engenharia social.

6.7 O Ciclo de Vida de um Incidente

O ciclo de vida do gerenciamento de incidentes de segurança computacional no modelo ITIL difere do modelo para CSIRTs.

Sob o ponto de vista dos CSIRTs, a resposta a incidentes é apenas uma parte do gerenciamento de Incidentes. Tão importante quanto uma resposta eficiente e eficaz para o incidente são as ações para preveni-lo. Comparando-se a uma brigada de incêndio, o CSIRT despende um grande esforço no sentido de treinar, simular situações, informar, promover

palestras, fazer auditorias e influenciar no ajuste da política de segurança da organização. A Figura 6-3 apresenta o ciclo de vida da gerencia de um incidente em um modelo para CSIRTs, compreendendo as etapas de: análise, coleta de informações do reclamante, provimento de assistência técnica e tratamento da informação para posterior resolução e resposta.

Figura 6-3. Ciclo de vida da Gerencia de um Incidente apresentado pelo CERT/CC [WEST-BROWN, 2003]

O ciclo de vida da Gerência de Incidentes no modelo ITIL apresenta atividades reativas, ou seja, a resposta ao incidente inicia-se quando ele é relatado pelo usuário ou quando se percebe um evento que não é parte da operação normal de um serviço. A Figura 6-4 apresenta as etapas previstas pelo modelo ITIL para o ciclo de vida do processo de gerenciamento de incidentes.

Figura 6-4: Ciclo de vida da Gerência de Incidentes apresentado pelo modelo ITIL [OGC,2000]

6.8 Proposta de Expansão do Modelo ITIL

Para que o modelo ITIL seja utilizado na composição de um modelo para Governança da Segurança da Informação, neste trabalho propõe-se uma expansão de seus processos nos módulos de *Suporte a Serviços* e *Entrega de Serviços*. Essa expansão terá como base a incorporação das principais atividades prevista para CSIRTs.

Com essa proposta pretende-se tornar o modelo ITIL capaz de tratar as particularidades de incidentes de segurança computacional e permitir mais ações proativas condizentes com necessidades atuais da infra-estrutura de TIC.

Neste trabalho propõe-se ainda mapear os processos do modelo ITIL em um nível operacional (*Suporte a Serviços*) e em um nível tático (*Entrega de Serviços*). Este mapeamento facilitará a identificação de quais processos do modelo ITIL serão responsáveis pela implementação dos objetivos de controle previstos no modelo COBIT e na norma ISO 17799.

Figura 6-5: Proposta de mapeamento do modelo ITIL original e nível Operacional (*Suporte a Serviços*) e nível Tático (*Entrega de Serviços*)

6.8.1 Proposta para a Gerência de Incidentes

As funções previstas para o processo de gerência de incidentes do modelo ITIL serão expandidas para incluir a capacidade de considerar eventos que ainda não podem ser classificados como incidentes. Assim, eventos como um alerta de vulnerabilidade publicado em um *site* ou recebido por e-mail pela organização deverá ser analisado como um incidente, sendo que toda informação relacionada deve ser registrada.

O *Service Desk* deverá estar preparado para receber alertas de segurança computacional e registrá-los. Para que possa receber o maior número possível de alertas, o *Service Desk* deverá estar em contato com os principais centros de divulgação de alertas e CSIRTs. Isso poderá ser feito através da participação de listas de discussão específicas, cadastro em malas diretas para disseminação de alertas etc.

Uma vez registrados, os eventos devem ser classificados pelos especialistas para que possam ser publicados e divulgados para a comunidade e informados pelo *Service Desk* ao usuário a cada chamada recebida. Com isso, o *Service Desk* estará estruturado para disseminar informações sobre segurança computacional, tais como alertas, vulnerabilidades e aplicações de novos *patches*, comportando-se proativamente no sentido de minimizar o impacto de incidentes relacionados com a segurança computacional.

Durante o processo de triagem do evento, a gerência de incidentes deverá fazer uma pesquisa da Base de Dados de Configuração (CMDB) para identificação de Itens de Configuração (*CI-Configuration Item*) que possam ser afetados pela vulnerabilidade. Caso seja encontrado algum item de configuração que possua as características descritas nos sistemas afetados pela vulnerabilidade, o incidente deverá ser priorizado e encaminhado ao mesmo tempo para a gerência de Problemas e para a Gerência de Mudanças. A priorização do incidente (alerta) deverá considerar o número de CIs afetados pelo mesmo e, ainda, o grau de dependência da organização em relação ao CI afetado.

A gerência de incidentes deverá tratar os diversos tipos de eventos relacionados com a segurança computacional como um incidente. Exemplos desses eventos são os seguintes: alertas provenientes de sistemas de gerenciamento, alertas provenientes do IDS, alertas provenientes do *Firewall* e percepção do usuário em relação a comportamento anormal de um sistema ou rede.

Entre os indicadores de performance a serem incluídos no modelo para permitir a avaliação e possíveis ajustes encontram-se o seguinte: número de alertas registrados; número de incidentes relatados ao *Service Desk* referentes a exploração das vulnerabilidades descritas nos alertas; número de usuários atingidos pela divulgação do alerta; número de alertas registrados após a ocorrência de incidentes relacionados com o alerta.

6.8.2 Proposta para o Processo de Gerenciamento de Problemas

O processo de gerência de problemas deverá considerar a análise periódica de eventos registrados pela Gerência de Incidentes e apresentar um plano de ação para atacar a causa raiz antes que incidentes de segurança computacional possam ocorrer. Um comportamento esperado para o processo de Gerência de Problemas é que esse processo seja capaz de minimizar, ou se possível não permitir, a ocorrência de incidentes de segurança computacional em função de falhas ou vulnerabilidades que já foram descobertas e divulgadas.

O tratamento de vulnerabilidades é proposto para esse processo, sendo que suas atividades serão estendidas para realizar o seguinte:

- a) Análise da vulnerabilidade** - Executar a análise técnica e examinar a vulnerabilidade em hardware e em software. Isto inclui a verificação da vulnerabilidade suspeita e o exame técnico do hardware ou software para determinar onde está localizada e como pode ser explorada. A análise poderá incluir revisar o código fonte, usar depurador para determinar onde a vulnerabilidade ocorre ou tentar reproduzir o problema em um ambiente de teste.
- b) Resposta à vulnerabilidade** - Determinar a ação apropriada para eliminar ou reparar a vulnerabilidade. Isso pode incluir o desenvolvimento de *patches* de correção e soluções de contorno. Também envolve notificar outras organizações (CSIRTs) sobre a estratégia de eliminação, a possibilidade de gerar e distribuir alertas em um nível de compreensão definido pelo público alvo. Estabelecer um elo de colaboração entre organizações surge como uma proposta promissora para um trabalho colaborativo.
- c) Coordenar a Resposta à Vulnerabilidade** - Notificar as várias partes da organização sobre ações adotadas em relação à vulnerabilidade e compartilhar informação sobre

como foi eliminada a vulnerabilidade. Verificar se a estratégia de resposta à vulnerabilidade foi bem implementada.

Após uma análise de evento, a gerência de problemas deverá encaminhar uma requisição de mudança (RFC) para a gerência de mudanças, de forma que a base de conhecimento seja atualizada com as informações da estratégia de resposta à vulnerabilidade. Esse processo também deverá prover mecanismos para que essas informações sejam públicas, de fácil acesso e amplamente divulgadas dentro da organização e também fora dela quando for necessário.

Entre os indicadores de desempenho a serem incluídos no modelo para permitir a avaliação e possíveis ajustes encontram-se os seguintes: número de vulnerabilidades corrigidas; número de contatos com outros centros especializados em segurança; número de Requisições de Mudança (RFCs) geradas a partir da análise de vulnerabilidade; número de incidentes relacionados à vulnerabilidade reportados ao *Service Desk* após a análise da vulnerabilidade.

6.8.3 Proposta para o Processo de Gerenciamento de Mudanças

Do ponto de vista de segurança computacional, o processo de Gerência de Mudanças é um dos mais importantes processos no nível operacional. É nesse processo que novas medidas de segurança serão introduzidas na infra-estrutura de TI e onde medidas existentes serão aferidas, de acordo com as mudanças na infra-estrutura de TI. É também onde é checado se as mudanças no sistema são implementadas sem comprometer o ambiente de segurança existente.

Além do apresentado acima, o processo de gerenciamento de mudanças passará a exercer atividades proativas relacionadas com a publicação de eventos relacionados com a segurança computacional. Esse processo deverá ser responsável pela busca de eventos, por exemplo, vulnerabilidades que passam a ser de conhecimento público, e cuidar para que seja reduzido ao mínimo o tempo entre a publicação do evento e a disseminação de seu conteúdo dentro da organização.

6.8.4 Proposta de Inclusão do processo de Gerenciamento de Comportamento

Neste trabalho propõe-se a inclusão de um novo processo no modelo ITIL, denominado Gerenciamento de Comportamento. Esse processo irá permitir que objetivos de controle específicos de segurança computacional sejam tratados no nível tático. Essa proposta advém da necessidade de se definir serviços proativos no nível tático em um modelo para Governança da Segurança Computacional.

Serviços proativos são necessários para melhorar a infra-estrutura e os processos de segurança de uma organização antes que um incidente ocorra. A meta principal deste processo é ajudar a evitar um incidente a partir da análise de desvios de comportamento na infra-estrutura de TIC e, se o incidente ocorrer, reduzir seu impacto e abrangência.

O responsável pelo processo de Gerenciamento de Comportamento deverá ser um especialista em segurança computacional, que deverá estar dedicado exclusivamente à análise do comportamento das mais diversos elementos e atividades que podem conter indícios a respeito da ocorrência de um incidente. Essa atividade levará a uma análise periódica de dados provenientes dos mais diversos elementos do ambiente, tais como *Firewall*, Sistemas de Detecção de Intrusão – SDI, Agentes, *Proxy*, Roteadores, MIB, sensores, ferramentas de gerenciamento, *logs* etc.

Os seguintes são alguns exemplos de informações que podem ser geradas a partir dos dados assim coletados: previsão de manutenção de equipamento; indicadores de desempenho; regras para a redefinição da política de segurança; atualização de softwares com base em variações de formas de ataque e reconfiguração de equipamentos com base em informações extraídas dos dados históricos.

Entre outros exemplos de atividades previstas para este processo estão:

- **Publicações sobre Segurança** - Esta atividade está relacionada com a elaboração de alertas de intrusão, alertas sobre vulnerabilidades e medidas de segurança para o nível operacional e tático. Estas publicações irão informar todos os membros da organização sobre novas formas de ataque e proteção, como uma nova vulnerabilidade descoberta ou um novo *patch* de correção. Durante o processo de

publicação deverá ser levada em consideração uma adequação do nível da linguagem escrita aos vários níveis de conhecimento dos indivíduos da organização. As publicações irão permitir que a organização proteja seus sistemas e rede contra novos tipos de comprometimento antes que eles possam ser explorados.

- **Monitoramento de novas tecnologias** - Monitorar e observar o desenvolvimento de novas técnicas, atividades de intrusão e tendências relacionadas para ajudar a identificar futuras ameaças. Essa atividade envolverá ler documentos publicados em listas de discussão especializadas em segurança computacional, inclusive listas organizadas por invasores, *sites* especializados em segurança, notícias atuais e artigos publicados em revistas de perfil científico, tecnológico, político e governamental para extrair informações relevantes sobre segurança dos sistemas e da rede da organização.
- **Auditoria de segurança** - Esta atividade provê uma revisão e análise detalhada da infra-estrutura de segurança da organização, baseados nos requisitos definidos no nível estratégico da organização. Isso poderá envolver recomendações para a revisão da política de segurança em prática na organização. Existem diferentes tipos de auditoria que podem ser utilizadas, incluindo os seguintes:
 - revisão da infra-estrutura: revisão das configurações de hardware e software, roteadores, *firewalls*, servidores etc;
 - revisão das práticas adotadas: entrevistar empregados e administradores de sistemas e redes para determinar se suas práticas de segurança estão de acordo com a política de segurança prevista para organização;
 - varreduras automáticas: usar ferramentas de detecção de vulnerabilidades para identificar quais sistemas e redes podem estar vulneráveis;
 - testes de penetração: testar a segurança do ambiente através da simulação de ataques;

Para a realização das atividades apontadas, torna-se necessário a autorização formal de todos os envolvidos. Alguns dos testes apontados podem ser proibidos pela política de segurança da organização, necessitando de uma aprovação prévia.

- **Configuração e manutenção de ferramentas de segurança, aplicações, infraestrutura e serviços** - Desenvolver e disseminar guias de como configurar corretamente e manter seguro as ferramentas, aplicações e a infraestrutura usada pela equipe de segurança.
- **Desenvolvimento de Ferramentas de Segurança** - Essa atividade inclui o desenvolvimento de novas ferramentas que são necessárias na organização.

6.9 Considerações Finais

A necessidade de Governança de Segurança da Informação leva à necessidade de um modelo que possa ser utilizado em todos os níveis organizacionais. Este capítulo apresentou a proposta de expansão do modelo ITIL para que este possa ser utilizado no nível operacional e tático do modelo proposto para Governança da Segurança da Informação. Com essa expansão será possível contemplar todos os objetivos de controle previstos na ISO 17799 e no modelo COBIT

A expansão proposta para o modelo ITIL foi desenvolvida após uma revisão do termo incidente de segurança computacional, a correlação das atividades previstas em um CSIRT com as atividades previstas no modelo ITIL e o seu mapeamento na Estrutura de Decisões utilizada em Sistemas de Informação.

A validação do modelo proposto, apresentado na Figura 6.6, será apresentada no Capítulo 8, juntamente com a validação de toda a proposta deste trabalho. Para validação serão apresentados os resultados obtidos a partir da implantação da proposta no Centro de Computação Eletrônica da Universidade de São Paulo.

Na Figura 6.6 encontram-se destacados os processos ITIL modificados, o novo processo inserido no modelo e os seus relacionamentos.

Figura 6-6: Proposta de adaptação do Modelo ITIL com base nas melhores práticas para a implantação de CSIRTs.

