BRENO MINUCCI LESSA
brenolessa@bol.com.br

Gestão Estratégica da Segurança da Informação

Belo Horizonte
2004

BRENO MINUCCI LESSA

Gestão Estratégica da Segurança da Informação

Monografia apresentada ao Programa do curso de Pós-Graduação *latu-sensu* em Gerência de Tecnologia da Informação, da Universidade Fumec, como requisito parcial à obtenção do título de Especialista em Gerência de Tecnologia da Informação, sob a orientação do Professor Osvaldo Manoel Corrêa.

Belo Horizonte

2004

À minha família, pois deu-me ânimo nos momentos difíceis e solitários da confecção desta obra.

Agradeço ao meu orientador Professor Osvaldo Manoel Corrêa, que garantiu a qualidade deste trabalho;

Agradeço à Universidade Fumec, que me garantiu subsídios para pesquisa e dissertação.

Agradeço aos meus mestres da pós-graduação por construírem minha ainda inacabada visão da Gerência de Tecnologia da Informação;

Agradeço aos meus colegas da pós-graduação, que me apresentaram ao longo do curso outras formas de conhecimento;

Agradeço ao Wagner, diretor-superintendente da Belgo Mineira Sistemas, pelos primeiros e valiosos comentários ainda na fase do projeto da monografia;

Agradeço à BMS, especialmente ao Fernando Sampaio, por garantir uma parte dos recursos financeiros empregados no curso;

Agradeço aos demais colegas de trabalho, que me ajudaram bastante na compreensão de estratégias;

Agradeço ao meu pai, minha mãe e minhas irmãs pela força indescritível fornecida no período de confecção;

Agradeço aos meus tios Binho e Wilma que com seus olhares letrados retificaram minha escrita; e

Agradeço à Joana que, com seu conhecimento artístico (entre outros incontáveis), proveu o tratamento das imagens apresentadas.

Sinopse

Este trabalho propõe-se demonstrar que a gestão de segurança de informação deve ocorrer primeiramente no nível estratégico da corporação, visto quão importante e abrangente é o assunto para a organização, baseado nas formas de proteção da informação utilizadas atualmente.

Resumo

A dependência da informação para as empresas vem crescendo nos últimos anos. A competitividade aumenta o valor dessa informação no mundo globalizado. A preocupação com a segurança torna-se indispensável. Aplicar corretamente a segurança corporativa constitui-se em um diferencial competitivo. Conforme poderá ser verificada, a gestão da segurança da informação no nível estratégico é um fator essencial para que se possa, de forma integral, garantir este importante ativo para a organização.

Abstract

The companies' dependence on valuable information has been increasing for the past few years. The competitiveness of the market in the globalizing world increases the value of this information. The concern with corporation security becomes indispensable. To apply the corporative security correctly is a competitive advantage. As specified in this study, information security management in the strategic level is essential for the security of the companies' assets.

Sumário

1 INTRODUÇÃO

Nas últimas décadas, a informação vem se tornando cada vez mais abundante e necessária a qualquer corporação. Na década de 80 vieram os computadores pessoais ressaltando a facilidade de se desenvolver sistemas estatísticos da produção, logo em seguida surgiu a preocupação em consolidar todos estes dados para determinar informações de relevância para a organização. Na década de 90 veio a Internet e a antiga informática passou a ser chamada de Tecnologia da Informação, ou simplesmente TI.

Surgiram então os sistemas integrados de gestão, alavancando os sistemas de relacionamento com clientes e controle de suprimentos que, juntos, prometeram integrar os sistemas de produção e funções administrativas em toda a organização. Por sua vez, esta integração trouxe uma visão holística para que se possa concretizar rapidamente, desde a tomada de decisões táticas, a um planejamento estratégico eficiente e facilmente mutável. Em paralelo ainda surgiram sistemas para a gestão do conhecimento da empresa, tornando o conhecimento tácito de seus colaboradores (conhecimentos individuais) em explícito (procedimentos operacionais) dentro de normas e condutas éticas.

Hoje, nenhuma corporação tem lugar no mercado sem todos estes sistemas já chamados de *commodities*[1], e não sobrevive sem *e-mail*, videoconferência, ferramentas de *groupware* como *chats* e mensagens instantâneas e portais corporativos baseados em gerenciamento eletrônico de documentos.

Vivemos em uma época onde os problemas são cada vez mais complexos e tentamos resolvê-los de uma forma eficiente com os modelos definidos de governança corporativa visando a uma melhor gerência de projetos estratégicos e remodelagem dos processos internos. Todos estes sistemas sempre demandam capacidade de transferência e armazenamento dos dados cada vez mais abundantes.

---

[1] *Commodity* é um termo do mercado financeiro que define mercadorias com características padronizadas, onde o único diferencial é o preço.

A cada dia se confirma que a gestão da informação é o ponto chave para qualquer sucesso e estamos constantemente submersos a ela com a vantagem desta *commodity* ser diferente do mercado financeiro, pois nós podemos constantemente transformá-la e agregar valor para nossas empresas serem sempre mais competitivas.

Mas as empresas em geral ainda não se preocupam o bastante com a proteção destas informações cruciais à constante sobrevida dos negócios.

> "A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócios". ABNT (2003, p.2).

Seguindo esta linha de raciocínio, ABNT (2003, p. 2) expõe-se que a segurança da informação é caracterizada pela preservação de:

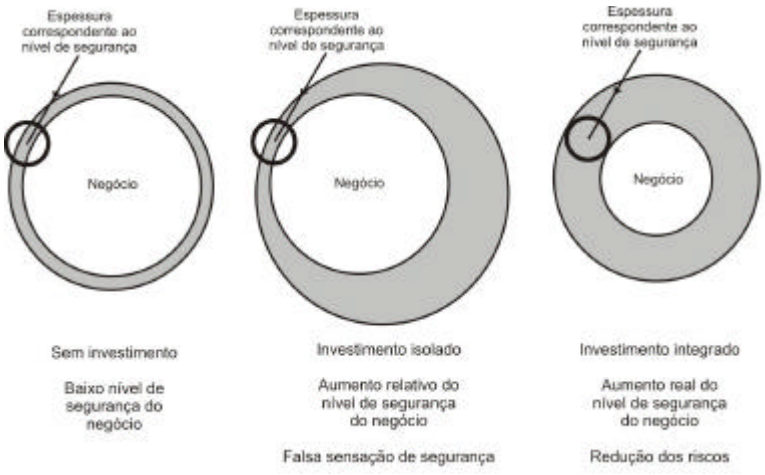
a) **confidencialidade:** garantia de que a informação é acessível somente por acesso autorizado;
b) **integridade:** salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
c) **disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

CAZEMIER (2003, p. 3) relata que administração de segurança é mais que trancar portas de salas ou insistir em disciplina com senhas. Aspectos de integridade de processamento de informação, como, quando ou veracidade, requerem consideração cuidadosa de fluxos de informação e proteções contra valores incorretos. E complementa que o papel da segurança é reduzir as chances de falha a um nível aceitável para a organização.

ITGI (2000, p. 45), em seu modelo de governança corporativa, diz que um dos objetivos da segurança é proteger a informação contra o uso não-autorizado, divulgação, modificação, dano ou perda.

A situação-problema vem baseada no nível de segurança praticado nas organizações. Hoje as empresas têm despendido recursos para proteger melhor sua informação, mas geralmente de formas pontuais, atacando a

segurança sob demanda. Mas o nível de segurança do negócio da corporação é sempre definido pelo ponto mais inseguro. Não adianta garantir proteção somente para algumas partes. Todo recurso gasto com a informação deve ser homogêneo e calculado, garantindo um nível de segurança uniforme.



Fonte: SÊMOLA (2003, p. 81)

Para se proteger das ameaças de interrupção dos negócios, as empresas têm a visão de que se investir em tecnologia elas estarão seguras. Como estas ameaças estão na maior parte ligadas a processos e pessoas, sendo geralmente a área de tecnologia responsável por mantê-la, têm-se uma equivocada sensação de segurança.

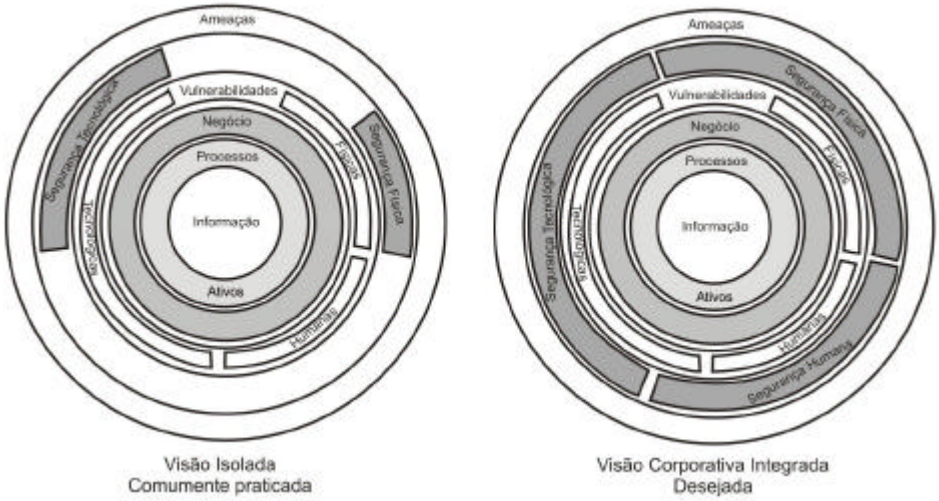
SÊMOLA (2003, p. 17) alerta para o problema com a seguinte pergunta: “Não estaria a equipe de segurança voltada apenas para os aspectos tecnológicos da segurança e, conseqüentemente, esquecendo-se dos aspectos físicos e humanos?” E completa com uma analogia: “De que adianta possuir duas trancas na porta social, se a outra, que permite acesso ao mesmo ambiente, só possui uma?”