7 Proposta para um Modelo de Governança da Segurança da Informação com Base em Sistemas de Informação

7.1 Considerações Iniciais

No capítulo 5 apresenta-se a motivação para o desenvolvimento de um modelo de Governança da Segurança da Informação. Os requisitos necessários para a obtenção desse modelo foram apresentados naquele capítulo juntamente com a proposta de uma combinação das potencialidades dos modelos ITIL, COBIT e da norma ISO 17799 para o atendimento desses requisitos. A partir do desenvolvimento neste trabalho de uma correlação entre os objetivos de controle apresentados nesses 3 modelos, foi identificada a necessidade de expansão do modelo ITIL para que o mesmo permita a implementação de todos os objetivos de controle necessários a um modelo de Governança da Segurança da Informação. Essa expansão do modelo ITIL foi apresentada no Capítulo 6.

Neste capítulo descreve-se como o modelo Governança da Segurança da Informação proposto neste trabalho será estruturado.

7.2 Utilização da Estrutura de Decisão de Sistemas de Informação Gerenciais

O ponto de partida para a construção do modelo de Governança da Segurança da Informação proposto neste trabalho consiste na definição de uma estrutura baseada nos modelos de tomada de decisão em Sistemas de Informações Gerenciais. Nessa estrutura, um *Data Warehouse* é responsável por armazenar os mais diversos tipos de dados relacionados com a segurança computacional provenientes do ambiente, e que serão úteis no processo da extração do conhecimento necessário ao gestor para o planejamento estratégico da organização.

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

Nessa estrutura, o processo de extração de conhecimento da base de dados tem no nível operacional os dados como matéria prima bruta. Através dos processos descritos no modelo apresentado no Capítulo 6, o sistema de informação permitirá que esses dados sejam coletados,

armazenados e trabalhados para que possam gerar informação no nível tático. A partir dos processos de auditoria, monitoração e 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, neste trabalho propõe-se a estruturação dos requisitos propostos no Capítulo 5 de uma forma que possa ter enfoque também em controles, processos, pessoas e tecnologias, compondo uma matriz 3x4 que pode ser representada através da proposta apresentada na Figura 7-1.

Figura 7-1: Estrutura proposta para um Modelo para Governança da Segurança da Informação.

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

- **Controles - o que:** Relação dos objetivos de controle a serem aplicados;
- **Processos - como:** Descrição dos processos necessários para implementação dos objetivos de controle;
- **Pessoas - quem:** Papéis e responsabilidades dos indivíduos envolvidos com os processos e objetivos de controle definidos;
- **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:

- **Operacional:** Atividades diárias, cotidianas e reativas;
- **Tático:** Atividade proativas com revisões periódicas, busca contínua pela qualidade e possibilidade de planejamento em longo prazo;

- **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 7.1 é apresentada a correlação entre os requisitos propostos no capítulo 5 para um modelo de Governança da Segurança da Informação e as estratégias propostas neste trabalho para sua implementação.

Tabela 7-1: Proposta de estratégia para implementação dos requisitos identificados neste trabalho para um modelo de Governança da Segurança da Informação.

Requisitos para um Modelo de Governança da Segurança da Informação	Estratégia para a Implementação
1. Os CEOs (<i>Chief Executive Officers</i>) 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 um modelo de Governança da Segurança da Informação, a Tabela 7.2 apresenta uma visão macro da proposta para um modelo de Governança da Segurança da Informação.

Tabela 7-2: Correlação da ISO 17799 com os modelos COBIT e ITIL como proposta para um modelo de Governança da Segurança da Informação.

	Operacional	Tático	Estratégico
Controles	1. ISO 17799 2. COBIT: Entrega e Suporte 3. COBIT: Aquisição e Implementação	1. ISO 17799 2. COBIT: Entrega e suporte	1. ISO 1799 2. Análise de Risco 3. COBIT: Auditoria 4. COBIT: Monitoramento 5. COBIT: Planejamento e Organização
Pessoas	1. ITIL: Suporte a Serviços (adaptado)	1. ITIL: Entrega de Serviços (expandido)	1. COBIT: Auditoria 2. COBIT: Monitoramento
Processos	2. ITIL: Suporte a Serviços (adaptado)	1. ITIL: Entrega de Serviços (expandido)	1. COBIT: Auditoria 2. COBIT: Monitoramento
Tecnologia	1. Ferramentas de <i>Workflow</i> 2. Ferramentas de Gerenciamento (coleta de dados) 3. <i>Data Warehouse</i>	1. Ferramentas de <i>Workflow</i> 2. Ferramentas de Gerenciamento (coleta de dados) 3. <i>Data Warehouse</i> 4. Ferramentas para testes de vulnerabilidade e penetração 5. Ferramentas para análise de logs	1. Ferramentas automatizadas para análise de Risco. 2. Ferramentas automatizadas para a extração de conhecimento

Este trabalho propõe a utilização dos modelos COBIT e ITIL e pelo fato de possuírem uma coleção das melhores práticas para auxiliar a Governança da Tecnologia da Informação e Comunicação, compiladas a partir da experiência profissional e práticas adotadas por *experts* que atuam pelo mundo todo. Esses modelos são reconhecidos e adotados internacionalmente em larga escala.

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 TIC oferecidos.

Esses objetivos de controle, que são apresentados em alto nível pelo modelo COBIT e de forma detalhada pela norma ISO 17799, deverão ser mapeados para os processos descritos no modelo ITIL. Dessa forma, neste trabalho propõe-se 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.

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. Uma 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.

7.3 O Nível Operacional

O nível operacional descreve atividades diárias, cotidianas e reativas para manter a infraestrutura de TIC em funcionamento. A seguir são detalhadas as dimensões *Controle-Processos-Pessoas-Tecnologia* para este nível.

7.3.1 Dimensão Controles: Definição dos Objetivos de Controle

Objetivos de Controle presentes no modelo COBIT e identificados neste trabalho para este nível são apresentados na Tabela 7-3:

Tabela 7-3: Objetivos de Controle identificados no modelo COBIT para o Nível Operacional

a) Domínio: Aquisição e Implementação:	b) Domínio: Entrega e Suporte:
AI3-Adquirir e Manter Infra-estrutura Tecnológica	DS5-Garantir Segurança de Sistemas
AI4-Desenvolver e Manter Procedimentos	DS7-Educar e Treinar Usuários
AI5-Instalar e Validar Sistemas	DS8-Auxiliar e Aconselhar Clientes
AI6-Gerenciar Mudanças	DS9-Gerenciar Configuração
	DS10-Gerenciar Problemas e Incidentes
	DS11-Gerenciar Dados
	DS13-Gerenciar a Operação

Os objetivos de controle do modelo COBIT descritos anteriormente deverão incorporar os objetivos de controle da norma ISO 17799 para que possam maximizar suas potencialidades em relação à segurança computacional.

7.3.2 Dimensão Processos: Implementação dos Objetivos de Controle

Os objetivos de controle identificados na norma ISO 17799 e no modelo COBIT serão implementados através dos processos descritos na proposta de adaptação do modelo ITIL para o nível Operacional apresentado no Capítulo 6. Assim, para o nível Operacional este trabalho propõe que sejam utilizados os seguintes processos:

- Gerenciamento de Incidentes/*Service Desk* (adaptado neste trabalho);
- Gerenciamento de Configurações;
- Gerenciamento de Problemas (adaptado neste trabalho);
- Gerenciamento de Mudanças (adaptado neste trabalho);
- Gerenciamento de Versões;

7.3.3 Dimensão Pessoas: Definição de Papéis e Responsabilidades dos Indivíduos Envolvidos

Nesta dimensão, deseja-se apresentar uma documentação clara e objetiva sobre o que é esperado de cada um dos envolvidos com o processo através de uma documentação formal contendo os papéis e responsabilidades para cada indivíduo. A partir de uma análise do detalhamento dos processos do modelo ITIL é possível extrair os indicativos para esta definição.

Uma relação clara de indicadores de performance e fatores críticos de sucesso devem ser definidos para que cada indivíduo possa saber se está cumprindo o que é esperado dentro de todo o processo.

Os processos do modelo ITIL que poderão ser utilizados para a extração dos indicadores para a definição dos papéis e responsabilidade estão presentes no módulo *Suporte a Serviços*, sendo relacionados a seguir:

- Gerenciamento de Incidentes/*Service Desk* (adaptado neste trabalho);
- Gerenciamento de Configurações;
- Gerenciamento de Problemas (adaptado neste trabalho);

- Gerenciamento de Mudanças (adaptado neste trabalho);
- Gerenciamento de Versões;

7.3.4 Dimensão Tecnologia: Ferramentas de Apoio ao Modelo

Nesta dimensão deverão ser escolhidas as ferramentas para que a implementação do modelo para Governança da Segurança da Informação seja realizada conforme o previsto par o nível operacional do processo de tomada de decisão em sistemas de informações gerenciais. A estrutura de banco de dados deverá ser definida para armazenar os mais diversos dados provenientes do ambiente e que possam ser relacionados para gerar informação acerca do ambiente a ser protegido.

As bases de dados propostas no modelo ITIL deverão ser consideradas e correlacionadas para a obtenção de um *Data Warehouse*. Entre as bases de dados que deverão ser propostas para o nível operacional, o modelo ITIL apresenta as seguintes:

- Base de dados para registro de Incidentes;
- Base de dados para registro de problemas;
- Base de dados para Erros conhecidos;
- CMDB (*Configuration Management Data Base*): Base de Dados dos itens de configuração do ambiente;
- Base de dados para soluções de contorno;

Ferramentas de fluxo de trabalho deverão ser analisadas para fornecer apoio à implantação dos processos previstos para o nível Operacional. Preferencialmente, essas ferramentas deverão possuir a capacidade de registro automático de incidentes a partir de dados coletados por agentes/sensores (por exemplo: agentes SNMP) espalhados pelo ambiente e, ainda, o registro automático dos *logs* gerados pelos mais diversos sistemas que compõem a infraestrutura de TIC.

7.4 O Nível Tático

O nível tático será responsável pela garantia da qualidade dos serviços de TIC oferecidos e pela busca contínua de melhoria dessa qualidade. Para isso, os dados coletados e armazenados

no nível operacional serão correlacionados através do sistema de informação para gerar informações que possam úteis ao incremento do nível de qualidade.

7.4.1 Dimensão Controles: Definição dos Objetivos de Controle

Objetivos de Controle presentes no modelo COBIT e identificados neste trabalho para este nível são os apresentados na tabela 7.4:

Tabela 7-4: Objetivos de Controle identificados no modelo COBIT para o Nível Tático

a) Domínio: Aquisição e Implementação:	b) Domínio: Entrega e Suporte:
AI1-Identificar Soluções Automatizadas	DS1-Definir e Gerenciar Níveis de Serviço
AI3-Adquirir e Manter Infra-estrutura Tecnológica	DS2-Gerenciar Serviços de Terceiros
AI4-Desenvolver e Manter Procedimentos	DS3-Gerenciar Desempenho e Capacidade
AI5-Instalar e Validar Sistemas	DS4-Garantir Continuidade dos Serviços
	DS5-Garantir Segurança de Sistemas
	DS6-Identificar e Alocar Custos
	DS7-Educar e Treinar Usuários
	DS8-Auxiliar e Aconselhar Clientes
	DS12-Gerenciar Instalações

Os objetivos de controle do modelo COBIT descritos anteriormente deverão incorporar os objetivos de controle da norma ISO 17799 para que possam maximizar suas potencialidades em relação à segurança computacional.

7.4.2 Dimensão Processos: Implementação dos Objetivos de Controle

Este trabalho propõe que objetivos de controle identificados na norma ISO 17799 e no modelo COBIT sejam implementados através dos processos descritos na proposta de expansão do modelo ITIL para o nível Tático, apresentado no capítulo 6. Assim, para o nível Tático este trabalho propõe que sejam utilizados os seguintes processos:

- Gerenciamento de Nível de Serviço;
- Gerenciamento de Capacidade;
- Gerenciamento de Continuidade;
- Gerenciamento Financeiro;
- Gerenciamento de Disponibilidade;
- Gerenciamento de Comportamento (Definido neste trabalho).

7.4.3 Dimensão Pessoas: Definição de Papéis e Responsabilidades dos Indivíduos Envolvidos

Os papéis e responsabilidades para os indivíduos envolvidos no nível tático poderão ser definidos a partir dos indicativos presentes nos processos do modelo ITIL propostos neste trabalho para esse nível. Conforme proposto no Capítulo 6, os processos ITIL para o nível tático que poderão fornecer esses indicativos são os seguintes:

- Gerenciamento de Nível de Serviço;
- Gerenciamento de Capacidade;
- Gerenciamento de Continuidade;
- Gerenciamento Financeiro;
- Gerenciamento de Disponibilidade;
- Gerenciamento de Comportamento (Definido neste trabalho).

7.4.4 Dimensão Tecnologia: Ferramentas de Apoio ao Modelo

Assim como na dimensão tecnológica do Nível Operacional, é proposta a utilização ferramentas na dimensão tecnológica no Nível Tático que possam prover: a automação do fluxo de trabalho, tais como ferramentas de *workflow*, um *Data Warehouse* e o suporte automatizado ao gerenciamento da infra-estrutura de TIC. Essas ferramentas serão utilizadas nessa dimensão para correlacionar os dados obtidos (matéria prima), transformando-os em informações úteis ao processo de melhoria contínua da qualidade da segurança computacional dos serviços providos pela infra-estrutura de TIC.

É proposto também que nesta dimensão sejam utilizadas ferramentas automatizadas para a realização de testes de vulnerabilidades e testes de penetração. A partir da informação gerada por essas ferramentas, será possível identificar possíveis vulnerabilidades no ambiente a ser protegido.

Por último, é proposta a utilização de ferramentas automatizadas para análise de eventos, tais como *logs* que são armazenados como dados brutos no nível operacional. A dificuldade na extração de informação desse tipo de evento é diretamente proporcional ao volume de dados gerados. Dessa forma, a utilização de uma ferramenta automatizada torna-se imprescindível para

ajudar na análise em tempo hábil de eventos gerados pelos IDSs, *firewalls*, ferramentas de gerenciamento, roteadores etc.

7.5 O Nível Estratégico

O nível estratégico será responsável por extrair conhecimento das bases de dados que compõem o sistema de informação, promover auditorias e análises de risco e monitorar o ambiente de forma que os gestores da organização possam incorporar as questões de segurança computacional em suas ações de governança corporativa.

7.5.1 Dimensão Controles: Promover Análise de Risco, Auditoria e Definir Objetivos de Controle

Os objetivos de controle identificados neste trabalho para este nível são apresentados na Tabela 7-5.

Tabela 7-5: Objetivos de controle identificados no modelo COBIT para o nível Estratégico.

a) Planejamento e Organização:	b) Monitoramento:
PO1-Definir um Plano Estratégico de TI	M1-Monitorar os Processos
PO2-Definir a Arquitetura da Informação	M2-Avaliar a Adequação do Controle Interno
PO3-Determinar a Direção Tecnológica	M3-Obter certificação Independente
PO4-Definir a Organização e Relacionamentos de TI	M4-Providenciar Auditoria Independente
PO5-Gerenciar o Investimento em TI	
PO6-Comunicar metas e diretivas gerenciais	
PO7-Gerenciar Recursos Humanos	
PO8-Garantir Conformidade com Requisitos Externos	
PO9-Avaliar Riscos	
PO10-Gerenciar Projetos	
PO11-Gerenciar Qualidade	

Além de fornecer os objetivos de controle, o modelo COBIT será utilizado nessa dimensão para prover um guia de auditoria para avaliações periódicas desses objetivos de controle.

Uma Análise de Risco deverá ser realizada para permitir que os gestores tenham conhecimento acerca dos riscos existentes que podem comprometer a realização da missão da

organização. Este conhecimento guiará o gestor no nível de investimento ideal para cada objetivo de controle identificado.

7.5.2 Dimensão Processos: Auditoria e Monitoração dos Processos estabelecidos

Todos os processos precisam ser regularmente avaliados ao longo do tempo em relação à sua qualidade e conformidade com os controles exigidos. Nessa dimensão serão utilizados os objetivos de controle fornecidos pelo COBIT para Monitoramento e suas diretrizes de auditoria para permitir uma auditoria interna ou externa.

7.5.3 Dimensão Pessoas: Auditar e Monitorar as Atividades Exercidas pelos Indivíduos

Assim como na dimensão de processos, a auditoria também deve ser aplicada às pessoas. O conhecimento gerado a partir da auditoria irá guiar a organização numa tentativa de reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações.

7.5.4 Dimensão Tecnologia: Facilitar Análise de Risco e Extração de Conhecimento

Uma Análise de Risco deverá ter o suporte de um conjunto de ferramentas automatizadas caso ela seja realizada internamente. As ferramentas corretas deverão ser identificadas e disponibilizadas no momento da auditoria. Essas ferramentas vão desde planilhas eletrônicas com formulários de análise de Risco até ferramentas totalmente automatizadas com capacidade de coleta de dados e extração de conhecimento de base de dados.

Uma vez estruturado o sistema de informação, uma metodologia de extração de conhecimento de base de dados deve ser aplicada. A escolha dessas ferramentas está relacionada com a estrutura de *Data Warehouse* estabelecido para o nível operacional e para o nível tático.

7.6 Considerações Finais

Neste capítulo apresentou-se a proposta para um modelo de Governança da Segurança da Informação definido com base na estrutura utilizada pelo processo de tomada de decisão para os Sistemas de Informação Gerenciais.

Uma vez implementado, esse modelo permitirá aos gestores ter o gerenciamento das questões relativas à segurança computacional alinhadas ao planejamento estratégico da organização.

8 Estudo de Caso: A Segurança Computacional no CCE/USP

8.1 Considerações Iniciais

A Universidade de São Paulo (USP) possui uma Coordenadoria de Tecnologia da Informação (CTI) que é responsável pelo alinhamento de TIC com a atividade fim da Universidade: ensino, pesquisa e extensão de serviços à comunidade. A CTI traça as políticas para a Universidade na área, executa parte dessas políticas e coordena a execução da outra parte pelos Centros de Informática e Prefeituras dos *campi* da USP. Estão subordinados à CTI, o Centro de Computação Eletrônica (CCE) e os Centros de Informática dos *campi* de São Carlos (CISC), Ribeirão Preto (CIRP) e Piracicaba (CIAGRI). A CTI é responsável pela Governança de TIC na Universidade e os centros executores são responsáveis pela Gestão de TI nas suas áreas de atuação.

O CCE é o ponto de contato para a comunidade externa para as questões relacionadas com a segurança computacional e com administração das contas de e-mail abuse@usp.br e security@usp.br.

Um estudo de caso utilizando o modelo proposto neste trabalho foi realizado no Centro de Computação Eletrônica (CCE), que é o centro executor que oferece serviços de TIC para o campus da USP em São Paulo e que gerencia também o *backbone* da USPNet, rede de comunicação da USP. O estudo de caso foi realizado a partir da implementação no CCE de parte do modelo proposto e de encaminhamentos à CTI de propostas para a definição de uma Política de Segurança para a Universidade de São Paulo e para a criação de algumas normas envolvendo segurança computacional.

8.2 Cenário Encontrado no Início do Projeto

Os principais problemas relacionados com a segurança computacional encontrados no Centro de Computação Eletrônica no início do desenvolvimento deste trabalho foram os seguintes:

Nível Operacional

- Inexistência de um ponto único de contato para assuntos relacionados com segurança computacional;
- Inexistência de uma definição formal dos papéis e das responsabilidades das pessoas envolvidas com o tratamento das questões de segurança computacional;
- Inexistência de ações coordenadas para a resposta aos incidentes de segurança computacional.
- Os incidentes de segurança computacional eram tratados apenas de forma reativa;
- Os incidentes de segurança computacional recebidos não eram registrados e catalogados;
- As falhas de segurança muitas vezes eram percebidas inicialmente pelos próprios usuários.

b) Nível Tático

- Não era possível obter uma estatística a respeito dos incidentes relatados;
- Não havia um canal de comunicação com outros Centros de Resposta a Incidentes (CAIS, CERT-BR etc) para troca de informações;
- Análise de eventos relacionados à segurança computacional (análise de *logs*) era realizada de forma reativa;
- O CCE assumia muitas das ações que poderiam ser delegadas às unidades da USP conectadas a ele através da USPNet. Com isso, os roteadores de entrada/saída eram sobrecarregados com uma grande quantidade de *listas-de-acesso*;

c) Nível Estratégico

- Inexistência de uma política de segurança formal;
- Falta de Conhecimento que pudesse demonstrar de forma objetiva os riscos pertinentes ao ambiente;
- Impossibilidade de gerar conhecimento para a definição do quanto e onde investir em segurança computacional.

Os gráficos apresentados na figura 8-1 foram desenvolvidos para apresentar uma análise da situação apresentada pelo cenário descrito anteriormente e o quanto o mesmo poderia evoluir.

Os resultados obtidos serviram como motivadores para o desenvolvimento deste trabalho. A ferramenta utilizada na extração de dados para essa avaliação é proposta pelo *Corporate Governance Task Force* [NSCP, 2004]. O anexo B apresenta os formulários extraídos dessa ferramenta e utilizados neste trabalho.

A análise foi realizada para as questões relacionadas com Pessoas, Processos e Tecnologia, uma vez que modelo proposto neste trabalho considera essas dimensões em seu desenvolvimento. A dimensão Controles poderá ser avaliada a partir dos processos de auditoria propostos pelo modelo COBIT.

Figura 8-1: Análise de Gaps para o cenário descrito em relação a Pessoas, Processos e Tecnologia.

8.3 Adoção de Melhores Práticas para Gestão da Segurança Computacional

As primeiras ações para uma melhor gerência das questões relativas à segurança computacional no cenário descrito dizem respeito ao nível operacional do modelo proposto no Capítulo 7 deste trabalho.

Inicialmente, estruturou-se uma equipe de resposta aos incidentes de segurança computacional a partir de uma análise das melhores práticas para o estabelecimento de CSIRTs- *Computer Security Incidentes Response Teams*. O acrônimo CSIRT foi utilizado para denominar o grupo em função do mesmo ter reconhecimento internacional, o que facilitaria a interação com demais grupos ao redor do mundo. Para o estabelecimento do CSIRT, foram implementadas as seguintes ações:

Dimensão de Controles:

- Identificação dos controles estabelecidos na norma ISO 17799 e no modelo COBIT para o estabelecimento de um CSIRT local.

Dimensão de Pessoas:

- Identificação das pessoas (papéis e responsabilidades) envolvidas com as ações do CSIRT;
- Capacitação das pessoas envolvidas para lidar com as particularidades dos incidentes de segurança computacional;
- Capacitação da equipe de operações existente CCE, que possui uma jornada de trabalho 24horas x 7dias da semana x 365dias por ano, para uma primeira resposta aos incidentes como forma de minimizar os impactos decorrentes dos mesmos;

Dimensão de Processos

- Implementação de uma estrutura de resposta a incidentes contemplando as etapas de Triagem e Encaminhamento, Análise de Incidentes, *Feedback* e Divulgação de resultados conforme proposto pelos trabalhos de West-Brown(2002) e Alberts (2004).

Dimensão de Tecnologia

- Implementação da Ferramenta *SiRI* [BERNARDES et al, 2003] para auxiliar na automatização do fluxo de trabalho do CSIRT estabelecido;
- Utilização de ferramentas de Gerenciamento para coleta de dados de equipamentos tidos como críticos para a infra-estrutura de TIC.

Pode-se dizer que a partir das iniciativas para a implementação do CSIRT houve uma motivação da equipe envolvida, criando-se a cultura de “segurança computacional” no Centro de Computação Eletrônica. Isso pode ser comprovado pela dedicação das pessoas envolvidas na busca contínua por novos modelos e ferramentas que possam elevar o nível de maturidade dos processos utilizados para gerenciamento da segurança computacional.

As primeiras ações (associadas ao nível operacional do Modelo Proposto neste trabalho) permitiram outras ações relacionadas e que podem ser associadas ao nível tático e estratégico. Dois exemplos dessas ações são apresentados nas subseções a seguir:

8.3.1 Exemplo 01: Definição de uma Política para Servidores de E-mail

A partir de uma base de dados contendo os registros dos incidentes realizados através da ferramenta *SiRI* [BERNARDES et al., 2003], foi possível estabelecer uma categorização dos tipos de incidentes e, ainda, o desenvolvimento de estatísticas relacionadas com essa categorização, conforme exemplificado na Figura 8-2. Com isso, foi possível identificar um volume alto de incidentes, cerca de 20 incidentes diários, relacionados com reclamações sobre o envio de SPAM a partir da exploração de equipamentos mal-configurados (*open-relay*) na Universidade de São Paulo.

As ações referentes a esse tipo de incidentes incluíam o seguinte:

- Notificar o responsável pela rede onde se encontrava o equipamento sobre o incidente e recomendar ações para a resolução do mesmo;
- No caso de recebimento de uma nova reclamação após a notificação do responsável, bloquear, através da implementação de *access-list* nos roteadores, o envio de e-mails a partir do equipamento envolvido.

Com o grande volume de incidentes relacionados a SPAM, as ações acima implicavam o seguinte:

- Volume alto de trabalho relacionado com o envio de notificações;
- Sobrecarga da capacidade de processamento dos roteadores com a inclusão de diversas *access-list*, e;
- Dificuldade de determinar o momento para a remoção da *access-list* da configuração dos roteadores.

Figura 8-2: Notificações recebidas sobre incidentes de segurança computacional originados na USP em 2004

A partir da análise das informações contidas nas estatísticas elaboradas, as seguintes ações foram estabelecidas:

- **Nível Tático** - Partindo do levantamento de todos os servidores de e-mail da universidade, criar um conjunto de regras permitindo o envio de e-mails somente a partir destes servidores. Esse no conjunto de regras representou cerca de 10% do volume de regras existentes até aquele momento. Com esse novo conjunto de regras houve uma diminuição significativa na carga de processamento nos roteadores. Houve uma redução de 87% no volume de notificações de incidentes referentes a SPAM, uma vez que o envio de e-mail passou a ser permitido apenas aos servidores reconhecidos pelas unidades da USP;

- **Nível Estratégico** - Aprovação de uma Política de Segurança pela CTI delegando maiores responsabilidades aos administradores locais de servidores de e-mail e criação de uma portaria para permitir que a equipe de segurança tenha autoridade para bloquear um servidor de e-mail quando o mesmo for identificado como origem de SPAMs.

8.3.2 Exemplo 02: Coleta de Dados Críticos

Em um final de semana de abril de 2003, um ataque bem sucedido a um roteador da USPNet acarretou a indisponibilidade de parte da rede por 36 horas. Apesar de o incidente ter sido identificado pela equipe de operações do CCE poucos instantes após a sua ocorrência, o fato do mesmo ter ocorrido no final de uma tarde de sábado, dificultou o processo de acionamento da equipe do NOC (*Network Operation Center*), responsável pelo restabelecimento dos serviços.

A falta de informação acerca do incidente levou a equipe do NOC a atribuir a indisponibilidade da rede primeiramente à possibilidade de uma falha no hardware do equipamento, o que contribuiu para prolongar o tempo de indisponibilidade dos serviços.

Nesse incidente, uma vulnerabilidade existente no sistema utilizado em um dos roteadores permitiu que um único microcomputador contaminado com um *worm* fosse capaz de explorar essa vulnerabilidade e elevar a taxa de utilização da CPU desse roteador a 100%, tornando esse roteador indisponível após algumas horas de utilização da carga máxima de sua CPU.

Figura 8-3: Taxa de utilização de CPU de um roteador envolvido em um incidente de segurança

A Figura 8.3 ilustra os dados referentes à taxa de utilização da CPU para o roteador envolvido no incidente descrito, destacando o momento onde ocorreu o incidente. O gráfico apresentado nessa figura foi gerado pela ferramenta de monitoramento MRTG (*Multi Router Traffic Grapher*), uma das ferramentas (nível operacional) utilizadas para o monitoramento da USPNet.

A partir da implementação no CCE de parte do modelo proposto neste trabalho, foram realizadas as ações descritas a seguir.