O nível de segurança de uma empresa está diretamente associado à segurança oferecida pela “porta” mais fraca. Por isso, é preciso ter uma visão corporativa capaz de viabilizar uma ação consistente e abrangente, levando a empresa a atingir o nível de segurança adequado à natureza do negócio.

Além do foco no negócio da empresa, MOREIRA (2001, p. 12) complementa que as medidas de segurança não podem assegurar 100% de proteção e a empresa deve analisar a relação custo/benefício de todas. A corporação precisa achar o nível de risco que estará disposta a correr.

Seguindo a ênfase ao custo/benefício da segurança, PALMA (2004) alerta que a segurança deve ser muito bem aplicada somente onde é necessária, pois segurar todas as informações da empresa demanda um grande recurso financeiro, e geralmente não é necessário segurar todas as informações da organização.

A informação é cada vez mais um dos patrimônios importantes para um posicionamento de destaque das empresas no mercado, e atualmente têm-se os investimentos direcionados somente à tecnologia para garantir tal segurança. Assim sendo, delimita-se o objetivo deste trabalho em uma abordagem holística da segurança da informação de uma empresa com o foco em sua gestão e seu posicionamento no organograma da organização, para atingir o objetivo bem exemplificado na figura a seguir, onde a segurança é contemplada de uma forma completa:



Fonte: SÊMOLA (2003, p. 18)

Tendo em vista como fornecer segurança às informações empresariais, obtendo benefícios reais e reduzindo o risco de perda nos negócios demonstrado por itens de controle, este trabalho está estruturado da seguinte forma: em primeiro lugar, descreveremos a justificativa de se proteger estrategicamente as informações. Posteriormente citaremos as formas de proteção das informações encontradas em extensas literaturas. Por fim, objetivamos demonstrar como conduzir, no nível estratégico, as informações corporativas com segurança e focados no negócio, visando a diminuir os riscos e conseqüentemente aumentar o lucro e a competitividade.

2 POR QUE PROTEGER ESTRATEGICAMENTE AS INFORMAÇÕES

Em um universo globalizado e competitivo, as informações empresariais são cruciais para a continuidade do negócio e existem várias ameaças a essas informações. Segundo OLIVA (2003), citando uma pesquisa realizada pelo *Computer Security Institute* - CSI e *Federal Bureau of Investigations* - FBI, as principais quebras de segurança nos sistemas de informação ocorrem por: vandalismo, espionagem industrial, descontentamento de funcionários internos e concorrência desleal.

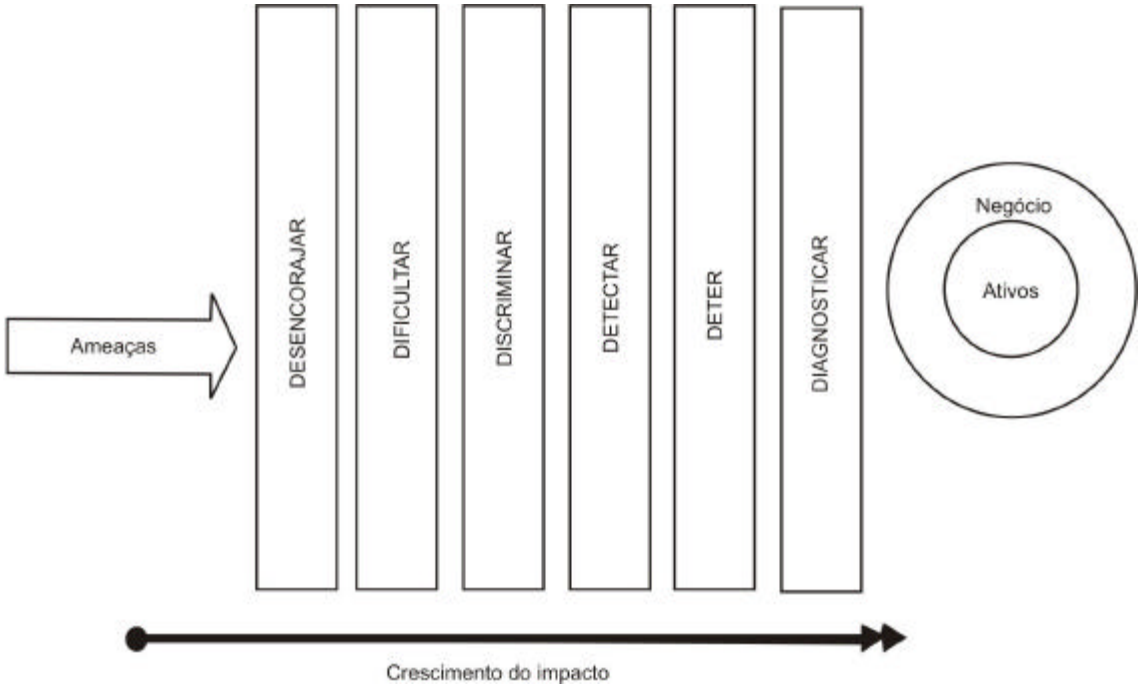
Atualmente, quase tudo pode ser considerado uma ameaça, uma vez que, sem algumas informações, pode-se decretar a falência de uma empresa. As ameaças também se tornam problemas quando a empresa possui o capital aberto em bolsas de valores, onde uma informação sigilosa pode comprometer toda a empresa. Outra ameaça é ao funcionamento dos processos empresariais dependentes de informação, onde BAIENSE (2003 p.16) coloca que basta imaginar uma ameaça ao fluxo de informação dentro de uma empresa para se vislumbrar a imagem do caos.

Como sujeito das ameaças aparece também a figura do *engenheiro social*. Um engenheiro social possui profundos conhecimentos de como extrair informações sigilosas de pessoas, e MITNICK (2003, p. 4) define como “um mágico inescrupuloso que faz você olhar a sua mão esquerda enquanto com a mão direita rouba seus segredos”. Segundo ele, esse personagem quase sempre é tão amistoso, desembaraçado e prestativo que você se sente feliz por tê-lo encontrado.

A mitigação das ameaças geralmente encontra uma barreira, pois administrar segurança quase sempre é um grande problema. Segundo (CAMPANA, 1997, p. 1), “segurança não acarreta novos programas, novas facilidades e, principalmente, não é um tópico importante para a gerência das empresas, pois segurança não gera receita”. Então, por que se preocupar com ela? Não seria melhor ignorá-la? Assim todos os esforços seriam canalizados para atividades "produtivas", com resultados visíveis.

Essa pode ser uma opção, desde que os riscos envolvidos sejam considerados. Podemos encarar segurança como uma espécie de seguro. Recursos são empregados com a finalidade de se tentar assegurar a continuidade do que se tem funcionando hoje. Uma empresa pode perfeitamente operar sem esse "seguro". Porém, se algum "imprevisto" ou incidente acontecer, qual será o custo? Assim como nos assuntos pessoais, é preciso segurar os bens valiosos da empresa. Basta que se defina qual o valor deste seguro.

Quanto menos protegermos as informações, maior o impacto nos negócios e ativos. A figura seguinte descreve o que devemos fazer para minimizar o impacto das ameaças nos ativos:



Fonte: SÊMOLA (2003, p. 53)

Nesta ilustração, Sêmola descreve o que fazer para diminuir o impacto das ameaças: desencorajar, dificultar, discriminar, detectar, deter e diagnosticar, sendo que, quanto mais a ameaça conseguir avançar nas barreiras de segurança, maior será o impacto. No próximo capítulo descreveremos as formas de proteção destas ameaças.

3 FORMAS DE PROTEÇÃO

Vários autores citam formas de proteção da informação, aumentando assim sua segurança. Todas as formas de proteção visam diminuir as ameaças ou pelo menos seu impacto à informação. O nível de proteção é proporcional à abrangência na organização. A seguir apresentaremos formas corporativas de proteção às ameaças da informação.

3.1 Classificação da Informação

A classificação da informação é essencial para que se defina como essa vai ser tratada do ponto de vista da segurança. Segundo ABNT (2003, p. 10), em geral, a classificação dada a uma informação é o caminho mais curto para se determinar como ela é tratada e protegida. Também cita que convém que a informação seja classificada para indicar a importância, a prioridade e o nível de proteção. Seguindo o tema, enfatiza que a informação possui vários níveis de sensibilidade e criticidade e alguns itens podem necessitar de um nível adicional de proteção ou de tratamento especial. Sugere, portanto, que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.

KOVACICH (1998, p. 104) destaca que as conseqüências de uma classificação errônea podem levar à superproteção, que é cara, ou à subproteção, que aumenta o risco e pode conduzir à perda da informação e, conseqüentemente, de dinheiro. MITNICK (2003, p. 210) justifica a classificação de informações como sendo fundamental para as categorias responsáveis pela liberação das informações confidenciais. Segundo o autor, essa política fornece uma estrutura para proteger as informações corporativas, tornando os empregados conscientes do nível de confidencialidade de cada informação.

Autores como Sêmola sugerem uma classificação levando-se em consideração a confidencialidade da informação, conforme figura seguinte:

Fonte: SÊMOLA (2003, p.107)

Mas há um problema quando se classifica a informação simplesmente pela sua confidencialidade. ABNT (2003, p. 10) sugere que a classificação da informação e seus respectivos controles de proteção levem em consideração as necessidades de negócios para compartilhamento ou restrição de informações e os respectivos impactos nos negócios como, por exemplo, o acesso não autorizado ou danos à informação. PALMA (2004) lembra que quando uma empresa utiliza níveis como confidencial, secreto, público e outros, apenas a questão da confidencialidade é destacada e isto gera um senso comum de proteção exclusivamente deste aspecto, deixando a integridade e a disponibilidade em segundo plano. E enfatiza que é importante observar que as informações possuem diferentes requisitos de confidencialidade, de integridade e de disponibilidade.

Considerando este contexto, as diversas sistemáticas não deveriam utilizar níveis de segurança cujos nomes apontam exclusivamente à manutenção da confidencialidade. É fundamental que a nomenclatura utilizada para cada nível represente a segurança através dos seus três aspectos principais. Uma alternativa seria utilizar uma sistemática de classificação que indicasse os três níveis. Por exemplo, um determinado relatório poderia apresentar a seguinte classificação: C2-I3-D1 – este código indica que a informação possui requisitos individuais para confidencialidade, integridade e disponibilidade.

Segundo Palma, uma alternativa mais simples seria classificar as informações com um qualificador único. Este pode ser numérico, ou pode estar associado a um nome. Porém os nomes utilizados não devem transparecer a

preservação exclusiva da confidencialidade. É interessante utilizar nomes como importante, crítico, vital, sensível, público. Esta nomenclatura teria a mesma função dos nomes utilizados na ilustração de Sêmola, porém os usuários estariam mais atentos à garantia não apenas da confidencialidade, mas da integridade e da disponibilidade das informações ao enquadrá-las em um dos níveis existentes.

KOVACICH (1998, p. 105) coloca que, se a informação tem valor, ela deve ser protegida e a proteção é cara. Deve-se proteger somente as informações necessárias e indispensáveis e por tempo determinado. O autor afirma também que o valor deve ser estabelecido pelo proprietário da informação, mas ressalta que o seu valor não deve ser baseado na importância para o proprietário, e sim para outras pessoas. Logo reforça a idéia da classificação correta da informação.

Outros autores já classificam a informação de forma completa, conforme figura seguinte:

Exigência de Segurança	**Sem critério** Segurança não é necessária	**Recomendável** Um certo grau de segurança é desejável	**Importante** Segurança é necessária pelos pontos-de-vista	**Essencial** Segurança é um critério primário
Confidencialidade	**Pública** A informação pode ser publicada	**Protegida** Somente podem ser vistos por um grupo seleto de pessoas	**Crucial** Somente podem ser vistos por pessoas diretamente envolvidas	**Obrigatória** Interesses do negócio podem ser gravemente afetados
Integridade	**Passiva** Sem proteção extra	**Ativa** Os processos de negócio toleram alguns erros	**Detectável** Um número mínimo de erros são permitidos	**Essencial** Processos de negócio não permitem erros
Disponibilidade	**Desnecessária** Sem garantia	**Necessária** Indisponibilidade ocasional é aceitável	**Importante** Em períodos de indisponibilidade há demora em processos	**Essencial** Indisponibilidade permitida somente em ocasiões excepcionais

Adaptado de CAZEMIER (2003, p. 29).

Assim sendo, para determinar o valor da informação, deve-se levar em consideração o custo de produção, o custo da perda para a organização e o custo do uso desta informação por terceiros. Para se determinar o seu valor, o custo de manutenção e proteção deve ser medido antes de se chegar a uma classificação. Posteriormente, deve-se fazer uma classificação garantindo sua confidencialidade, integridade e disponibilidade, fornecendo meios para a área de segurança definir como deve ser tratada a informação.

3.2 Política de Segurança

A política de segurança deve ser um elemento chave na gestão de segurança da empresa. MITNICK (2003, p. 208) define política de segurança como instruções claras que fornecem as orientações de comportamento do empregado para guardar as informações e é um elemento fundamental no desenvolvimento de controles efetivos para contra-atacar as possíveis ameaças à segurança. Como engenheiro social assumido, Mitnick enfatiza que essas políticas estão entre as mais significativas no que diz respeito a evitar e detectar os ataques da engenharia social.

O objetivo da política de segurança deve ser bem claro. Segundo OLIVA (2003), as informações do planejamento estratégico, o suporte à estratégia competitiva e o controle dos ativos e atividades que necessitem de informação são os aspectos organizacionais mais importantes que a política de segurança deve proteger.

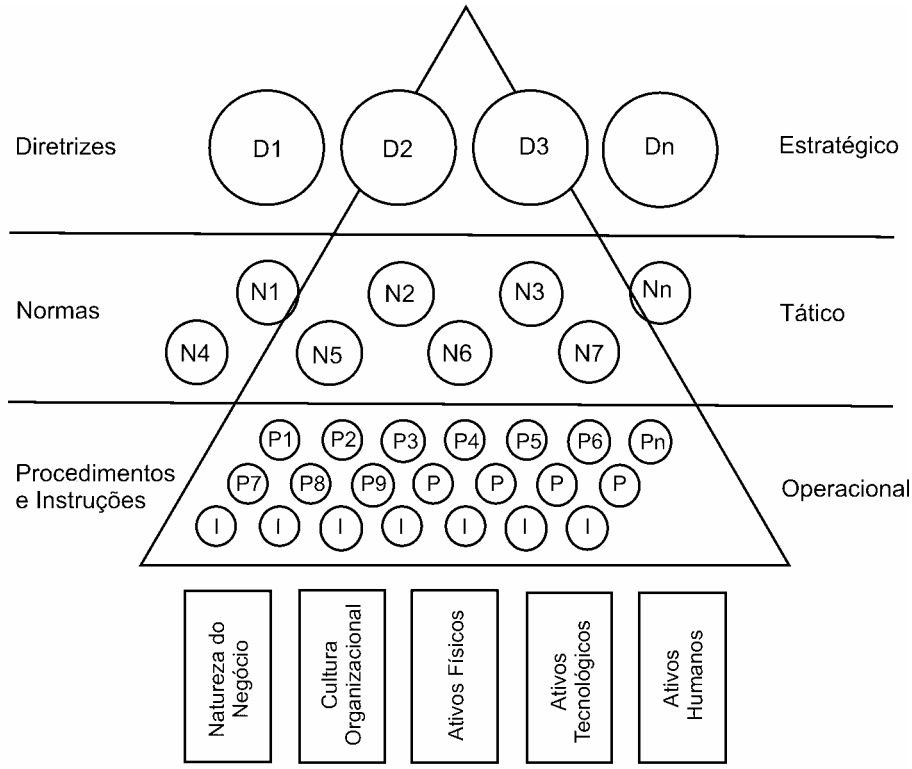
MITNICK (2003, p. 209) alega que, para que se divulgue uma política de segurança, é necessário um programa de conscientização da segurança:

> "O objetivo do programa de conscientização da segurança é a comunicação da importância das políticas de segurança e o dano que a falha em seguir essas regras pode causar. Dada a natureza humana, os empregados às vezes ignoram ou sabotam as políticas que parecem ser injustificadas ou que demandam muito tempo. A gerência tem a responsabilidade de garantir que os empregados entendam a importância das políticas e sejam motivados para atendê-las, e não tratá-las como obstáculos a serem contornados" MITNICK (2003, p. 209).

MARTINS (2003, p. 323) sugere que a política de segurança deva ser composta por um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção conveniente, de modo a garantir sua confidencialidade, integridade e disponibilidade. Segundo ele, essa política deve ser composta por um documento que contempla as diretrizes e regras de segurança na organização, envolvendo o detalhamento completo acerca de como cada medida de segurança é implantada.

A política de segurança deve ser bem ampla, abrangendo toda a organização e deve ser desmembrada em normas e procedimentos.

Sêmola exemplifica a política na figura abaixo:



Fonte: SÊMOLA (2003, p.106)

Observando a figura, poderemos concluir que a política de segurança deve ser desmembrada em diretrizes no nível estratégico, de normas no nível tático e de procedimentos e instruções no nível operacional, tendo em mente a natureza do negócio, a cultura organizacional e os ativos físicos, tecnológicos e humanos.

O maior problema da política de segurança é operacionalizá-la e MARTINS (2003, p. 323) descreve que o maior desafio de uma política de segurança não é iniciá-la, mas sim sustentá-la na organização, verificando permanentemente se as normas estão sendo seguidas e se há necessidade de atualizações. E acrescenta que, para se evitar que a política não caia no ostracismo e se torne apenas mais uma burocracia, a iniciativa deve ser disseminada maciçamente entre todos os funcionários. Isto deixa claro que deve ser definido um plano de continuidade da política de segurança.

BAIENSE (2003 p.17) aponta que elaborar uma estratégia de segurança e desmembrá-la numa política de segurança exige participação de executivos de vários setores, apoio incondicional da diretoria e adesão de todos os

funcionários, sugerindo assim a necessidade de a política de segurança ser corporativa.

A política de segurança deve conter as normas gerais para toda a organização nos aspectos mais relevantes. De acordo com a ABNT (2003, p. 4) convém que as seguintes orientações sejam seguidas na política de segurança:

a) definição de segurança da informação, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação;
b) declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação;
c) breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização, por exemplo:
   - conformidade com a legislação e cláusulas contratuais;
   - requisitos na educação de segurança;
   - prevenção e detecção de vírus e *software* maliciosos;
   - gestão da continuidade do negócio;
   - conseqüências das violações na política de segurança da informação;
d) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança;
e) referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que convém que os usuários sigam.

Mas as empresas brasileiras em geral ainda não aderiram à política de segurança. E isso pode estar gerando uma falsa sensação de segurança. Preocupado com a não-disseminação de uma política de segurança nessas empresas, Oliva realizou uma pesquisa em 2003 e comenta o resultado:

> "As empresas que não possuem uma política de segurança são as que consideram o impacto de incidentes de segurança mais baixo na competitividade da empresa, no caso de alteração de informações e da indisponibilidade das mesmas. Esse fato pode estar ocorrendo devido à não conscientização por parte dessas empresas da necessidade de segurança da informação, mesmo sendo afirmado por elas que os incidentes de segurança afetariam a estratégia competitiva com a quebra de credibilidade, com o vazamento de informações estratégicas e com a geração de imagem negativa no mercado. Talvez essas empresas nunca tenham tido um incidente de segurança, o que é pouco provável no mundo de hoje, ou pior, elas podem não saber que já ocorreram quebra de confidencialidade, alteração e indisponibilidade de suas informações, e por isso dão menor importância a eles" OLIVA (2003).