- **Nível Estratégico:** Foi nomeada, através de uma portaria do coordenador do CCE, uma comissão para o desenvolvimento da proposta de uma Política de Segurança a ser encaminhada à CTI para aprovação. No desenvolvimento desta política de segurança a comissão realizou uma análise de riscos para os principais equipamentos que compõem o *backbone* da USPNet levando em consideração os controles propostos pela norma ISO 17799. Como resultados dessa análise, foram identificados o nível de risco e o nível de impacto dos incidentes relacionados a esses equipamentos. Com isso, os equipamentos com alto nível de sensibilidade (equipamentos críticos para o correto funcionamento da USPNet, como os roteadores de core e de borda) foram identificados.
- **Nível Tático:** Com base na experiência extraída a partir desse ataque bem sucedido, as informações sobre esse tipo de ataque foram documentados em um banco de conhecimento e os dados relativos à taxa de utilização das CPUs dos equipamentos identificados passaram a ser monitorados.
- **Nível Operacional:** As ferramentas de gerenciamento de redes e agentes sensores foram ajustados para monitorar os equipamentos com alto nível de sensibilidade e coletarem dados que, quando correlacionados, pudessem gerar informações sobre quebras de segurança.

Com a adoção dessas medidas, um outro incidente com as mesmas características, foi tratado de uma forma diferente. Na Figura 8-4 é possível observar o tempo demandado desde o início da ocorrência do incidente até o seu encerramento.

Na Figura 8-4, a taxa média de utilização de CPU está próxima de zero pelo fato do gráfico apresentar os dados coletados entre as 12 horas de um sábado e 18 horas de um domingo, num período de férias escolares.

Figura 8-4: Taxa de utilização de CPU de um roteador envolvido em um Incidente de Segurança

Com a adoção de parte do modelo proposto neste trabalho, o incidente apresentado na figura 8.4, que possui as mesmas características do incidente apresentado na figura 8.3, foi tratado da seguinte forma:

- **Nível Operacional** - Os dados referentes à taxa de utilização da CPU do roteador começaram a ser coletados e armazenados como incidente após alcançarem um valor superior ao mínimo previamente definido como aceitável para este equipamento, com base no seu nível de impacto. Pelo fato desse roteador ser o “equipamento de borda” da rede e consequentemente possuir um valor alto para seu nível de impacto, um alerta foi gerado para o processo de Gerência de Comportamento, situado no nível tático. O processo gerência de comportamento foi implementado com base na proposta deste trabalho para a adaptação do processo de Gerência de Incidentes do modelo ITIL, descrito no capítulo 6.
- **Nível Tático** - O técnico responsável por receber os alertas gerados pelo processo de incidentes consultou a base de conhecimento e identificou um caso similar. Os procedimentos padrões para esse caso foram seguidos, sendo realizado um ajuste na configuração de uma *lista-de-acesso* para impedir o ataque. Com isso, incidente foi concluído antes que o roteador se tornasse indisponível. Ainda no nível tático, uma ferramenta para testes de vulnerabilidade foi utilizada para fazer uma varredura (*scanning*) na rede onde se localizava o microcomputador contaminado, em busca de outros equipamentos

na mesma situação e, ainda, numa tentativa de identificar qual ferramenta (*exploit*) foi utilizado no ataque.

- **Nível Estratégico** - Para o nível estratégico, uma coleção de informações como as descritas nesse caso irá gerar o conhecimento necessário para que um administrador identifique a importância em investimentos e atualização de ferramentas de testes de vulnerabilidade e penetração.

Para o nível operacional, foi utilizada a ferramenta de acompanhamento de fluxo de trabalho *Service Desk* da família *HPOpenview*. Na Figura 8-5 é possível observar o volume de incidentes registrados automaticamente nesta ferramenta.

The screenshot shows the HP OpenView Service Desk application window. The title bar reads 'hp OpenView service desk'. The menu bar includes 'Grupos', 'Editar', 'Visualização', 'Favoritos', 'Ferramentas', 'Ações', and 'Ajuda'. Below the menu is a toolbar with icons for search, refresh, and other functions. The main area displays a table of incidents. The table has columns for ID, CI, Data Descr., Sumário, Categoria, Status, and Data de Solução. The incidents are listed in descending order of ID, from 984 down to 900. The categories include Network, Hardware, and Software. The status of all incidents is 'Fechado' (Closed). The data of solution ranges from 04/02/05 00:46 to 04/02/05 17:53.

ID	CI	Data Descr.	Sumário	Categoria	Status	Data de Solução
984	CORCECEFR		Pressuranga-Motivo da queda ignorado	Network	Fechado	04/02/05 00:46
985	CORCECEFR		IF AT110131 Down <2> Capabilities: nIPRouter:nSNMPSupported:nRMON:nFrameRe	Network	Fechado	04/02/05 00:49
986	CORCECEFR		Pressuranga-Motivo da queda ignorado	Network	Fechado	04/02/05 00:52
987	CORCECEFR		Perdas de conexão/pacotes tanto pelo O.V.D quanto pelo Big Brother Ok agora	Network	Fechado	04/02/05 01:21
988	CORCECEFR		Pressuranga-Motivo da queda ignorado	Network	Fechado	04/02/05 01:22
989	BORDER		foundry:cpuutil:0 threshold exceeded (>= 85 * 1): 95. Sampled high of 95 at Fri	Network	Fechado	04/02/05 02:53
970	BORDER		foundry:cpuutil:0 threshold exceeded (>= 80 * 1): 11. Sampled high of 11 at Fri	Network	Fechado	04/02/05 02:59
971	CORCECEFR		Perdas de conexão/pacotes tanto pelo O.V.D quanto pelo Big Brother Ok agora	Network	Fechado	04/02/05 03:49
972	CORCECEFR		Pressuranga-Motivo da queda ignorado	Network	Fechado	04/02/05 04:13
973	CORCECEFR		Perdas de conexão/pacotes tanto pelo O.V.D quanto pelo Big Brother Ok agora	Network	Fechado	04/02/05 04:15
974	CORCECEFR		IF ethernet2/3 Down <2> Capabilities: nIPRouter:nSNMPSupported:nRMON:nOSPF	Network	Fechado	04/02/05 04:59
975	CORCECEFR		Pressuranga-Motivo da queda ignorado	Network	Fechado	04/02/05 05:58
976	SLB-WEBMAIL		Sistema com problemas de hardware	Hardware	Fechado	04/02/05 06:46
977	CORCECEFR		VLAN DEFAULT LINK OK, ocorrência fechada	Network	Fechado	04/02/05 07:01
978	SLB-WEBMAIL		Máquina travada. Não apresentou as requisições webmail	Hardware	Fechado	04/02/05 09:21
979	CORCECEFR		Pressuranga	Network	Fechado	04/02/05 10:00
980	CORCECEFR		Várias unidades acusaram perda de conexão e UP em seguida Ok Agora	Network	Fechado	04/02/05 10:00
981	CORCECEFR		Pressuranga-Motivo da queda ignorado	Network	Fechado	04/02/05 10:04
982	CORCECEFR		Pressuranga	Network	Fechado	04/02/05 11:06
983	CORCECEFR		Perdas de conexão/pacotes tanto pelo O.V.D quanto pelo Big Brother Ok agora	Network	Fechado	04/02/05 11:06
984	CORCECEFR		VLAN DEFAULT LINK OK, ocorrência fechada	Network	Fechado	04/02/05 11:13
985	CORCECEFR		IF ethernet8/17 Down <2> Capabilities: nIPRouter:nSNMPSupported:nRMON:nOSPF	Network	Fechado	04/02/05 13:09
986	TAMBACQUI		IF VIA Down <2> Capabilities: nNode:nSNMPSupported Root Cause: tambacqui tele	Network	Fechado	04/02/05 13:30
987	ARIANA		IF Intel(R) Down <2> Capabilities: nNode:nSNMPSupported Root Cause: ariana tele	Network	Fechado	04/02/05 13:31
988	LAMBARI		IF Realtek Down <2> Capabilities: nNode:nSNMPSupported Root Cause: lambari tele	Network	Fechado	04/02/05 14:14
989	LAMBARI		IF Realtek Down <2> Capabilities: nNode:nSNMPSupported Root Cause: lambari tele	Network	Fechado	04/02/05 14:26
990	LAMBARI		IF Realtek Down <2> Capabilities: nNode:nSNMPSupported Root Cause: lambari tele	Network	Fechado	04/02/05 14:37
991	LAMBARI		IF VIA Down <2> Capabilities: nNode:nSNMPSupported Root Cause: tambacqui tele	Network	Fechado	04/02/05 14:51
992	CORCECEFR		IF ethernet5/1 Down <2> Capabilities: nIPRouter:nSNMPSupported:nRMON:nOSPF	Network	Fechado	04/02/05 15:15
993	CORCECEFR		IF vs17 Down FAVORABLES Capabilities: nIPRouter:nSNMPSupported:nRMON:nOSPF	Network	Fechado	04/02/05 15:17
994	CORCECEFR		IF ethernet2/3 Down <2> Capabilities: nIPRouter:nSNMPSupported:nRMON:nOSPF	Network	Fechado	04/02/05 16:13
995	CORCECEFR		IF ethernet13/2 Down <2> Capabilities: nIPRouter:nSNMPSupported:nRMON:nOSPF	Network	Fechado	04/02/05 16:20
996	CORCECEFR		Rua Olímpica intervenção do usuário que liga/desliga o equipamento	Network	Fechado	04/02/05 16:34
997	ARIANA		IF 143.107.204.97 Down <2> Capabilities: nNode:nSNMPSupported Root Cause: ariana tele	Network	Fechado	04/02/05 17:05
998	CORCECEFR		IF AT110101 Down <2> Capabilities: nIPRouter:nSNMPSupported:nRMON:nFrameRe	Network	Fechado	04/02/05 17:11
999	CORCECEFR		IF ethernet13/1 Down <2> Capabilities: nIPRouter:nSNMPSupported:nRMON:nOSPF	Network	Fechado	04/02/05 17:39
900	CORCECEFR		IF ethernet13/1 Down <2> Capabilities: nIPRouter:nSNMPSupported:nRMON:nOSPF	Network	Fechado	04/02/05 17:53

Figura 8-5: Ferramenta *Service Desk* (*HPOpenview*) com incidentes registrados automaticamente.

É importante observar que no cenário de atendimento ao incidente descrito anteriormente, o volume de dados coletados era pequeno, uma vez que a implantação do modelo

proposto neste trabalho estava em uma fase inicial. Atualmente, com um enorme volume de dados coletados nos equipamentos que compõem o ambiente a ser protegido, torna-se impraticável uma análise e correlação manual desses dados para que se consiga, em tempo hábil, gerar informações que permitam ações emergenciais.

A Figura 8-5 apresenta parte dos 212 incidentes que foram registrados no dia 04/02/2005 e que poderiam conter dados relevantes para uma ação emergencial.

Isso reforça a proposta deste trabalho de modelar o sistema de segurança computacional com base na infra-estrutura de tomada de decisão dos Sistemas de Informação Gerenciais.

8.4 Cenário Atual com parte do Projeto Implementado

Com parte do modelo proposto neste trabalho implementado no Centro de Computação Eletrônica, é possível descrever o cenário atual da seguinte forma:

Nível Operacional

- Existência de um ponto único de contato
- Uma equipe de resposta aos incidentes de segurança computacional estabelecidas e executando as atividades prevista para um CSIRT;
- Existência de revezamento entre membros da equipe de segurança de forma que sempre haja uma pessoa com dedicação exclusiva ao tratamento de incidentes de segurança computacional;
- Disseminação de alertas de vulnerabilidade para toda a comunidade envolvida com gerenciamento de TIC na Universidade;
- Documentos formais contendo a definição de papéis e responsabilidades das pessoas envolvidas com o tratamento das questões de segurança computacional sendo desenvolvido;
- Existência de ações coordenadas de resposta aos incidentes de segurança computacional;
- Incidentes de segurança computacional sendo tratados de forma proativa a partir da implementação do módulo de Gerenciamento de Incidentes e Gerenciamento de problemas descrito no capítulo 6 deste trabalho;
- Incidentes de segurança computacional sendo recebidos, priorizados, escalonados;

- Utilização de uma ferramenta automatizada para controle do fluxo de trabalho para auxílio aos processos de gerenciamento incidentes e gerenciamento de problemas;
- Ferramentas de gerenciamento e coleta de dados implementadas e ajustadas para coleta de dados sobre segurança computacional;
- Data Warehouse para a composição de um sistema de informação sendo modelado;
- Objetivos de controle definidos no modelo COBIT e na norma ISO 17799 identificados para o nível operacional;

Nível Tático

- Estatísticas a respeito dos incidentes de segurança computacional gerados periodicamente e disponibilizados para toda a comunidade;
- Canal de comunicação e troca de experiências estabelecidos com Centros de Resposta a Incidentes nacionais (CAIS, CERT-BR etc) e Internacionais (AusCERT, FIRST etc). Inclusive, com o desenvolvimento de projetos em parceria;
- Análise de eventos relacionados com segurança computacional sendo analisados de forma proativa através da implementação do processo de gerência de comportamento proposto no Capítulo 6 deste trabalho;
- Estabelecimento de um programa de distribuição das responsabilidades de gerenciamento das questões de segurança computacional distribuídas para as unidades com atribuição formal de responsabilidades e estabelecimento de programas de treinamento;
- Utilização de ferramentas de gerenciamento de redes para coleta de informações relacionadas a segurança computacional para o nível tático;
- Utilização de ferramentas de testes de vulnerabilidades e penetração;

Nível Estratégico

- Existência de uma política de segurança desenvolvida com base nos controles definidos na ISO 17799 e definida formalmente;

- Conhecimento sobre a situação atual do ambiente e os riscos inerentes ao mesmo sendo divulgados para o conselho administrativo;
- Investimentos da área de Segurança da Informação sendo feitos com base em conhecimento acerca do ambiente a ser protegido;

A partir dessa análise do cenário atual é possível utilizar a ferramenta proposta pelo *Corporate Governance Task Force* [NSCP, 2004] para uma análise de *gaps* que represente a situação atual. Os gráficos a seguir foram desenvolvidos para apresentar uma análise comparativa entre o cenário atual no Centro de Computação Eletrônica da Universidade de São Paulo e o cenário encontrado em 2000. Os resultados obtidos e apresentados na Figura 8.6 podem ser comparados com os resultados obtidos na Figura 8.1.

A evolução deste cenário representa a contribuição deste trabalho após sua implementação parcial no Centro de Computação Eletrônica da Universidade de São Paulo. A área a ser preenchida nos gráficos apresentados na Figura 8.6 representa a evolução que pode ser alcançada quando todo o modelo proposto neste trabalho for implementado, colocado em prática e atingido o nível de maturidade condizente com as necessidades apontadas pela análise de risco desenvolvida para aquele Centro.