Conforme demonstrado, podemos concluir que são enormes os benefícios de uma política de segurança e ainda não foi disseminada por desconhecimento por parte das empresas. OLIVA (2003) sugere para as empresas que já estão desenvolvendo ou que pretendem desenvolver sua política de segurança que sejam adotadas as boas práticas recomendadas pela NBR ISO/IEC 17799[2], uma vez que pode ser requisitada no futuro uma certificação de segurança. Dessa forma, se os investimentos realizados em projetos de segurança estiverem de acordo com a forma, serão preservados, não sendo necessário o retrabalho. Além disso, a empresa poderá adotar o processo de gestão da segurança da informação de acordo com uma norma internacional, aplicada e reconhecida como as melhores práticas. E para as empresas que já elaboraram suas políticas de segurança, recomenda-se que em seu plano de revisões sejam realizadas as adequações necessárias para estarem de acordo com a NBR ISO/IEC 17799 e, assim, beneficiarem-se de um modelo já testado e aprovado por empresas em todo o mundo.

3.3 Segurança Física

A segurança física é importante para limitar o acesso pessoal à informação sigilosa. Em sua norma, ABNT (2003, p. 13) defende a definição de áreas de segurança tendo como objetivo prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização.

---

[2] Norma da ABNT citada no corpo do trabalho e na bibliografia.

ABNT (2001, p. 2), em outra norma referente à segurança física, aponta alguns riscos consideráveis, com objetivos bem práticos:

a) incêndio (dentro e fora do local), com suas conseqüências: gases e partículas, calor, desmoronamento, alagamento e corrosão;
b) explosões (dentro e fora do local);
c) intempéries (raio, vendaval, granizo);
d) água (vazamento, transbordamentos, derrame) e outros líquidos, inclusive material em fusão;
e) impacto de veículos ou aeronaves;
f) curto-circuito e outros danos elétricos;
g) atos por pessoas (roubo, assalto, desvio, sabotagem, infidelidade);
h) interrupção no fornecimento de utilidades ou distinção em sistema de climatização;
i) descarga eletrostática;
j) emissões eletromagnéticas (luz, raios-X, raios-gama);
k) campos magnéticos;
l) umidade, fungos;
m) roedores, insetos.

Na mesma norma, ABNT (2001, p. 2-3) descreve fatores de segurança que devem ser considerados:

a) localização: do terreno, do edifício no terreno e dentro do edifício;
b) construção: do edifício, do andar do edifício e do local das informações;
c) infraestrutura elétrica: pára-raios, energia e iluminação;
d) climatização: controle e segurança da temperatura e umidade, renovação do ar, pressão diferenciada e riscos inerentes ao sistema;
e) móveis, utensílios e equipamentos: carga combustível e riscos de ignição;
f) sistemas de controle de acesso;
g) sistemas de detecção e combate de incêndio, alagamento e outros sinistros;
h) operações de manuseio, procedimentos: produção, manutenção, transportes e atividades na vizinhança.

E em ABNT (2003, p. 13) recomendam-se alguns controles de entrada física:

a) Convém que visitantes das áreas de segurança sejam checados quanto à permissão para acesso e tenham registradas data e hora de sua entrada e saída. Convém que estas pessoas obtenham acesso apenas às áreas específicas, com propósitos autorizados e que esses acessos sigam instruções baseadas nos requisitos de segurança e procedimentos de emergência próprios da área considerada.
b) Convém que o acesso às informações sensíveis, instalações e recursos de processamento de informações seja controlado e restrito apenas ao pessoal autorizado. Convém que os controles de autenticação, como, por exemplo, cartões com PIN (número de identificação pessoal ou *personal identification number*), sejam usados para autorizar e validar qualquer acesso. Convém que, ainda, seja mantida em segurança uma trilha de auditoria contendo todos os acessos ocorridos.
c) Convém que todos os funcionários utilizem alguma forma visível de identificação e sejam incentivados a informar à segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado.
d) Convém que os direitos de acesso às áreas de segurança sejam regularmente revistos e atualizados.

Tem-se constatado também espionagem industrial profissional, onde funcionários “espiões” se candidatam a algum cargo da empresa, geralmente de baixo nível de requisitos, mas com acesso total à empresa (ex. faxineiro), para que possa realizar seus trabalhos. Neste caso, ABNT (2003, p. 17) fornece uma solução, onde a organização deve considerar a adoção de uma política de mesa limpa para papéis e mídias removíveis e uma política de tela limpa para os recursos de processamento da informação, de forma a reduzir riscos de acesso não autorizado, perda e danos à informação durante e fora do horário normal de trabalho. A norma enfatiza que a política deve levar em consideração as classificações da segurança das informações, os riscos correspondentes e os aspectos culturais da organização.

3.4 Segurança Lógica

Em uma época em que a Internet é a maior fonte de informações disponível temos que nos preocupar também com a chamada segurança lógica.

A segurança lógica está intimamente ligada aos recursos de TI de uma empresa, e refere-se basicamente às permissões de acesso às informações. Neste ponto, que chamamos de “autenticação”, temos um “Calcanhar de Aquiles”, onde a senha pessoal de acesso é um fator importante para a proteção. ABNT (2003, p. 30) alerta quanto ao uso de senhas e sugere que todos os usuários de sistemas de informação sejam informados para:

a) manter a confidencialidade da senha;
b) evitar o registro das senhas em papel, a menos que o papel possa ser guardado de forma segura;
c) alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
d) selecionar senhas de qualidade, com um tamanho mínimo de seis caracteres que sejam:
   - fáceis de lembrar;
   - não baseadas em coisas que outras pessoas possam facilmente adivinhar ou obter a partir de informações pessoais, por exemplo nomes, números telefônicos, datas de nascimento, etc.;
   - isentas de caracteres idênticos consecutivos ou de grupos de caracteres somente numéricos ou alfabéticos;
e) alterar a senha em intervalos regulares ou baseando-se no número de acessos (senhas pra contas privilegiadas devem ser alteradas com maior freqüência do que senhas normais) e evitar a reutilização de senhas antigas;
f) alterar senhas temporárias no primeiro acesso ao sistema;
g) não incluir senhas em processos automáticos de acesso ao sistema, por exemplo armazena-las em macros ou teclas de função;
h) não compartilhar senhas individuais.

Há outros mecanismos para substituir as senhas na referida autenticação. Hoje, podemos utilizar formas de identificação como “o que você sabe”, “o que você tem” e “o que você é”. Estas formas podem ser exemplificadas respectivamente como senha, cartões magnéticos e impressão

digital. Estas últimas formas têm evoluído bastante com reconhecimento de íris, cartões inteligentes que armazenam informações, certificação digital, etc., mas explicá-los todos aqui tangenciaria o objetivo do nosso trabalho.

3.5 Gerenciamento do Risco

Um dos grandes desafios da área de segurança é medir os benefícios dos projetos de segurança. O Gerenciamento do Risco visa descrever os riscos e colocá-los em um patamar aceitável pela organização, permitindo assim controlar os benefícios da segurança. KOVACICK (1998, p. 117-119) expõe que o objetivo do gerenciamento de riscos é aumentar a segurança com o menor custo possível, fornecendo a melhor proteção à informação da organização no armazenamento, processamento ou transmissão ao menor custo consistente com o valor da informação.

> "Definir uma política de gerenciamento de risco exige um alinhamento de ações estratégicas, táticas e operacionais. No nível estratégico, a empresa precisa determinar a estrutura e os controles de segurança a serem adotados em consonância com a legislação pertinente, os riscos do negócio e os requerimentos de segurança de parceiros e clientes. No nível tático, a Análise de Impacto nos Negócios e a Análise de Risco são as duas ferramentas utilizadas para definir a aplicação da política. No nível operacional, a divulgação de guias, processos e procedimentos são os recursos utilizados para implementar tudo o que foi projetado" BAIENSE (2003, p. 15).

RAMOS (2002) indica que o resultado do Gerenciamento do Risco dá à organização o controle sobre seu próprio destino – através do relatório final, pode-se identificar quais controles devem ser implementados em curto, médio e longo prazo. Há então uma relação de valor; ativos serão protegidos com investimentos adequados ao seu valor e ao seu risco.

3.5.1 Identificação dos Riscos

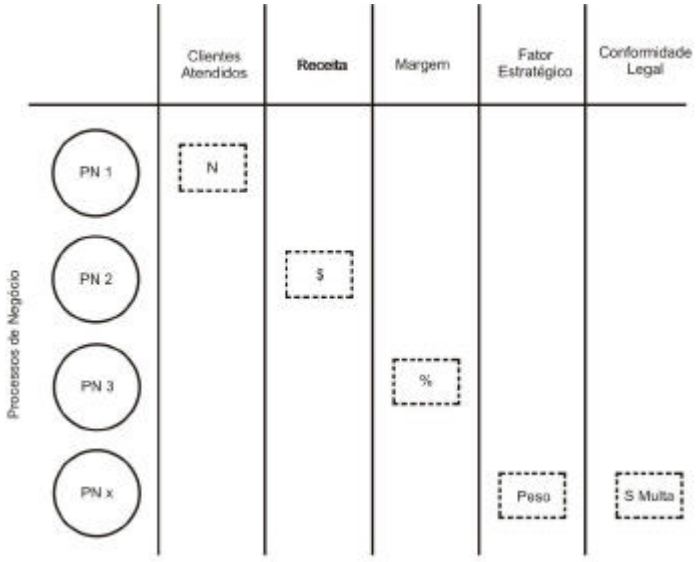
Para que sejam coletadas as informações necessárias ao gerenciamento de riscos, MOREIRA (2001, p. 11) sugere que primeiramente seja seguido um processo de identificação e posteriormente avaliação dos fatores de risco presentes no ambiente organizacional. Segundo esse autor, este passo inicial possibilita uma visão do impacto negativo causado aos

negócios, e que através da aplicação desse processo é possível futuramente determinar as prioridades de ação em função do risco identificado, para que seja atingido o nível de segurança desejado pela organização. O processo de identificação e avaliação dos fatores de risco proporciona também informações para que se possa prever o tamanho e o tipo de investimento necessário para prevenir os impactos na organização causados pela perda ou indisponibilidade dos recursos fundamentais para o negócio. O mesmo autor em um outro artigo completa que “os riscos não podem ser determinados sem o conhecimento de até que ponto um sistema é vulnerável à ação das ameaças” MOREIRA (2001, p. 22-23).

Segundo PRADO (2002)**,** nessa etapa devem ser identificados os riscos a que o negócio (o foco sempre deve ser este) está sujeito. Junto com esta identificação deve ser realizada uma análise para identificação de ameaças e vulnerabilidades. Esta análise inicial, segundo o autor, pode ser tanto quantitativa – baseada em estatísticas, numa análise histórica dos registros de incidentes de segurança – quanto qualitativa – baseada em know-how, geralmente realizada por especialistas, que têm profundos conhecimentos sobre o assunto. Devido à sua agilidade, geralmente as empresas tendem a adotar o modelo qualitativo, que não requer cálculos complexos. Independentemente do método adotado, esta primeira fase deve contemplar algumas atividades, como o levantamento de ativos a serem analisados, definição de uma lista de ameaças e identificação de vulnerabilidades nos ativos.

Em um processo de análise de segurança, devem-se identificar os processos críticos vulneráveis e saber se os riscos a ele associados são aceitáveis ou não. O nível de vulnerabilidade decai à medida que são implantados controles e medidas de proteção adequadas, diminuindo também os riscos para o negócio. Pode-se dizer que os riscos estão ligados ao nível de vulnerabilidade que o ambiente possuir, pois, para se determinar os riscos, as vulnerabilidades precisam ser identificadas.

SÊMOLA (2003, p. 89), consciente da dificuldade de identificação dos riscos, sugere como deve ser feita uma avaliação dos processos de negócio quanto ao risco:



Fonte: (SÊMOLA 2003, p. 89)

Esta ilustração sugere os riscos sejam colocados em uma matriz juntamente com os processos de negócio, para que seus respectivos valores possam ser melhor identificados. Os riscos apresentados como exemplo são: Clientes Atendidos, Receita, Margem, Fator Estratégico e Conformidade Legal. Segundo o autor esta matriz auxilia na identificação dos riscos em relação ao negócio, uma vez que sua visualização é analítica.

3.5.2 Quantificação dos Riscos

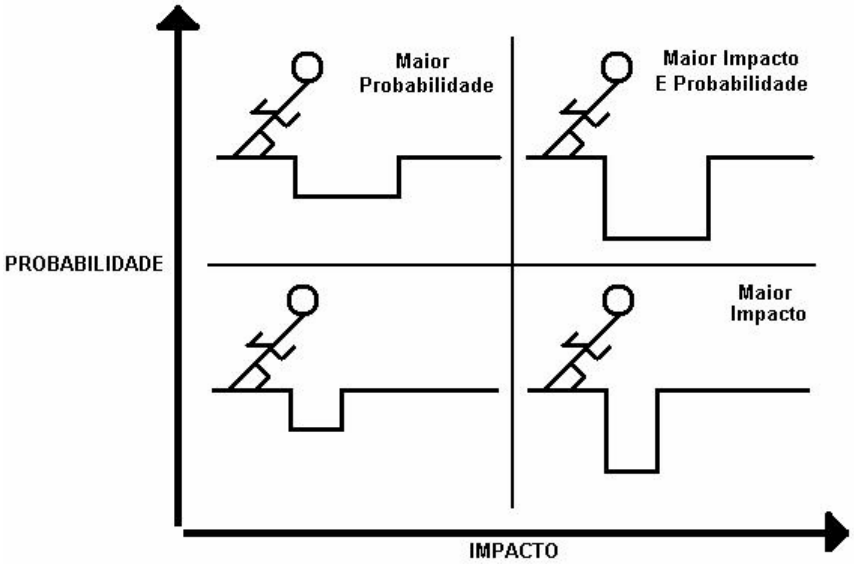
Concluída a primeira fase de identificação dos riscos, PRADO (2002) sugere que se inicie uma segunda fase chamada por ele de “Quantificação dos Riscos”. Nessa etapa é mensurado o impacto que um determinado risco pode causar ao negócio. Como é praticamente impossível oferecer proteção total contra todas as ameaças existentes, é preciso identificar os ativos e as vulnerabilidades mais críticas, possibilitando a priorização dos esforços e os gastos com segurança.

O objetivo desta fase é definir ações com as respectivas prioridades para que se minimizem os riscos. Para isso, de acordo com ABNT (2003, p. 2), nesta segunda fase deve ser realizada uma avaliação sistemática:

a) do impacto nos negócios como resultado de uma falha de segurança, levando-se em conta as potenciais conseqüências da perda de confidencialidade, integridade ou disponibilidade da informação ou de outros ativos;

b) da probabilidade de tal falha realmente ocorrer à luz das ameaças e vulnerabilidades mais freqüentes e nos controles atualmente implementados.

Com base nas considerações acima podemos concluir que o risco é medido em relação ao impacto nos negócios e em relação à probabilidade deste risco ocorrer. Quanto maiores se apresentam a probabilidade e o impacto, maior o risco exposto.



Fonte: o autor

Neste desenho podemos diferenciar claramente a probabilidade do impacto fazendo uma analogia para um buraco no chão. De baixo para cima aumentamos a probabilidade da queda pela largura do buraco. Da esquerda para a direita aumentamos o impacto da queda pela profundidade do buraco. O gerenciamento do risco nesta fase inicial visa a listar os grandes riscos presentes no quadrante apontado como “maior impacto e probabilidade” no desenho.

PRADO (2002) cita uma técnica utilizada no mercado para auxiliar esta segunda etapa: BIA, do inglês *Business Impact Analisys*, ou análise de impacto. Esta técnica consiste, basicamente, da estimativa de prejuízos financeiros decorrentes da paralisação de um serviço. Você é capaz de responder quanto sua empresa deixaria de arrecadar caso um sistema estivesse indisponível durante duas horas? O objetivo do BIA é responder questões desse tipo.

BAIENSE (2003, p. 15) conclui que esta fase ajuda o executivo a entender as ameaças presentes em cada processo e cada ativo dentro da empresa. Segundo o autor, reconhecer as brechas, quantificar e qualificar a extensão dos danos que podem causar são os passos fundamentais para promover uma gestão adequada.

3.5.3 Tratamento dos Riscos

A terceira fase do gerenciamento do risco tem como objetivo fornecer ações para minimizar os riscos, priorizando os maiores riscos apontados na segunda fase.

PRADO (2002) nomeia esta terceira fase como “Tratamento dos Riscos”. Segundo o autor, uma vez que os riscos foram identificados e a organização definiu quais serão tratados, as medidas de segurança devem ser de fato implantadas. O ROI (*Return Of Investment* ou retorno de investimento) e o BIA servem justamente para auxiliar nesta tarefa. Alguns riscos podem ser eliminados, outros reduzidos ou até mesmo aceitos pela empresa, tendo sempre a situação escolhida documentada. Só não é permitido ignorá-los.

RAMOS (2001) define duas das maneiras mais conhecidas e utilizadas pelo gerentes de segurança da informação para o cálculo do ROI: são as análises de custos por incidente (individualizada por evento), e a análises de custos acumulados (geralmente mensal ou anual).

A primeira destas técnicas é chamada de *Single Loss Expectancy* (SLE). O cálculo do SLE mensura em termos financeiros o impacto de um incidente. Para início devemos listar todos os ativos (tudo aquilo que é importante para a organização) e identificar as ameaças e vulnerabilidades existentes. Não devemos esquecer de potencializar o valor do risco pela importância do ativo no contexto da organização.

O cálculo de nossa segunda força de argumentação, instrumento capaz de mensurar os resultados de um bom projeto ou produto de segurança da informação, é baseado em incidentes percebidos ao longo de um período. Esta fórmula equaciona a *Single Loss Expectancy*, e o número de eventos ocorridos em um determinado espaço de tempo.

SLE x número de ocorrências anuais = *Annualized Loss Expectancy*

MENEGOTTO (2003) coloca que uma análise de riscos possibilita a detecção de falhas e, o mais importante, a possibilidade da aplicação de controles objetivos nos pontos mais críticos e com real necessidade de investimento. Assim há possibilidade de verificar perdas e conseqüências da falta de controles adequados.

3.5.4 Monitoração dos Riscos

Em uma última fase, PRADO (2002) expõe que o Gerenciamento de Riscos é um processo contínuo, que não termina com a implantação de uma medida de segurança. Através de uma monitoração constante, é possível identificar quais áreas foram bem sucedidas e quais precisam de revisões e ajustes. O mais importante de um gerenciamento de riscos é mantê-lo funcionando ao longo da vida da empresa. Para isso, o PMI – *Project Management Institute* (2000, p.127) citou que, nesta fase, devem ser realizados continuamente:

a) Planejamento de Resposta a Riscos: desenvolver procedimentos e técnicas para aumentar oportunidades e para reduzir ameaças de riscos para os objetivos do projeto.
b) Controle e Monitoração dos Riscos: monitorar os riscos residuais, identificar novos riscos, executar os planos de redução de risco e avaliar sua efetividade durante todo o ciclo de vida do projeto.

RAMOS (2002) menciona que as partes da gerência do risco, isoladas, representam muito pouco ou quase nada. Alinhados e geridos de forma adequada, estes componentes podem apontar caminhos seguros na busca ao nível adequado de segurança de uma organização. Segundo o autor, para uma correta gestão do risco, utiliza-se como métrica as melhores práticas de segurança da informação do mercado, apontadas na norma NBR ISO/IEC 17799. A partir destas informações faz-se possível a elaboração do perfil de risco, que segue a fórmula:

(Ameaça) x (Vulnerabilidade) x (Valor do Ativo) = RISCO ou resumindo:

(Probabilidade) x (Impacto) = RISCO

Uma análise de riscos deve ser realizada – sempre – antecedendo um investimento. Antes de a organização iniciar um projeto, um novo processo de negócio, o desenvolvimento de uma ferramenta ou até mesmo uma relação de parceria, deve-se mapear, identificar e assegurar os requisitos do negócio.