Figura 8-6: Análise de *Gaps* comparativo: Cenário em 2000 X Cenário em 2005

9 Conclusão

Neste trabalho apresentou-se um modelo para Governança da Segurança da Informação que possui 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 com as 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 do negócio, conduziu este trabalho a considerar as questões de Governança da Tecnologia da Informação e Comunicação.

Para o desenvolvimento do modelo de Governança da Segurança da informação desenvolvido neste trabalho, foram identificados e apresentados 13 requisitos mínimos. Esses requisitos foram mapeados numa estrutura matricial que contempla os níveis de decisão, a saber, operacional, tático e estratégico, e as dimensões que amparam cada um desses níveis de decisão, a saber, 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 Computacional e o Negócio da Organização.

O modelo apresentado considerou a utilização das melhores práticas dos modelos de apoio à Governança de TIC 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 da Segurança da Informação.

A partir da implementação de parte do modelo desenvolvido neste trabalho no Centro de Computação Eletrônica da Universidade de São Paulo, foi possível identificar algumas potencialidades, dos quais as seguintes ficaram mais evidentes:

- O modelo permite uma implementação modular e de forma gradual, com capacidade de atender necessidades específicas em qualquer célula da matriz apresentada;
- O modelo permite a melhoria contínua da qualidade dos controles, processos, pessoas e tecnologia;
- O modelo pode ser aplicado em organizações de qualquer tamanho, sendo possível a inserção de novos controles conforme as necessidades da organização;
- Componentes do modelo podem sofrer ajustes, serem substituídos, desenvolvidos ou adquiridos de terceiros em cada uma das células apresentadas.

9.1 Trabalhos Futuros

A seguir é relacionado um conjunto de propostas para motivar a continuidade de pesquisas relacionadas com este tema:

- Experimentar ferramentas de Análise de Risco para identificar as que possuem as maiores potencialidades para seleção dos objetivos de controle para o modelo desenvolvido;
- Identificar as técnicas de Extração de conhecimento que melhor se ajustam às necessidades do modelo;

- Relacionar detalhadamente cada um dos objetivos de controle do modelo COBIT com cada atividade dos processos descritos no modelo ITIL numa tentativa de evoluir o modelo para novos objetivos de controle e novos processos;
- Propor modelos de Banco de Dados que possam substituir o modelo de *Data Warehouse* para que a dimensão tecnológico seja de fácil implementação em pequenas organizações;
- Fazer simulações utilizando o modelo para evoluir a base de conhecimento;
- Utilizar Ontologias para padronização da base de conhecimentos;
- Definir planos de MOC (*Management of Change*) para cada uma das células do modelo desenvolvido para a criação de uma estratégia de minimização dos impactos a partir da implementação do modelo;

Anexo A

SiRI - UM SISTEMA PARA A GESTÃO DAS ATIVIDADES DE RESPOSTA A INCIDENTES EM EQUIPES DE SEGURANÇA COMPUTACIONAL

**Mauro Cesar Bernardes, Rafael Tavares, Stenio Firmino Pereira Filho, Maria Isabel
Teixeira Chagas, Alberto Camilli, Edson dos Santos Moreira**

Centro de Computação Eletrônica (CCE) - Universidade de São Paulo (USP)
Av. Prof. Luciano Gualberto, travessa 3 número 71 – Cidade Universitária
05508-900 – São Paulo – SP – Brasil

{mcesar,rafaelt,stenio,mit,camilli}@usp.br, edson@icmc.sc.usp.br

Resumo: Este artigo descreve um Sistema de apoio às atividades de Report a Incidentes de Segurança Computacional em um CSIRT (Computer Security Incident Response Team) de uma organização. Um CSIRT pode oferecer uma variedade de serviços, entretanto, um serviço eficaz de Resposta a Incidentes deve ser mandatório. O sistema aqui apresentado auxilia as organizações a reduzir os efeitos dos incidentes de segurança, fornecendo subsídios para reduzir o tempo de sua detecção e report e organização dos dados. Uma vez que o sistema fornece informações importantes para a prevenção de incidentes, espera-se que o CSIRT possa reduzir o tempo de reação e passar a exercer atividades pró-ativas de segurança.

1. Introdução

Com a crescente facilidade de se obter informações sobre quebras de segurança, o lançamento de modernas técnicas e sua conseqüente divulgação pela Internet, o número de tentativas de ataque e o sucesso dessas tentativas tem crescido de forma assustadora. Isso pode ser comprovado através de diversas pesquisas realizadas por órgãos especializados em segurança [CERT,2002][NBSO,2002]. Conseqüentemente, torna-se necessário o desenvolvimento constante de novas técnicas que possam prover segurança computacional.

No meio computacional, o termo segurança é usado com o significado de minimizar a vulnerabilidade de dados, informação, conhecimento e a infra-estrutura que os suporta. Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém [ISO, 1989].

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação (intencional ou não) de informações confidenciais por elementos não autorizados e a utilização não autorizada do computador ou de seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizada nos termos de uma política de segurança [SOARES, 1995]. Zorkle e Levit ainda acrescentam que a segurança depende de mais do que da integridade do software e mecanismos de proteção do sistema operacional em uso; ela também é dependente da própria configuração e

uso do software com base na política de segurança previamente definida [ZERKLE & LEVITT, 1996].

De encontro à necessidade de um tratamento rápido e efetivo às questões relativas a segurança computacional nas organizações, observa-se o enorme crescimento do número de equipes de resposta a incidentes de segurança (CSIRTs) [West-Brown, 2002][MANDIA, 2001][SCHULTZ, 2002].

Um *Computer Security Incident Response Team-CSIRT*, ou Grupo de Resposta a Incidentes de Segurança, é uma organização ou grupo responsável por receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança computacional, entre tantas outras atividades possíveis.

Normalmente, um CSIRT presta serviços para uma comunidade bem definida, que pode ser a entidade que o mantém, como uma empresa, um órgão governamental ou uma organização acadêmica. Um CSIRT também pode prestar serviços para uma comunidade maior, como um país, uma rede de pesquisa ou clientes que pagam por seus serviços.

O CSIRT pode ser um grupo formal ou um grupo "*ad hoc*". Um grupo formal tem no trabalho de resposta a incidentes a sua principal função. Um grupo "*ad hoc*" é reunido quando há um incidente de segurança em andamento ou para responder a um incidente quando necessário.

No momento de se criar um CSIRT, deve-se ter muito bem definido quais atividades o mesmo irá exercer. O CSIRT poderá oferecer uma série de atividades reativas e pró-ativas em relação ao conceito de segurança computacional. Entretanto, a atividade de Resposta a Incidente torna-se indispensável para que um grupo possa ser chamado de CSIRT.

Este artigo irá apresentar um sistema para auxílio nas atividades de Resposta a Incidentes e como o mesmo poderá ser utilizado para organizar os dados relativos a tais atividades e ainda, tornar-se um valioso recurso para extrair informações essenciais para que o CSIRT possa exercer atividades tidas como pró-ativas.

2. As atividades de um CSIRT

Em ambientes onde é freqüente a ocorrência de incidentes de segurança, torna-se vital a existência de um ponto de contato único e de procedimentos eficientes e eficazes de resposta a incidentes. Este ponto de contato único pode receber diversos nomes, sendo o *Computer Security Incident Response Team- CSIRT* o mais comumente empregado [WEST-BROWN, 2002][MANDIA, 2001] [SCHULTZ, 2002]. Em função do tamanho deste ambiente, as atividades podem ser exercidas por uma pessoa ou por um grupo.

Uma vez estabelecidos, muitos *CSIRTs* tem falhado atualmente por não terem claramente definidas suas atividades, os procedimentos para executar as mesmas e ainda, pela falta de comunicação e inter-relacionamento entre estas atividades. Outro ponto falho observado tem relação com a organização da grande quantidade de dados gerados pelos incidentes. Estes dados, quando bem trabalhados, fornecem informações essenciais para que se consiga incrementar o grau de segurança do ambiente a ser protegido.

2.1 O Serviço de Resposta a Incidentes

As atividades do serviço de resposta a incidentes podem ser organizadas em quatro funções: "Triagem", "Análise do Incidente", "Retorno ao reclamante (Feedback)" e "Divulgação dos resultados" [WEST-BROWN, 2002].

Estas quatro funções são totalmente inter-relacionadas, podendo ser representadas conforme a Figura 1.

2.1.1 Função de Triagem

A função de triagem fornece um ponto único de contato e é o local responsável por receber, ordenar, identificar os pontos envolvidos com o incidente, encaminhar o incidente para os pontos responsáveis ou para um grupo de especialistas, receber as respostas e divulgá-las. Esta função requer diversos canais de comunicação (e-mail, telefone, fax, etc). Outra importante atividade desta função é associar um identificador a cada incidente, de forma a estabelecer uma referência para o mesmo ao longo do tempo e através das demais funções do serviço de resposta a incidentes.

Figura 1: As principais funções do serviço de Resposta a Incidentes e suas relações

2.1.2 Função de análise do Incidente

Esta função fornece suporte aos pontos relacionados ao incidente. Estas atividades vão desde a divulgação de conhecimento adquirido com casos semelhantes ocorridos no CSIRT até o compartilhamento de informações recebidas de outras fontes.

2.1.3 Função de Divulgação dos Resultados

Esta função é responsável por tratar e divulgar os dados relativos ao incidente. Entre suas atribuições está o acompanhamento do ciclo de vida de cada incidente, cuidar para que o mesmo tenha um encerramento e que estas informações sejam encaminhadas ao reclamante.

Os dados recebidos nesta função, quando bem trabalhados, irão gerar informações vitais para a redefinição dos requisitos de controle da política de segurança em vigor na organização e, conseqüentemente, contribuir para a redução do número de incidentes.

2.1.4 Função de Feedback

A função de *feedback* fornece suporte para uma resposta a elementos que não estão diretamente relacionados a um incidente. Esta é uma função extremamente importante no momento de lidar com a mídia e ainda, para fornecer um mecanismo de segurança frente a exploração das técnicas de engenharia social.

3. O tratamento de um Incidente através do SiRI

O SiRI foi implementado com o objetivo de realizar todas as funções necessárias para o sucesso de um serviço de Resposta a Incidentes em um CSIRT.

Para a utilização do sistema o novo usuário (membro do CSIRT) deverá preencher o cadastro com informações sobre sua localização. Um *e-mail* com o pedido será enviado ao administrador do sistema para que o mesmo autorize a sua inclusão. Após a autorização do administrador, o novo usuário receberá um e-mail com um link para uma página onde deverá cadastrar sua senha de acesso.

Criados o usuário e a senha, o mesmo terá acesso às atividades de Resposta a Incidentes coordenadas pelo SiRI.

Os usuários envolvidos com a “Função de Triagem” serão os responsáveis por alimentar o sistema com novos incidentes. Estes incidentes são recebidos pelo CSIRT através das contas de e-mail que possuem endereços definidos conforme RFC 2142, os endereços *security@dominio*, *abuse@dominio*, *postmaster@dominio* [RFC 2142].

Ao cadastrar o incidente, o mesmo receberá uma identificação que irá acompanhá-lo durante todo o seu ciclo de vida no sistema. Esta identificação é composta por uma combinação sugestiva com o seguinte formato: *númeroserie-mês/ano*.

Após ser cadastrado no sistema, o incidente receberá o *status* de “análise”. Neste momento o sistema irá gerar um e-mail com a confirmação do recebimento do *report* ao reclamante. O incidente permanecerá com o *status* de análise até que sejam identificados o ponto de origem do mesmo e a pessoa (ou administrador) dentro da organização responsável pela máquina (IP) envolvida com o acidente. Uma vez identificado o responsável, o sistema irá enviar um e-mail ao mesmo com a notificação do incidente.

Uma vez enviada a notificação ao responsável, o sistema modificará o *status* do incidente para “administrador”. Este *status* indica que o sistema está esperando um posicionamento do administrador quanto ao tratamento do incidente.

Caso o administrador não forneça uma resposta ao incidente dentro de um prazo que foi definido no momento do cadastramento do incidente no sistema (com base em sua gravidade), o sistema modificará o *status* deste incidente para “crítico”.

Estando em estado crítico, o incidente merece uma intervenção por parte das pessoas envolvidas com a função de “análise do incidente” do CSIRT. Esta função poderá determinar que um novo e-mail seja enviado ao administrador cobrando um posicionamento sobre o incidente ou ainda, que seja estabelecido alguma outra forma de contato com o mesmo. No caso de *e-mail*, o mesmo poderá ser gerado automaticamente pelo sistema.

A figura 2 apresenta uma visão geral dos *status* dos incidentes no sistema SiRI. A partir dos diversos *links* desta página, pode-se facilmente buscar maiores informações sobre qualquer incidente. Estas informações incluem todos os *logs* obtidos até o momento, informações sobre todo o ciclo de vida do incidente, além de quaisquer informações necessárias para o relacionamento do mesmo com as pessoas/administradores envolvidos.

Figura 2: Uma visão geral dos *status* dos incidentes no sistema SiRI

Em qualquer momento durante as atividades descritas anteriormente, o usuário do sistema poderá agregar dados ao incidente. Estes dados irão gerar informações valiosas para o CSIRT sobre as atividades de Resposta a Incidentes.

A pessoa eleita pelo usuário do sistema no momento do cadastro do incidente, também poderá incluir informações sobre o mesmo por meio de uma senha recebida juntamente com a notificação do incidente. A partir desta senha de acesso o responsável também poderá acompanhar todo o ciclo de vida dos incidentes sob sua responsabilidade.

Apesar das funções apresentadas até o momento contribuírem significativamente para as atividades de Resposta a Incidentes, principalmente na minimização do tempo de resposta ao incidente, a maior potencialidade do sistema SiRI reside nas informações geradas pelo mesmo a partir dos dados de todos os incidentes.

Estas informações, sintetizadas por meio de diversos relatórios e gráficos, permitem ao CSIRT identificar pontos falhos no processo de gerenciamento de segurança computacional. A figura 2 apresenta uma das páginas de acesso às informações geradas pelo sistema.

Uma vez identificado os pontos falhos, o CSIRT poderá trabalhar de forma pró-ativa e não somente reativa. Com isso, procura-se minimizar a quantidade de ocorrências dos incidentes.

Figura 2: Um exemplo de página de acesso às diversas informações geradas pelo sistema SiRI

4. Plataformas de desenvolvimento

O sistema foi desenvolvido utilizando a linguagem PHP 4.3 e o Banco de Dados MySQL.