O processo de análise de riscos deve envolver especialistas em análise de riscos e especialistas no negócio da empresa – esta sinergia possibilita o foco e a qualidade do projeto. Um projeto de Análise de Risco sem o envolvimento da equipe da empresa, muito dificilmente retratará a real situação da operação.

A execução do projeto deve ser realizada em tempo mínimo. Em ambientes dinâmicos a tecnologia muda muito rapidamente. Um projeto com mais de um mês em determinados ambientes, ao final, pode estar desatualizado e não corresponder ao estado atual da organização.

Com estas definições podemos infiltrar a gestão de riscos dentro da organização, reduzindo os custos de incidentes de segurança e retornando o real valor de uma gestão de segurança.

3.6 Plano de Continuidade de Negócios

Do Gerenciamento de Riscos, explanado anteriormente, pode-se surgir a necessidade de garantir a disponibilidade da informação de uma empresa e conseqüentemente prolongar sua existência. Caso haja esta necessidade, a solução é desenvolver um Plano de Continuidade de Negócios.

ABNT (2003, p. 45) descreve que o objetivo do Plano de Continuidade de Negócios é não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastre significativo.

O Plano de Continuidade de Negócios (também chamado simplesmente de PCN ou BCP – do inglês *Business Continuity Plan*) visa estabelecer processos e procedimentos para que, em caso de emergência, mantenha-se a continuidade de operação da organização, minimizando o impacto em seus negócios. Para isso, KOVACICH (1998, p. 122-123) define como deve ser estruturado o plano de continuidade de negócios:

a) propósito: razão e objetivo do plano;

b) escopo: escopo e aplicabilidade do plano;

c) premissas e restrições: pré-requisitos, prioridades, incidentes inclusos e exclusos;
d) responsabilidades: quem vai ser responsável por o quê;
e) estratégias: ações para contingência e periodicidade de testes;
f) pessoal: lista das pessoas-chave, endereços, telefones e prioridade de aviso.
g) informação: identificação das informações e ativos vitais;
h) ativos: lista de inventário, contrato de manutenção e reposição;
i) documentação: informação atualizada dos ativos de produção e contingência;
j) telecomunicação: identificação e manutenção dos dispositivos de voz e dados;
k) suprimentos: lista de tudo que é necessário para a continuidade da operação como material de escritório, mesas, telefones, computadores e impressoras;
l) transporte: listar o que deve ser transportado, sua origem e procedimento para transporte;
m)utilidades: equipamentos para energia elétrica, ar condicionado, etc.

Mas ainda encontramos problemas ao realizar um plano de continuidade de negócios. SCHNEIDER (2003) expõe que o que acontece, principalmente em nível nacional, é que a continuidade de uma empresa ainda é vista de maneira distorcida. À vista da alta gerência, os profissionais de continuidade estão preocupados com catástrofes e desastres ao invés de procurarem alternativas para aumentar a produtividade e rentabilidade. E o autor ainda vai contra alguns princípios básicos da administração atual: “Ainda permeia nas organizações nacionais a visão conservadora das gerências, onde as palavras mágicas e atrativas são: ROI e redução do TCO (*Total Cost of Ownership* ou Custo Total de Propriedade)”.

Schneider tenta descrever o real motivo de não se investir em plano de continuidade, e conclui-se que no modelo adotado atualmente é muito difícil convencer a alta administração a implementar planos como estes.

Mas ABNT (2003, p. 46) insiste na necessidade deste plano e descreve alguns elementos-chave na gestão da continuidade dos negócios:

a) entendimento dos riscos que a organização está exposta, no que diz respeito à sua probabilidade e impacto, incluindo a identificação e priorização dos processos críticos do negócio;
b) entendimento do impacto que as interrupções provavelmente terão sobre os negócios e estabelecimento dos objetivos do negócio relacionados com as instalações e recursos de processamento da informação;
c) consideração de contratação de seguro compatível que possa ser parte integrante do processo de continuidade;
d) definição e documentação de estratégia de continuidade consistente com os objetivos e prioridades estabelecidas para o negócio;
e) detalhamento e documentação de planos de continuidade alinhados com a estratégia estabelecida;
f) testes e atualizações regulares dos planos e procedimentos implantados;
g) garantia que a gestão da continuidade do negócio esteja incorporada aos processos e estrutura da organização. A responsabilidade pela coordenação do processo de gestão de continuidade do negócio deve ser atribuída a um nível adequado dentro da organização, por exemplo ao fórum de segurança da informação.

SCHNEIDER (2003) defende sua aplicação indicando que o Plano de Continuidade visa a prevenir a ocorrência de desastres, minimizar o impacto de um desastre e viabilizar a ativação de processos alternativos quando da indisponibilidade dos processos vitais.

Como passo inicial no desenvolvimento do processo de continuidade, deve ser elaborado o BIA, já citado no item 3.5, mas que, segundo o autor, sua definição e objetivo são desconhecidos por muitos. No BIA serão identificados os impactos de um possível desastre sobre as operações de uma organização. Além da identificação da criticidade dos processos, esta avaliação fornecerá informações que permitirão definir o escopo do plano e a tolerância quanto à paralisação dos processos vitais.

Ainda segundo Schneider, uma vez identificada a criticidade dos processos, será necessário avaliar o grau de exposição destes ativos críticos. A avaliação do grau de exposição é uma função que envolve algumas variáveis como perdas possíveis, ameaças, vulnerabilidades e controles. Os ativos que,

ao serem impactados implicarem uma perda significativa, deverão ser alvos de estudo pormenorizado na avaliação do Grau de Exposição.

Sabendo o quão exposta sua organização está, inicia-se a elaboração das estratégias de continuidade visando aos objetivos dos planos. Devemos considerar: o custo da implantação, a manutenção dos procedimentos, a eficácia dos procedimentos, a cultura organizacional e a estratégia de resposta organizacional. Exemplos definidos na estratégia como tipos de site (*Hot-site, Warm-site, Cold-site*), acordos de reciprocidade, bureau de serviços externos, auto-suficiência e realocação da operação são aspectos fundamentais que devem ser considerados.

Após esse árduo processo de levantamento de dados, requisitos, cálculos, análise de dados, chegamos à fase de definição dos Planos de Continuidade, onde os objetivos vão desde a prevenção de ocorrências de desastres à manutenção dos processos vitais em operação.

Como citado anteriormente, recomenda-se que sejam criados os planos para serem executados antes (prevenção), durante (emergencial) e após (manutenção) o desastre.

Finalmente, chegamos à implementação dos planos de continuidade. Conforme SCHNEIDER (2003), a implementação compreende as ações que visam a tornar um plano efetivamente testado e atualizado. Essa definição visa ao treinamento do pessoal, à implantação dos procedimentos, treinamentos e simulações. Também à manutenção e aperfeiçoamento permanente do plano como um todo, sua documentação e infraestrutura.

3.7 Segurança em Pessoas

Pessoas merecem um tópico à parte por formarem o ponto mais fraco da segurança, pois elas necessitam constantemente de treinamento conciso e coerente para que possam desempenhar bem sua função de segurança. MITNICK (2003, p. 4) alerta com uma frase única: “a segurança não é um problema para a tecnologia – ela é um problema para as pessoas e a direção”.

Ainda Mitnick, como exímio conhecedor de técnicas de obtenção de informações sigilosas, enfatiza o poder do engenheiro social e alerta para o problema das pessoas:

> “Um engenheiro social experiente pode ter acesso a praticamente qualquer informação-alvo usando as estratégias e táticas de sua habilidade. Os tecnologistas experientes têm desenvolvido soluções de segurança da informação para minimizar os riscos ligados ao uso dos computadores, mas mesmo assim deixaram de fora a vulnerabilidade mais significativa: o fator humano. Apesar de nosso intelecto, nós humanos – você, eu e todas as outras pessoas – continuamos sendo a ameaça mais séria à segurança do outro” MITNICK (2003, p. 7).

Para que a área de segurança reduza o risco de erro humano, fraude ou uso indevido das instalações da empresa, ABNT (2003, p. 10) cita que convém que as responsabilidades de segurança sejam atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a vigência de cada contrato de trabalho.

3.7.1 Seleção e Política de Pessoal

RAMOS (2002) confirma a estatística de que a grande maioria dos incidentes com a informação é proveniente de vulnerabilidades que são exploradas (consciente ou inconscientemente) por pessoas, seja no mau uso de recursos de TI, desconhecimento de regras de segurança ou liberação proposital de informações confidenciais. Com base nesta informação notamos o quão importante e indispensável é a participação do departamento de RH na consolidação de um plano de ação para a implementação e manutenção dos controladores culturais. O que o autor nomeia esta atitude como *“organizational culture”*, no ambiente corporativo, afirmando que a participação do departamento de Recursos Humanos inicia-se na definição dos requisitos de segurança para a identificação de cargos críticos, funções, regras e responsabilidades.