Apesar de atualmente o sistema estar em execução em uma máquina com o sistema operacional Solaris, o mesmo poderá ser executado em qualquer servidor executando a plataforma Unix ou Windows. O sistema poderá ser executado em qualquer hardware que suporte estas plataformas.

5. Conclusões

Ao contrário do gerenciamento das redes de computadores que, na maioria dos casos, apresentam ações cotidianas e estruturadas, o gerenciamento de um ambiente de segurança computacional apresenta ações aleatórias, não estruturadas e mutantes, de forma que qualquer decisão envolve um conhecimento especialista. Isso deve-se principalmente pela evolução constante nas formas de ataque e nos furos de segurança constantemente descobertos nos mais diversos softwares.

Dessa forma, o papel de um CSIRT e, mais especificamente, das atividades de resposta a incidentes torna-se essencial no cenário atual. Além disso, torna-se vital armazenar os dados envolvidos com as atividades de segurança e, principalmente, buscar formas de transformação desses dados em conhecimento.

Como uma ferramenta facilitadora das funções de resposta a incidentes, este artigo apresentou o sistema SiRI. Neste sistema, foi levada em consideração uma forma de minimizar o nível de incerteza que acompanha as ações no gerenciamento de resposta a incidentes de segurança computacional. Para isso, o uso de tecnologia da informação (e o conhecimento dela adquirido) foi considerado um elemento chave para o seu desenvolvimento.

Atualmente, além de contribuir muito para a minimização do tempo de resposta a incidentes de segurança, o sistema cuida de transformar os dados coletados de cada um dos incidentes e ainda, dos mais diversos elementos do ambiente, em informações e conhecimento necessários para o processo de tomada de decisão e a manutenção da política de segurança do

ambiente a ser protegido. Neste contexto, o aumento do grau de proteção de cada elemento de segurança, advindo de uma melhor configuração determinada pelo conhecimento adquirido através do sistema SiRI, passou a ter um impacto considerável no sucesso pela busca da segurança global do ambiente a ser protegido.

Uma vez que em ambientes complexos os dados existentes ou gerados irão ultrapassar em muito a capacidade dos analistas em realizar consultas e análise “ad-hoc”, o sistema provê uma ferramenta extremamente eficaz e eficiente para a solução deste problema.

6. Refererências Bibliográficas

CERT COORDINATION CENTER, CERT/CC Overview Incident and Vulnerability Trends. Carnegie Mellon University, 2000. Disponível on-line em: <http://www.cert.org>. Visitado em 23/10/2001.

MANDIA, K; PROSISE, C. Incident Response: Investigating Computer Crime. Osborne/McGraw-Hill, 2001.

NBSO: NIC BR Security Office. Estatísticas dos Incidentes Reportados ao NBSO. Documento disponível on-line em <http://www.nic.br/stats.html>. Visitado em 15/02/2002.

International Organization for Standardization / International Electrotechnical Committee. "Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture". International Standard 7498-2, 1989.

RFC 2142 - Crocker, D. "Mailbox Names for Common Services, Roles and Functions", Internet Mail Consortium, May 1997

SCHULTZ, E.E; SHUMWAY, R. A Strategic Guide to Handling System and Network Security Breaches. New Riders Publishing, 2002.

SOARES, L. F. G., LEMOS, G., COLCHER, S. Redes de Computadores: das LANs, MANs e WANs às redes ATM. 2. Edição. Rio de Janeiro: Campus, 1995. 704 p.

WEST-BROWN, M.J.; STIKVOORT, D.; KOSSAKOWSKI, K., Handbook for Computer Security Incident Response Team (CSIRTs). Carnegie Mellon University URL:<http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html>, 2002. Visitado em 18/01/2003.

ZERKLE, Dan; LEVITT, Karl. NetKuang - A Multi-Host Configuration Vulnerability Checker. Departament of Computer Science. University of California at Davis. Disponível on-line em: <http://seclabs.cs.ucdavis.edu/papers/zl96.ps>, visitado em 13/01/1999.

Anexo B

Este anexo apresenta os formulários extraídos da proposta de avaliação apresentada pelo *Corporate Governance Task Force* [NSCP, 2004] para uma análise de *gaps* para a Governança da Segurança da Informação em Instituições de Ensino Superior.

Section III: People		
This section assesses the organizational aspects of your information security program. It should be completed by the president, chancellor, chief executive officer, or a designee.		
Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4		
	Information Security Function/Organization	Score
3.1	Is there a person or organization that has information security as their primary duty, with responsibility for maintaining the security program and ensuring compliance?	
3.2	Do the leaders and staff of your information security organization have the necessary experience and qualifications?	
3.3	Does your information security function have the authority it needs to manage and ensure compliance with the information security program?	
3.4	Does your information security function have the resources it needs to manage and ensure compliance with the information security program?	
3.5	Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes and audits?	
3.6	Has specific responsibility been assigned for the execution of business continuity and disaster recovery plans (either within or outside the information security function)?	
3.7	Do you have an ongoing training program in place to build skills and competencies for information security for members of the information security function?	
3.8	Is someone in the information security function responsible for liaising with units to identify any new security requirements based on changes to operations?	
3.9	Does the information security function actively engage with other units (human resources, student affairs, legal counsel) to develop and enforce compliance with information security policies and practices?	
3.10	Does the information security function report regularly to institutional leaders and the governing board on the compliance of the institution to and the effectiveness of the information security program and policies?	
3.11	Are the senior officers of the institution ultimately responsible and accountable for the information security program, including approval of information security policies?	
3.12	Do the unit heads and senior managers have specific programs in place to	

	comply with information security policies and standards with the goal of ensuring the security of the information and systems that support the operations and assets under their control?	
3.13	Have you implemented an information security education and awareness program such that all administrators, faculty, staff, contractors, external providers, students, guests, and others know the information security policies that apply to them and understand their responsibilities?	
	TOTAL PEOPLE SCORE	

Section IV: Processes		
This section assesses the processes that should be part of an information security program. It should be completed by the president, chancellor, chief executive officer, or a designee.		
Scoring: <i>Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4</i>		
	Security Technology Strategy	Score
1	Does your institution have an official information security architecture, based on your risk management analysis and information security strategy?	
2	Is the security architecture updated periodically to take into account new needs and strategies as well as changing security threats?	
3	As the architecture evolves, is there a process to review existing systems and applications for compliance and for addressing cases of noncompliance?	
4	Have you instituted processes and procedures for involving the security personnel in evaluating and addressing any security impacts before the purchase or introduction of new systems?	
5	If a deployed system is found to be in noncompliance with your official architecture, is there a process and defined timeframe to bring it into compliance or to remove it from service, applications or business processes?	
6	Do you have a process to appropriately evaluate and classify the information and information assets that support the operations and assets under your control, to indicate the appropriate levels of information security?	
7	Are there specific, documented, security-related configuration settings for all systems and applications?	
8	Do you have a patch management strategy, policy, and procedures in place and responsibilities assigned for monitoring and promptly responding to patch releases, security bulletins, and vulnerabilities reports?	
Policy Development and Enforcement		
9	Are written information security policies consistent, easy to understand, and readily available to administrators, faculty, employees, students, contractors, and partners?	
10	Is there a method for communicating security policies to administrators, faculty, employees, students, contractors, and partners?	

11	Are consequences for noncompliance with corporate policies clearly communicated and enforced?	
12	Are there documented procedures for granting exceptions to policy?	
13	When policies are updated or new policies are developed, is an analysis conducted to determine the financial and resource implications of implementing the new policy?	
14	Do your security policies effectively address the risks identified in your risk analysis/risk assessments?	
15	Are relevant security policies included in all of your third-party contracts?	
16	Are information security issues considered in all important decisions within the organization?	
	Information Security Policies and Procedures	
	Based on your information security risk management strategy, do you have official written information security policies or procedures that address each of the following areas?	
17	Individual employee responsibilities for information security practices	
18	Acceptable use of computers, e-mail, Internet, and intranet	
19	Protection of organizational assets, including intellectual property	
20	Managing privacy issues, including breaches of personal information	
21	Identity management, including excursions or breaches of sensitive identity information	
22	Access control, authentication, and authorization practices and requirements	
23	Data classification, retention, and destruction	
24	Information sharing, including storing and transmitting institutional data on outside resources (ISPs, external networks, contractors' systems)	
25	Vulnerability management (patch management, antivirus software)	
26	Disaster recovery contingency planning (business continuity planning)	
27	Incident reporting and response	
28	Security compliance monitoring and enforcement	
29	Change management processes	
30	Physical security and personnel clearances or background checks	
31	Reporting security events to affected parties, including individuals, public, partners, law enforcement, and other security organizations as appropriate	
32	Prompt investigation and correction of the causes of security failures	
33	Data backups and secure off-site storage	
34	Secure disposal of data, old media, or printed materials that contains sensitive information	
	Physical Security	
	For your critical data centers, programming rooms, network operations centers, and other sensitive facilities or locations:	
35	Are multiple physical security measures in place to restrict forced or unauthorized entry?	
36	Is there a process for issuing keys, codes, and/or cards that require proper authorization and background checks for access to these sensitive	

	facilities?	
37	Is your critical hardware and wiring protected from power loss, tampering, failure, and environmental threats?	
Security Program Administration		
38	Do you maintain a current inventory of both the physical network elements (routers/switches, subnets, DNS, DHCP servers) and also the logical network assets (domain names, network addresses, access control lists)?	
39	Do you have a configuration-management process in place to ensure that changes to your critical systems are for valid business reasons and have received proper authorization?	
40	Does your organization periodically test and evaluate or audit your information security program, practices, controls, and techniques to ensure they are effectively implemented?	
41	Do you conduct a periodic independent evaluation or audit of your information security program and practices for each business unit?	
42	Does each periodic independent evaluation or audit test the effectiveness of information security policies, procedure, and practices of a representative subset of each business unit's information systems?	
43	Does each periodic independent evaluation or audit assess the compliance of each business unit with the requirements of a standard information security framework and related information security policies, standards, procedures, and guidelines?	
44	Are security-performance metrics instituted, evaluated, and reported?	
TOTAL PROCESSES SCORE		

Section V: Technology		
This section assesses the major technology topics related to information security. It should be completed by the president, chancellor, chief executive officer, or a designee with input from the chief security officer or chief information officer.		
Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4		
	Security Technology	Score
1	Are Internet-accessible servers protected by more than one security layer (firewalls, network IDS, host IDS, application IDS)?	
2	Are there controls between the layers of end-tier systems?	
3	Are your networks, systems, and applications periodically scanned to check for vulnerabilities as well as integrity of configurations?	
4	Do you constantly monitor in real time your networks, systems and applications for unauthorized access and anomalous behavior such as viruses, malicious code insertion, or break-in attempts?	
5	Are security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments automatically logged?	
6	Is sensitive data encrypted and associated encryption keys properly protected?	

7	Are there effective and reliable mechanisms in place to manage digital identities (accounts, keys, tokens) throughout their life cycle, from registration through termination?	
8	Do all of your systems and applications support and enforce automatic password change management or automatic expiration of passwords, as well as password complexity and reuse rules?	
9	Do you have an authentication system in place that applies higher levels of authentication to protect resources with higher levels of sensitivity?	
10	Do you have an authorization system that enforces time limits and defaults to minimum privileges?	
11	Do your systems and applications enforce session/user management practices including automatic timeouts, lockout on login failure, and revocation?	
12	Do you employ specific measures to prevent and detect rogue access for all of your wireless LANs?	
13	Do you employ specific measures to secure the servers that manage your network domain names and addresses (DNS and DHCP servers)?	
14	Do you employ specific measures to secure your remote access services (VPN and dial-up) as well as to secure remote access client systems?	
15	Is every desktop workstation and server protected with antivirus software?	
16	Is there an audit trail to verify that virus definitions files are updated frequently and systematically?	
17	Is every desktop workstation and server updated regularly with the latest operating system patches?	
18	Taking into account severity and urgency, are there mechanisms in place to report and respond to a variety of anomalies and security events?	
	TOTAL TECHNOLOGY SCORE	

10 Referências Bibliográficas

[ABNT, 2001]	ABNT. <i>Tecnologia da informação – Código de prática para a gestão da segurança da Informação</i> . NBR ISO/IEC 17799. 30/09/2001.
[ALBERTS et al, 2004]	ALBERTS, C.; DOROFEE, A.; KILLCRECE, G.; RUEFLE, R.; ZAJICEK, M. <i>Defining Incident Management Processes for CSIRTs: A Work in Progress</i> . CMU/SEI-2004-TR-015. Carnegie Mellon University, 2004, 164p. Disponível on-line em www.cert.org/archive/pdf/04tr015.pdf , visitado em 23/11/2004.
[ALLEN, 2004]	ALLEN, J. H. Building a Practical Framework for Enterprise-Wide Security Management. Secure IT Conference. Software Engineering Institute - Carnegie Mellon University. Pittsburgh. April 28, 2004. Disponível on-line em http://www.cert.org/archive/pdf/secureit_csm_allen_may0304.pdf , visitado em 10/01/2005.
[AMARAL, 1997]	AMARAL, A., <i>Desmistificando Definitivamente o Data Warehousing</i> . Revista Developers Magazine. ISSN 1413-9514, Brasil, Fevereiro, 1997, pp. 14-17.
[ANONYMOUS, 2000]	ANONYMOUS. <i>Maximum Linux Security</i> . Sams Publishing, 2000.
[AMBROSIO et al, 2000]	AMBROSIO, D.R.; BERNARDES, M.C.; PEREIRA FILHO, S.F. & MOREIRA, E.S. <i>Algoritmos Inteligentes Para Busca de Padrões na Detecção de Intrusão</i> . Anais do Simpósio de Segurança em Informática do CTA/ITA. Editor Clovis Torres Fernandes. São José dos Campos: CTA/ITA/IEC, outubro de 2000, pag. 19-2.
[AUDY & BRODBECK, 2003]	AUDY, J.L.N; BRODBECK, A.F. <i>Sistemas de Informação: planejamento e alinhamento estratégico nas organizações</i> . Porto Alegre: Bookman, 2003. ISBN 85-363-0192-9
[BELLOVIN&CHESWICK, 1994]	BELLOVIN, S.; CHESWICK, W. <i>Firewalls and Internet Security: Repelling the Wily Hacker</i> . Addison-Wesley. 1994.
[BERNARDES& MOREIRA, 1999a]	BERNARDES, M.C. <i>Avaliação do Uso de Agentes Móveis em Segurança Computacional</i> . Dissertação (Mestrado) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo. São Carlos, 1999. 112p.
[BERNARDES& MOREIRA, 1999b]	BERNARDES, M.C. & MOREIRA, E. S. <i>Avaliação do Uso de Agentes Móveis em Segurança Computacional</i> . Simpósio de Segurança em Informática. ITA/CTA. São José dos Campos, 14 a 16 de setembro de 1999. Anais do simpósio pag. 131-138.