ABNT (2003, p. 10) recomenda que, para diminuir o risco de insegurança causados pelas pessoas e principalmente pelos colaboradores da empresa, sejam feitas verificações de controle no momento da seleção de candidatos:

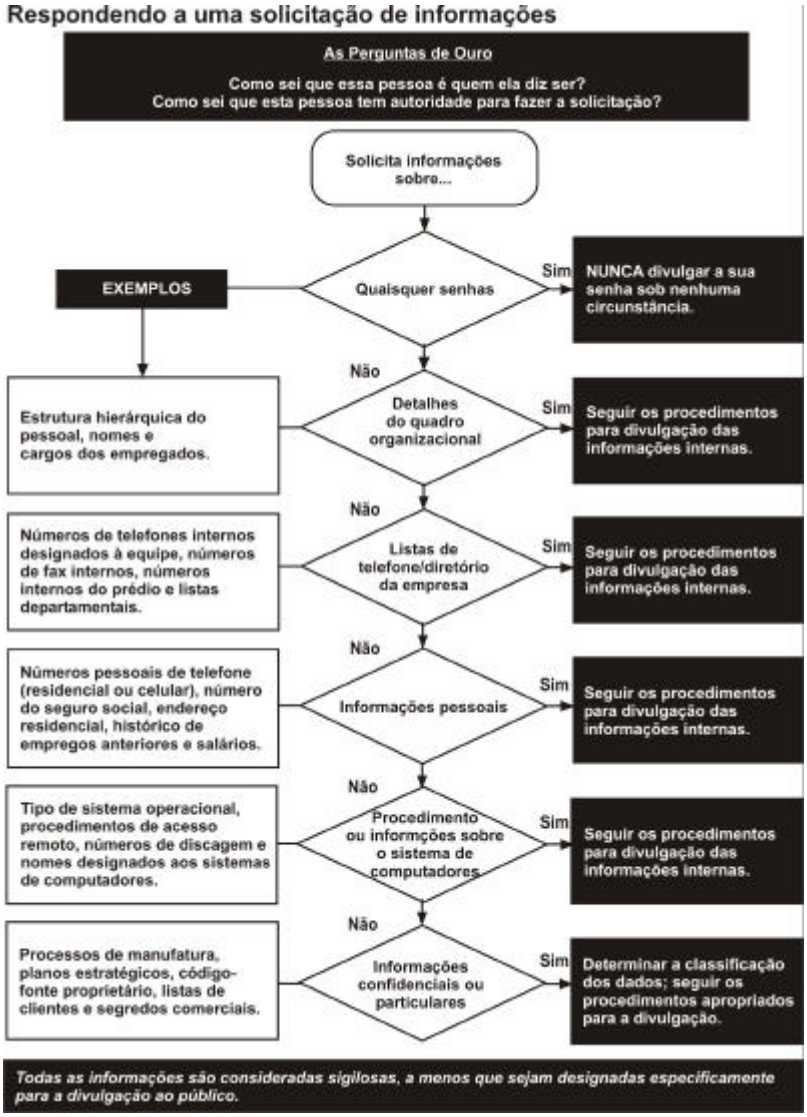
a) disponibilidade de referências de caráter satisfatório, por exemplo, uma referência profissional e uma pessoal;
b) verificação da exatidão e inteireza das informações do *curriculum vitae* do candidato;

c) confirmação das qualificações acadêmicas e profissionais;
d) verificação da identidade (passaporte ou documento similar).

3.7.2 Educação e Treinamento em Segurança da Informação

Depois de realizar um criterioso recrutamento e seleção de pessoal, segundo ABNT (2003, p. 12), convém que todos os funcionários da organização e, onde forem relevantes, prestadores de serviços, recebam treinamento apropriado e atualizações regulares sobre as políticas e procedimentos organizacionais. Isto inclui requisitos de segurança, responsabilidades legais e controles do negócio, assim como treinamento sobre o uso correto das instalações de processamento da informação como, por exemplo, procedimentos de acesso ou uso de recursos de TI, antes que seja fornecido qualquer acesso aos serviços ou informações.

Mitnick sugere que seja feito um fluxograma para resposta às perguntas conforme figura seguinte:

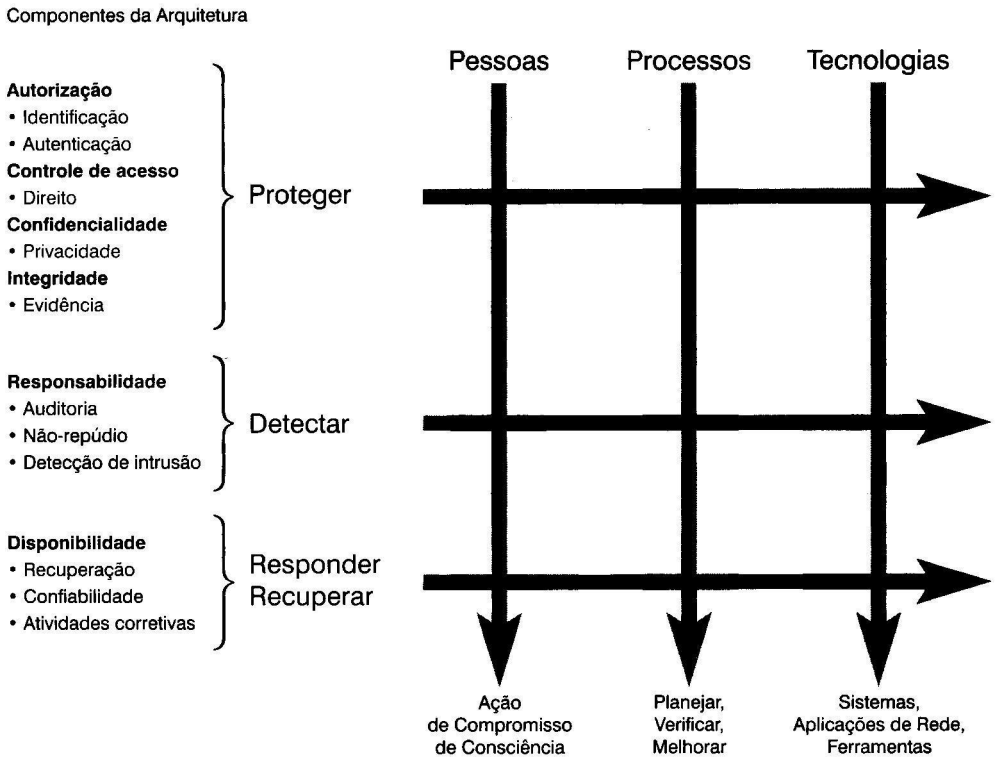


Fonte: MITNICK (2003, p. 270)

(MAGULL, Rich *In:* BAIENSE, 2003 p.14) alerta: “As pessoas não podem gerenciar riscos que não conhecem, com ferramentas que não entendem e recursos que não sabem que existem” (*apud.)*. O especialista defende que, numa empresa consciente dos riscos a que está exposta, as chances de um incidente provocar perdas caem drasticamente quando as pessoas sabem como reconhecer, reportar e responder a problemas. Com empregados bem treinados, melhoram as chances de se detectar e prevenir acidentes de segurança antes que eles causem danos.

4 GESTÃO ESTRATÉGICA DE SEGURANÇA DA INFORMAÇÃO

Para que se consiga instituir as formas de proteção descritas no capítulo anterior do trabalho, faz-se necessária uma gestão estratégica de segurança da informação, onde os controles não podem ser pontuais, mas sim corporativos.



Fonte: McCARTHY (2003, p. 70)

McCarthy sugere as ações de proteger, detectar, responder e recuperar a informação abrangendo pessoas, processos e tecnologia. Tentaremos descrever nos tópicos seguintes como se estruturar esta área estratégica.

4.1 Objetivos

O maior objetivo de uma gestão estratégica de segurança de informações não é garantir o nível máximo de segurança, mas sim controlar os riscos para que eles não sejam ameaças para a empresa. Segundo BAIENSE (2003 p.16), Gestão da Segurança da Informação é o nome genérico que os especialistas dão a um conjunto de estratégias, normas, procedimentos e

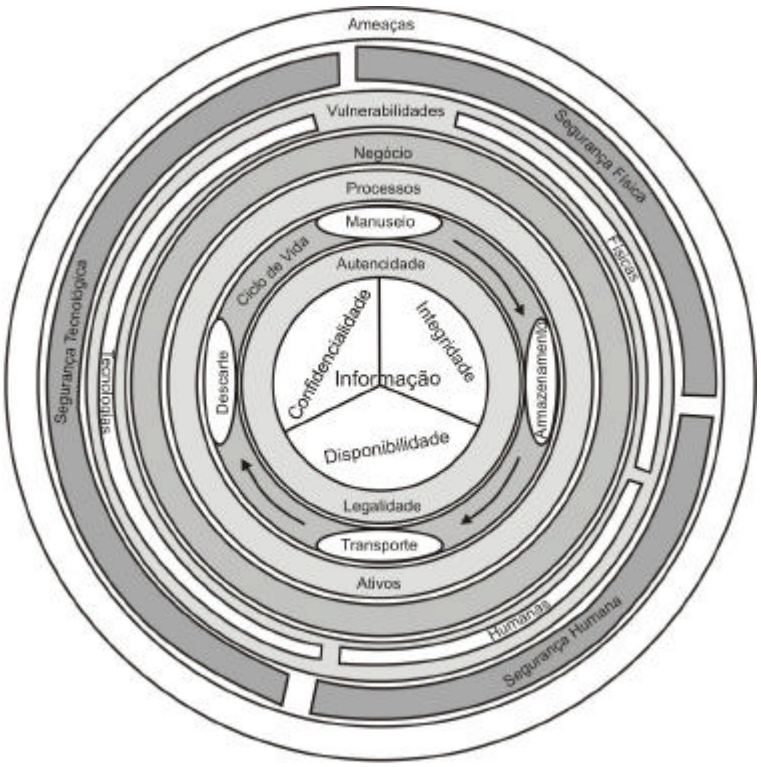
controles para implementar não uma operação à prova de falhas, mas um correto gerenciamento de risco. Em última análise, implementar a segurança da informação significa adequar e manter o risco em um nível compatível com a atividade da empresa. Porém MITNICK (2003, p. 8) alerta que a segurança corporativa é uma questão de equilíbrio. Pouca ou nenhuma segurança deixa sua empresa vulnerável, mas uma ênfase exagerada atrapalha a realização dos negócios e inibe o crescimento e a prosperidade da empresa. O desafio é atingir um equilíbrio entre a segurança e a produtividade.

Conseqüentemente, o ponto crucial para uma correta gestão seria aplicar corretamente os recursos destinados à segurança organizacional, não “engessando” os processos empresariais nem tão pouco realizando um ínfimo controle sobre a segurança.

KOVACICH (1998, p. 59), mais prático, cita alguns passos da gestão de segurança:

a) montar o planejamento estratégico, tático e anual;
b) determinar a organização do departamento de segurança;
c) determinar as funções do departamento de segurança;
d) determinar o fluxo dos processos de segurança na organização.