[BERNARDES& MOREIRA, 2000a]	BERNARDES, M.C. & MOREIRA, E. S. <u>Implementação de um Sistema de Detecção de Intrusão Baseado em Agentes Móveis</u> . Anais do 5º Workshop de TMN/18º Simpósio Brasileiro de Redes de Computadores, 25 de maio de 2000. Editado por Carlos Becker Westphall (UFSC), 2000, pag. 13-23.
[BERNARDES et al, 2003]	BERNARDES, M.C.;TAVARES, R.; PEREIRA FILHO, S.F.; CHAGAS, M.I.T.;CAMILLI,A.;MOREIRA.E.S. <u>SiRI- Uma sistema para a gestão das atividades de Resposta a Incidentes em Equipes de Segurança Computacional</u> . Anais do 21º Simpósio Brasileiro de Redes de Computadores, Natal, 19 a 23 de maio de 2003. Editores Thaís Vasconcelos Batista [et al.], Natal, RN: UFRN/DIMAp:UNP, 2003. pag. 941 a 947.
[BERNARDES& MOREIRA, 2000b]	BERNARDES, M.C & MOREIRA, E. S. <u>A Proposal for Intrusion Detection System Based on Mobile Agents</u> . Proceedings of Fifth Int Symposium on Parallel and Distributed Engineering, eds Nixon and Ritchie, pub. IEEE CS Press, Limerick, June/2000.
[BERNARDES& MOREIRA. 2000c]	BERNARDES, M.C.& MOREIRA, E. S. <u>An Architecture for an Intrusion Detection System Based on Mobile Agents</u> . I Simposion Internacional de Sistemas Distribuidos Avanzados – SISDA’2000, Guadalajara, Jalisco, México, março 2000. ISBN: 970.692.045-5.
[BEUREN, 1998]	BEUREN, I.M. <u>Gerenciamento de Informação</u> . São Paulo: Editora Atlas, 1998.
[BIO, 1994]	BIO, S.R. <u>Sistemas de Informação: um enfoque gerencial</u> . São Paulo: Atlas, 1994.
[BONIFÁCIO, 1998]	BONIFÁCIO Jr., J. M. <u>Sistemas de Segurança Distribuído: Integração de Firewalls com Sistemas de Detecção de Intrusão</u> . São Carlos, 1998. Tese (Mestrado) - Instituto de Ciências Matemáticas e de Computação de São Carlos, Universidade de São Paulo.
[BONIFÁCIO Jr. et al. 1998a]	BONIFÁCIO Jr., J. M.; CANSIAN, A.M.; CARVALHO, A.C.P.L; MOREIRA, E.S. <u>Neural Networks Applied in Intrusion Detection Systems</u> . In: Proceedings of the IEEE IJCNN '98 International Joint Conference on Neural Networks, Anchorage, Alaska, Maio 1998.
[BONIFÁCIO Jr. et al. 1998b]	BONIFÁCIO Jr., J. M.; CANSIAN, A.M.; CARVALHO, A.C.P.L; MOREIRA, E.S. <u>Um Ambiente de Segurança Distribuído para a Integração de Firewalls com Sistemas de Detecção de Intrusão</u> . In: XVI Brazilian Symposium on Computer Networks, SBRC'98. Rio de Janeiro, 1998.
[BONIFÁCIO Jr et al, 1998]	BONIFÁCIO JR., J.M.; MOREIRA, E.S. CANSIAN, A..M.; CARVALHO, A.C.P.L; <u>An adaptative Intrusion Detection System Using Neural Networks</u> . In: SEC'98, VIENA, AUSTRIA, 1998.

- [BRANDAO et al, 2004] BRANDAO, A.J.S.; MARTIMIANO, L.A.F; MOREIRA, E.S. *O Uso de Ontologias em Alertas de Vulnerabilidade*. XXII Simpósio Brasileiro de Redes de Computadores. IV Workshop em Segurança de Sistemas Computacionais. Gramado-RS, maio de 2004. P.75-86.
- [BROOKS, 1997] BROOKS, P.L. *Visualizando os Dados*. Revista DBMS, n 5 v1, Setembro, 1997, pp. 25-43.
- [BROWNLEE, 1998] BROWNLEE, N. & GUTTMAN, E. *Expectations for Computer Security Incident Response (RFC 2350)*. Disponível on-line em <http://www.ietf.org/rfc/rfc2350.txt?number=2350>. Visitado em 10/01/2005.
- [BSA, 2003] BUSINESS SOFTWARE ALLIANCE. *Information Security Governance: Toward a Framework for Action*. Disponível on-line em <http://www.bsa.org>. Visitado em 12/12/2004.
- [CAMPOS et al., 1999] CAMPOS, M.L. et al. *Data Warehouse*. Disponível on-line em <http://genesis.nce.ufrj.br/dataware/tutorial>. Visitado em 02/02/2000.
- [CANSIAN, et al. 1997a] CANSIAN, A.M.; MOREIRA, E.M.; CARVALHO, A.C.P.L.; BONIFÁCIO Jr., J.M. *Network Intrusion Detection Using Neural Networks*. In: Proceedings of International Conference on Computational Intelligence and Multimedia Applications, ICCIMA'97, Gold Coast, Australia, p.276-280, Fevereiro 1997.
- [CANSIAN et al. 1997b] CANSIAN, A.M.; MOREIRA, E.M.; MOURO, R.B.; MORISHITA, F.T.; CARVALHO, A.C.P.L.; *An Adaptative System for Detecting Intrusion in Networks*. In: Proceedings of the III International Congress on Information Engineering, Buenos Aires, Argentina, p.96-105, Abril 1997.
- [CANSIAN et al. 1997c] CANSIAN, A.M.; MOREIRA, E.M.; CARVALHO, A.C.P.L.; BONIFÁCIO Jr., J.M. *Um Modelo Adaptativo para Detecção de Comportamento Suspeito em Redes de Computadores*. In: Proceedings of the XV Brazilian Symposium on Computer Networks, SBRC'97, p. 51-60, São Carlos, Maio 1997.
- [CANSIAN 1997] CANSIAN, A. M. *Desenvolvimento de um sistema adaptativo de detecção de intrusos em redes de computadores*. São Carlos, 1997. 153p. Tese (Doutorado) – Instituto de Física de São Carlos, Universidade de São Paulo.
- [CARBONELL, 1987] CARBONELL, J.G& LANGLEY, P. *Machine Learning*. Encyclopedia of Artificial Intelligence, Ed. John Wiley & Sons, USA, 1987, pp. 464-488.
- [CARUSO, 2003] CARUSO, J.B. *Information Technology Security: Governance, Strategy and Practice in Higher Education*. EDUCASE Center for Applied Research, September, 2003. Disponível on-line em <http://www.educause.edu/ecar/>. Visitado em 16/03/2005.

[CATELLI, 1999]	CATELLI, Armando. <u>Controladoria: uma abordagem da gestão econômica-GECON</u> . São Paulo: Atlas, 1999.
[CERT, 2000]	CERT COORDINATION CENTER, <u>CERT/CC Overview Incident and Vulnerability Trends</u> . Carnegie Mellon University, 2000. Disponível on-line em: http://www.cert.org . Visitado em 23/10/2001.
[CERT, 2001a]	CERT COORDINATION CENTER, <u>CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL</u> . Disponível on-line em: http://www.cert.org/advisories/CA-2001-19.html . Visitado em 19/07/2001
[CERT, 2001b]	CERT COORDINATION CENTER, <u>CERT Advisory CA-2001-22 W32/Sircam Malicious Code</u> . Disponível on-line em: http://www.cert.org/advisories/CA-2001-22.html . Visitado em 25/07/2001
[CERT, 2001c]	CERT COORDINATION CENTER, <u>CERT Incident Note IN-2001-09 - "Code Red II: " Another Worm Exploiting Buffer Overflow In IIS Indexing Service DLL</u> . Disponível on-line em: http://www.cert.org/incident_notes/IN-2001-09.html . Visitado em 06/08/2001
[CERT, 2001d]	CERT COORDINATION CENTER, <u>CERT Advisory CA-2001-26 Nimda Worm</u> . Disponível on-line em: http://www.cert.org/advisories/CA-2001-26.html . Visitado em 18/09/2001.
[CERT, 2005a]	CERT COORDINATION CENTER, <u>CERT/CC Statistics 1988-2005</u> . Documento disponível on-line em http://www.cert.org/stats/cert_stats.html . Visitado em 12/02/2005.
[CERT, 2005b]	CERT COORDINATION CENTER, <u>Governing for Enterprise Security</u> . (2005) Disponível on-line em http://www.cert.org/governance/ges.html . Visitado em 01/03/2005
[CGTFR, 2004]	CORPORATE GOVERNANCE TASK FORCE REPORT. <u>Information Security Governance: A Call to Action</u> . April, 2004. Disponível on-line em: http://www.cyberpartnership.org/InfoSecGov4_04.pdf . Visitado em 02/02/2005.
[CHEN et al., 1997]	CHEN, M.; HAN, J. & YU, Philip S. <u>Data Mining: An Overview from Database Perspective</u> . 1997. Disponível on-line em: http://master.cpe.ku.ac.th/mcpe/204562/survey97.pdf . Visitado em março de 2002.
[CHAPMAN, 1992]	CHAPMAN, D. B. Network (In) Security Through IP Packet Filtering. In: <u>Proceedings of USENIX Security Symposium III</u> , p.63-76. Setembro 1992. Disponível on-line em: http://www.cert.lu/security/documents.html . Visitado em 17/11/1998.

- [CICILIANI, 1994] CICILIANI, R. Desenvolvimento de um Agente SNMP para Plataformas Rodando DOS. São Carlos, 1994. 107p. Dissertação (Mestrado) – Instituto de Ciências Matemáticas de São Carlos, Universidade de São Paulo.
- [COSTA, 2000] COSTA, G.M. Tecnologia de Data Warehousing e Gestão Empresarial: Uma contribuição ao estudo da utilização da tecnologia de Data Warehousing. Dissertação (Mestrado). São Paulo: FEA/USP, 2000.
- [CUSTODIO, 1981] CUSTODIO, I. Avaliação de Sistemas de Informação. Dissertação (mestrado). FEA/USP, 1981.
- [DAVIS, 1982] DAVIS, G.B. Strategies for information requirements determination. IBM System Journal, v.21,n1, p.4-30, 1982.
- [DEGHI, 1999] DEGHI, Gilmar Jonas. Contribuição ao estudo de ambientes de desenvolvimento de sistemas: uma abordagem com orientação a objeto. Dissertação (Mestrado) – Faculdade de Economia, Administração e Contabilidade da USP. São Paulo: FEA/USP, 1999.
- [EIN-DOR&SEVGEV, 1978] EIN-DOR, P. & SEVGEV, E. Administração de sistemas de Informação. Traduzido por Marina Cunha Brenner. Rio de Janeiro: Campus, 1978.
- [ENTRUST, 2004] ENTRUST. Information Security Governance (ISG): An Essential Element of Corporate Governance. April, 2004. Disponível on-line em: <http://www.entrust.com/governance/>. Visitado em 16/03/2005.
- [FAYYAD, 1996a] FAYYAD, U.M., PIATESKY-SHAPIRO, G & SMYTH, P., Advanced in Knowledge and Data Mining. AAAI/MIT Press, 1996.
- [FAYYAD, 1996b] FAYYAD, U.M., PIATESKY-SHAPIRO, G & SMYTH, P., The KDD process for Extracting Useful Knowledge from Volumes of Data. Communications of the ACM, v. 39, n 11, November 1996, pp. 27-34.
- [FAYYAD, 1996c] FAYYAD, U.M. Data Mining and Knowledge Discovery: Making Sense Out of Data. IEEE EXPERT, October, 1996, pp. 20-25.
- [FELIX, 1998] FELIX, L.CM. Data Mining no Processode Extração de Conhecimentode Base de Dados. Dissertação (mestrado). ICMC/USP, São Carlos, 1998
- [FRASER, 1997] Fraser, B., ed. Site Security Handbook (RFC 2196). Network Working Group (1997). Disponível on-line em: <http://www.ietf.org/rfc/rfc2196.txt>. Visitado em 14/01/2005.
- [GIL, 1995] GIL, A. L. Sistemas de Informações contábil/financeira. São Paulo: Atlas, 1995.
- [GLYMOUR, 1997] GLYMOUR, C.; MADIGAN, D.; & PADHRAIC, S. Statistical Themes and Lessons for Data Mining. Data Mining an Knowledge Discovery v. 1, Kluwer Academic Publishers, London U.K., 1997, pp. 11-28.

[CGTRF, 2004]	CORPORATE GOVERNANCE TASK FORCE REPORT. <i>Information Security Governance: A Call to Action</i> . April, 2004. Disponível on-line em: www.cyberpartnership.org/InfoSecGov4_04.pdf . Visitado em 15/11/2004.
[GUERREIRO, 1989]	GUERREIRO, R. <u><i>Modelo conceitual de sistema de informação de gestão econômica: uma contribuição à teoria da comunicação da contabilidade</i></u> . Tese. São Paulo: FEA/USP, 1989.
[HORNGREN et al, 1996]	HORNGREN, C.T.; HARRISON Jr, W.T.;ROBINSON, M.A. <i>Accounting</i> .3ª. ed. New Jersey: Prentice Hall, 1996.
[HIROSE, 2000]	HIROSE, C.H. <u><i>Projeto de um Sistema de Monitoramento de Ambientes de Intranet Usando DataWarehousing</i></u> . São Carlos, 2000, 75 p. Dissertação (Mestrado) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.
[INMON, 1997]	INMON, W.H. <i>Como construir o Datawarehouse</i> . Editora Campus, Rio de Janeiro, 1997.
[ITGI, 2000]	THE IT GOVERNANCE INSTITUTE. <i>COBIT: Control Objectives for information and related Technology</i> . Printed in the United States of America, 2000. ISBN: 1-893209-13-X.
[ITGI, 2001]	THE IT GOVERNANCE INSTITUTE. <i>Information Security Governance: Guidance for Boards of Directors and Executive Management</i> . 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 02/02/2005.
[IIA, 2001]	THE INSTITUTE OF INTERNAL AUDITORS. <i>Information Security Governance: What Directors Need to Know</i> . (2001). The Critical Infrastructure Assurance Project. ISBN 0-89413-457-4. Disponível on-line em www.theiia.org/eSAC/pdf/ISG_1215.pdf . Visitado em 14/01/2005.
[ISO, 2000]	International Organization for Standardization / International Eletrotechnical Committee. <i>Information technology- Code of practice for information security management. Reference number ISO/IEC 17799:2000(E)</i> .
[ISS, 2001]	Internet Security Systems (ISS). <i>Computer Security Incident Response Planning: Preparing for the Inevitable</i> . (2001) Disponível on-line em http://documents.iss.net/whitepapers/csirplanning.pdf . Visitado em 05/01/2005.

- [KILLCRECE et al, 2003] KILLCRECE, G.; KOSSAKOWSKI, K.P.; RUEFLE, R.; ZAJICEK, M. *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*, Carnegie Mellon University, CMU/SEI-2003-TR-001. ESC-TR-2003-001, October 2003. Networked Systems Survivability Program. 291p. Disponível on-line em <http://www.cert.org/archive/pdf/03tr001.pdf>, visitado em 23/11/2004.
- [KRUSE, 2002] Kruse, Warren G. II & Heiser, Jay G. *Computer Forensics: Incident Response Essentials*. Reading, MA: Addison-Wesley, 2002.
- [LAUDON & LAUDON, 2004] LAUDON, k. c.; LAUDON, J.P. *Essentials of Management Information Systems: Managing the Digital Firm*. sixth Edition. Prentice-Hall, Inc. 2004. ISBN 85-87918-39-7
- [LIEIRA, 1995] LIEIRA, J. F. *Utilização de Áudio e Vídeo em Sistemas Gerenciadores de Redes de Computadores*. São Carlos, 1995. 111p. Dissertação (Mestrado) – Instituto de Ciências Matemáticas de São Carlos, Universidade de São Paulo.
- [LIEIRA & MOREIRA, 1997] LIEIRA, J. & MOREIRA, E.S. *Utilização de Som e Imagem em Sistemas de Gerenciamento de Redes de Computadores*. In: Congresso de Informática e Telecomunicações do Mato Grosso. Anais. Cuiabá, 1997. v. II. p. 119-133.
- [LUCAS, 1997] LUCAS Jr., H.C. *Information Technology for Management*. Sixth Edition, International Editions, McGrawHill, 1997.
- [MANDIA, 2001] MANDIA, K; PROSISE, C. *Incident Response: Investigating Computer Crime*. Osborne/McGraw-Hill, 2001.
- [MANNILA, 1997] MANNILA, H. *Methods and Problems in Data Mining*. In Proc. International Conference on Database Theory. Ed. Springer-Verlag, Delphi, Greece, 1997.
- [MARTIMIANO, 2004] MARTIMIANO, L. A. F., Brandão, A. J. S., Moreira, E. S.; *Towards a security network incident ontology to ease the security knowledge management*. I2TS'2004 - 3rd International Information and Telecommunication Technologies Symposium. UFSCar. São Carlos-SP. Dec. 2004. pp. 88-96.
- [MARTIMIANO, 2005] Martimiano, L. A. F., Moreira, E. S.; *An OWL-based Security Incident Ontology*. *Protege Conference 2005*, Madrid, Spain. July 2005 (to be presented)
- [MILAGRES, 2004] MILAGRES, F.G. *Uso de Informações de Contexto em Segurança Computacional*. São Carlos, 2004. 101p. Dissertação (Mestrado) – Instituto de Ciências Matemáticas de São Carlos, Universidade de São Paulo.
- [MIRANDA, 1992] MIRANDA, O.M.Z. *A implementação da Tecnologia de Informação em um hospital – um estudo de caso*. Dissertação (Mestrado em Administração). São Paulo: FEA/USP, 1992.

- [MORISHITA, 1997] MORISHITA, F. T. *Uma Avaliação Evolutiva dos Protocolos de Gerenciamento da Internet: SNMPv1, SNMPv2 e SNMPv3*. São Carlos, 1997. 68p. Dissertação (Mestrado) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.
- [MOURO, 1997] MOURO, R. B. *Uma Arquitetura Operacional Extensível para Ferramentas de Gerenciamento de Redes*. São Carlos, 1997. 60p. Dissertação (Mestrado) – Instituto de Ciências Matemáticas de São Carlos, Universidade de São Paulo.
- [MOURO, MORISHITA & MOREIRA 1997] MOURO, R. B.; MORISHITA, F. T.; MOREIRA, E. S. *NetTracker :Uma Arquitetura Operacional Extensível Para Ferramentas de Gerenciamento de Redes*. São Carlos, 1997. 15º Simpósio Brasileiro de Redes de Computadores. p164-174. 1997.
- [MORAES, 1995] MORAES, S. *Voz em Sistemas Computacionais: Projeto e Implementação de Módulos de Processamento de Voz em Gerenciamento de Redes*. São Carlos, 1995. 103p. Dissertação (Mestrado) – Instituto de Ciências Matemáticas de São Carlos, Universidade de São Paulo.
- [MURDICK & ROSS, 1975] MURDICK, R.G. & ROSS, J. E. *MIS in action*. ST. Paul, West, 1975.
- [NAVY, 1996] Department of the Navy. *Computer Incident Response Guidebook*, Module 19 (NAVSO P-5239-19) (1996).. Disponível on-line em: <http://www.nswc.navy.mil/ISSEC/Guidance/P5239-19.html>. Visitado em 25/01/2005.
- [NBSO, 2005] NBSO: NIC BR Security Office. *Estatísticas dos Incidentes Reportados ao NBSO 1999-2005*. Documento disponível on-line em <http://www.nic.br/stats.html>. Visitado em 12/02/2005.
- [NCSP, 2004] NATIONAL CYBER SECURITY PARTNERSHIP. *Information Security Governance Assessment Tool for Higher Education*. 2004. Disponível on-line em: <http://www.cyberpartnership.org>. Visitado em 15/03/2005.
- [ODA, 1994] ODA, C. S. *Desenvolvimento de um Sistema Monitor Gráfico Baseado em Protocolo de Gerenciamento SNMP*. São Carlos, 1994. 111p. Dissertação (Mestrado) – Instituto de Ciências Matemáticas de São Carlos, Universidade de São Paulo.
- [ODA & MOREIRA, 1995] ODA, C.S., MOREIRA, E.S. *Representação Dinâmica de Objetos em Ambientes de Gerenciamento de Redes de Computadores*. In: Simpósio Brasileiro de Redes de Computadores. Anais: Belo Horizonte, MG, 1995.
- [OGC, 2000] Office of Government Commerce (OGC). *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, 2001a]	Office of Government Commerce (OGC). <i>ITIL: The Key to Managing IT Services – Best Practice for Service Delivery</i> . Printed in the United Kingdom for the Stationery Office, 2001. ISBN0 11 330017 4.
[OGC, 2001b]	Office of Government Commerce (OGC). <i>ITIL: The Key to Managing IT Services – Best Practice for Security Management</i> . Printed in the United Kingdom for the Stationery Office, 2001. ISBN0 11 330014 X.
[OLIVEIRA, 1997]	OLIVEIRA, Djalma P. R. <i>Sistemas. Organização & Métodos</i> . 8ª edição. São Paulo, Editora Atlas, 1997.
[OLIVEIRA, 1998]	OLIVEIRA, Djalma P. R. <i>Sistemas de Informações Gerenciais</i> . 5ª edição. São Paulo: Editora Atlas, 1998.
[PAULK et al, 1993]	PAULK, M.C.; CURTIS, B; CHRISSIS, M.B.;WEBER, C.V. <i>Capability Maturity Model for Software, version 1.1</i> . Technical Report, Carnegie Mellon Software Engineering Institute, CMU/SEI-93-TR-024, February 1993. Disponível on-line em: http://www.sei.cmu.edu/cmm/ . Visitado em 12/01/2005.
[PEREIRA FILHO, 2000]	PEREIRA FILHO, S.F. <i>Análise Comparativa de Ambientes Servidores de Agentes Móveis</i> . São Carlos, 2001. Dissertação de Mestrado. Instituto de Ciências Matemáticas e de Computação de São Carlos, Universidade de São Paulo.
[REAMI, 1998]	REAMI, E. R. <i>Especificação e Prototipagem de um Ambiente de Gerenciamento de Segurança Apoiado por Agentes Móveis</i> . São Carlos, 1998, 82p., Dissertação (Mestrado) – Instituto de Ciências Matemáticas de Computação de São Carlos, Universidade de São Paulo.
[REZENDE, 1998]	REZENDE, S.O.; OLIVEIRA, R.B.T.; FELIX, L.C.M. & ROCHA, C.A.J. <i>Visualization for Knowledge Discovery in Database</i> . In Proc. of International Conference on Data Mining, Rio de Janeiro, Brazil, Setember, 1998.
[RUDD, 2004]	RUDD, Colin. <i>An Introductory Overview of ITIL</i> . Publicado por iTSMF Ltd, Webbs Court, United Kingdom, 2004. Version 1.0a. Disponível on-line em: http://www.itsmf.com/publications/ITIL/Overview.pdf . Visitado em 13/03/2005.
[RUSSO&SCHOEMAKER, 1993]	RUSSO,J.E. & SHOEMAKER, P.J.H. <i>Tomada de Decisões-Armadilhas</i> . São Paulo: Saraiva, 1993.
[SANS, 2003]	The SANS Institute. <i>Computer Security Incident Handling Step-by-Step</i> . The SANS Institute, October 2003.
[SANTOS, 1998]	SANTOS, A.A. <i>Informática na Empresa</i> . Editora Atlas, 1998.

[SHULTS & SHUMWAY, 2002]	SCHULTZ, E.E; SHUMWAY, R. A Strategic Guide to Handling System and Network Security Breaches. New Riders Publishing, 2002.
[SHULTS, 1990]	SCHULTZ , Eugene; BROWN, David S.; & LONGSTAFF, Thomas A. <i>Responding to Computer Security Incidents</i> . (1990). Disponível on-line em ftp://ftp.cert.dfn.de/pub/docs/csir/ihg.txt.gz .
[SHIREY, 2000]	SHIREY, R. <i>Internet Security Glossary (RFC 2828)</i> . Disponível on-line em http://www.ietf.org/rfc/rfc2828.txt (2000). Visitado em 25/01/2005.
[SIMCSIK, 1993]	SIMKCSIK, Tibor. <i>O.M.I.S – Informação e Sistemas</i> – Vol. II. São Paulo, Makron Books, 1993.
[SOARES, 1995]	SOARES, L. F. G., LEMOS, G., COLCHER, S. <i>Redes de Computadores: das LANs, MANs e WANs às redes ATM</i> . 2. Edição. Rio de Janeiro: Campus, 1995. 704 p.
[SOKOL, 2000]	Sokol, Marc S. & Curry, David A. <i>Security Architecture and Incident Management for E-business</i> . Internet Security Systems (whitepaper), 2000.
[STAIR, 1996]	STAIR, R.M. <i>Principles of Information System – A managerial approach</i> . Second Edition, Boyd & Fraser, 1996.
[SYMANTEC, 2001]	Symantec Corp. <i>Advance Planning for Incident Response and Forensics</i> . (2001). Disponível on-line em http://enterprisecsecurity.symantec.com/SecurityServices/content.cfm?ArticleID=1557 . Visitado em 15/12/2004.
[TAVARES&MOREIRA, 2001]	TAVARES, D.M .& MOREIRA, E.S. <i>Avaliação de Técnicas de Captura para Sistemas Detectores de Intrusão</i> . Anais do Simpósio Segurança em Informática. Editor Clóvis Torres Fernandes. São José dos Campos: CTA/ITA/IEC, 2001.
[TACHIZAWA, 1989]	TACHIZAWA, E. T. <i>Um enfoque sistêmico ao uso da informação no apoio às decisões</i> . Dissertação (mestrado)
[TANLER, 1997]	TANLER, R. <i>The Intranet Data Warehouse</i> . John Wiley & Sons, 1997.
[van GREMBERGEN, 2003]	VAN GREMBERGEN, Wim. <i>Strategies for Information Technology Governance</i> . Idea Group Publishing, 2003. ISBN 1-591140-140-2.

[van WYK, 2001]	van WYK, Kenneth R. & FORNO, Richard. <i>Incident Response</i> . Sebastopol, CA: O'Reilly & Associates, Inc., 2001.
[VERMONT, 2001]	State of Vermont. <i>Incident Response Procedure</i> . (2001). Disponível on-line em http://www.dii.state.vt.us/Home/pdf/sov_intrusion_procedures.pdf
[WACK&CARNAHAN, 1994]	WACK, J. P.; CARNAHAN, L. Keeping Your Site Comfortably <u>Secure: An Introduction to Internet Firewalls</u> . In: National Institute of Standards and Technology Publication. 1994. WWW: http://www.raptor.com/lib/index.html
[WEILL&ROSS, 2004]	WEILL, Peter; Ross, Jeanne W. <i>IT Governance: how top performers manage IT decision rights for superior results</i> . Harvard Business School Publishing, 2004. ISBN 1-59139-253-5.
[WEST-BROWN et al, 1998]	WEST-BROWN, M.J.; STIKVOORT, D.; KOSSAKOWSKI, K., <u>Handbook for Computer Security Incident Response Team (CSIRTs)</u> . Carnegie Mellon University URL: http://www.sci.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html , 1998. Visitado em 18/01/2003.
[ZERKLE & LEVITT, 1996]	ZERKLE, Dan; LEVITT, Karl. <u>NetKuang - A Multi-Host Configuration Vulnerability Checker</u> . Departament of Computer Science. University of California at Davis. Disponível on-line em: http://seclabs.cs.ucdavis.edu/papers/zl96.ps , visitado em 13/01/1999.