Sêmola, alguns anos após, descreve o objetivo da segurança estratégica no desenho seguinte:



Fonte: SÊMOLA (2003, p. 51)

Neste desenho é exposto em camadas o posicionamento da informação na empresa, composta de processos, que fazem parte do negócio, sujeito às vulnerabilidades, protegidas das ameaças externas por estratégias de segurança.

KOVACICH (1998, p. 59) completa sucintamente com algumas responsabilidades da gestão estratégica da segurança de informações:

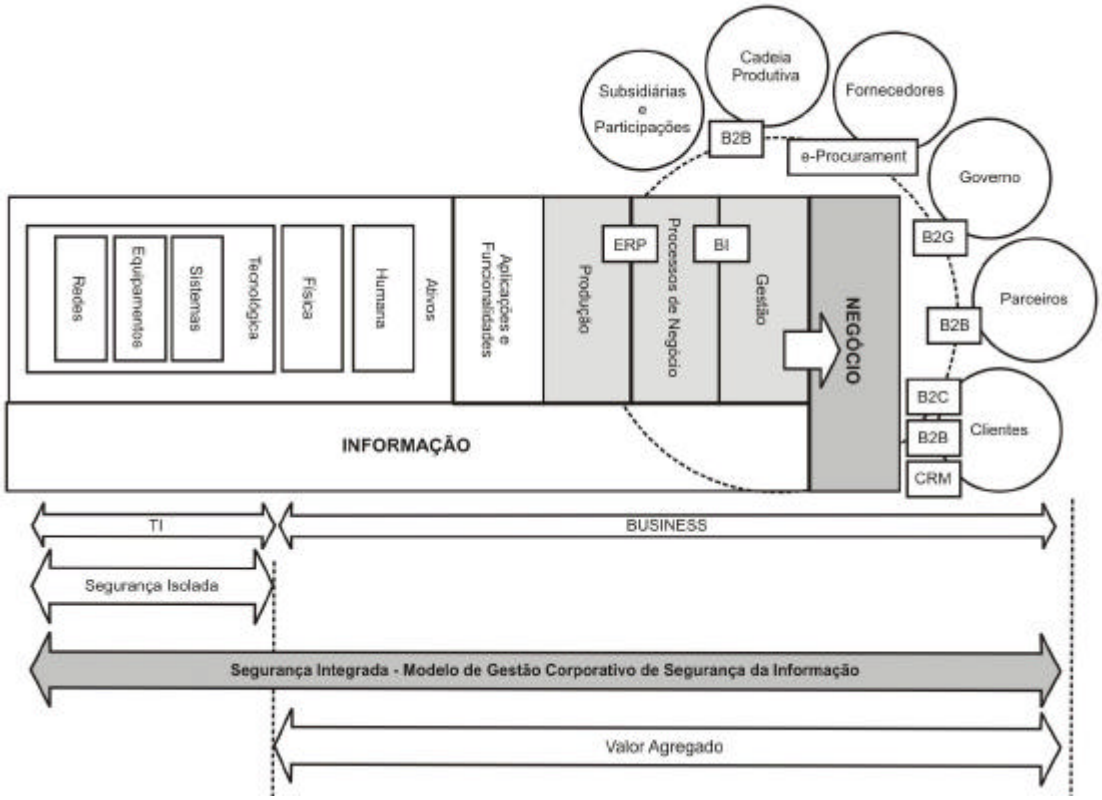
a) gerenciamento de pessoas;
b) foco nos resultados da segurança;
c) gerenciamento de processos;

4.2 Benefícios

O maior benefício visível em uma gestão estratégica de segurança é abranger a corporação como um único objeto, não possibilitando assim investimentos isolados em segurança ou o “ofuscamento” de áreas de risco.

Mas a descrição dos benefícios não é simples, conforme observa OLIVA (2003). Segundo o autor, cabe ressaltar a importância de uma visão global do negócio e do mercado pelos gestores de segurança, uma vez que, normalmente, os projetos de segurança da informação necessitam de aprovação da alta administração. Já que, em segurança, o cálculo do retorno sobre o investimento (ROI) é de difícil quantificação, se faz necessária a percepção e o entendimento das relações existentes com a estratégia competitiva e com a continuidade do negócio, para uma melhor argumentação de viabilidade do mesmo. Além disso, a estratégia de segurança da informação deve estar alinhada aos objetivos estratégicos definidos pela organização, uma vez que ela dá suporte e sustentação à estratégia competitiva, protegendo os ativos críticos da informação, minimizando riscos operacionais, controlando o ambiente organizacional e dando proteção à vantagem competitiva.

Sêmola tenta descrever o valor agregado (benefícios) de uma gestão integrada na ilustração seguinte:



Fonte: SÊMOLA (2003, p. 37)

Na ilustração visualizamos o valor agregado referido quando se possui uma gestão estratégica. Fica evidente o foco no negócio (*Business)* e a abrangência em toda cadeia produtiva.

4.3 Requisitos

Para se administrar estrategicamente a segurança corporativa devem ser atendidos alguns requisitos, que, sem eles, fica praticamente impossível gerar resultados. ABNT (2003, p. 2) cita três fontes principais dos requisitos de segurança:

A primeira fonte é derivada da avaliação de risco dos ativos da organização. Através da avaliação de risco são identificadas as ameaças aos ativos, as vulnerabilidades e sua probabilidade de ocorrência é avaliada, bem como o impacto potencial é estimado.

A segunda fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender.

A terceira fonte é o conjunto particular de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

FONTES (2001) ressalta que a área de segurança deve ser um elemento formal no organograma da empresa. Não é algo passageiro e nem deve ser algo informal. A informalidade não ajuda em nada quando se trata de dedicar recursos. A existência da Segurança da Informação como um elemento da estrutura organizacional, compatível com o porte e negócio da empresa, demonstra a seriedade do assunto para a organização.

Conforme podemos concluir, a área de segurança deve ser formalizada pela empresa, inserindo-a no *board* empresarial. Isto implica também que devem ser alocados recursos para desempenhar tal função.

4.4 Escopo

O escopo da gestão estratégica é bem amplo e visa a definir em linhas gerais como a segurança será tratada dentro da organização, baseadas em um plano diretor. BAIENSE (2003 p.18) coloca que, no plano diretor, os executivos

vão definir uma estratégia de segurança, baseados nos desafios do mercado, nos planos de curto, médio e longo prazo e nas novas demandas apontadas no Business Plan. Para isto, os gestores devem fazer um cuidadoso levantamento dos processos de negócio, identificando aqueles que têm maior impacto financeiro e estratégico sobre as operações da empresa.

A idéia, nesta fase, é mapear a relevância dos processos de negócio, a sensibilidade de cada um deles à quebra de segurança, a prioridade na resolução de problemas e as aplicações, infra-estrutura física, tecnológica e humana que suporta cada um deles. Assim é possível montar um plano indicando os projetos necessários, de acordo com a prioridade identificada.

Segundo o autor, este plano diretor tem como complemento a política de segurança, um guia prático com diretrizes, normas, procedimentos e instruções para cada um dos níveis da operação – estratégico, tático e operacional, conforme descrito anteriormente. Ela vai se ocupar não só dos aspectos de confidencialidade, integridade e disponibilidade da informação, mas também com a conformidade aos requisitos legais, como direito autoral e obrigações contratuais da empresa.

BAIENSE (2003 p.18) afirma ainda que, além de se preocupar com a prevenção, o gestor precisa pensar em como remediar uma situação em que não foi possível evitar o incidente.

4.5 Prestadores de Serviço

As normas e padrões internacionais definem um capítulo à parte para os prestadores de serviços, ou, como dizemos comumente no Brasil, os terceiros da organização.

Segundo ABNT (2003, p. 8), convém que acordos envolvendo o acesso de prestadores de serviços aos recursos de processamento da informação da organização sejam baseados em contratos formais que contenham ou façam referência a todos os requisitos de segurança, para garantir a conformidade com as normas e políticas de segurança da organização. Convém que o contrato garanta que não existam mal-entendidos entre a organização e prestadores de serviços. Convém que as organizações considerem a indenização a ser paga por seus fornecedores em situações de violações de

contrato. ABNT completa que convém que os seguintes termos sejam considerados e incluídos nos contratos:

a) a política geral sobre segurança da informação;

b) proteção dos ativos, incluindo:

- procedimentos para proteção dos ativos da organização, incluindo informação e *software*;
- procedimentos para determinar se houve algum comprometimento destes ativos, por exemplo se houve perda ou modificação de dados;
- controles para garantir a devolução ou destruição das informações e ativos em um determinado momento durante ou no final do contrato;
- integridade e disponibilidade;
- restrições relacionadas com a cópia e divulgação da informação;

c) descrição de cada serviço que deve estar disponível;

d) níveis de serviço desejados e não aceitáveis;

e) condições para transferência da equipe de trabalho, onde for apropriado;

f) as respectivas obrigações dos envolvidos no acordo;

g) responsabilidades com aspectos legais, por exemplo leis de proteção de dados, especialmente levando em consideração diferenças nas legislações vigentes se o contrato envolver a cooperação com organizações de outros países;

h) direitos de propriedade intelectual e direitos autorais e proteção de qualquer trabalho colaborativo;

i) acordos de controle de acesso, abrangendo:

- métodos de acesso permitidos e controle e uso de identificadores unidos como ID e senhas de acesso;
- processo de autorização para acesso e privilégios para os usuários;
- requisitos para manter uma lista de usuários autorizados a usar os serviços disponibilizados e quais são seus direitos e privilégios;

j) definição de critérios de verificação do desempenho, sua monitoração e registro;

k) direito de monitorar e revogar as atividades de usuários;

l) direito de auditar as responsabilidades contratuais ou ter a auditoria executada por prestadores de serviço;

m) estabelecimento de um processo escalonável para a resolução de problemas; convém que também sejam considerados procedimentos de contingência, onde apropriados;

n) responsabilidades envolvendo a instalação e manutenção de *hardware* e *software*;
o) registros com estrutura clara e formato preestabelecido;
p) procedimentos claros e específicos para gerenciamento de mudanças;
q) quaisquer controles de proteção física e mecanismos necessários para garantir que tais controles estão sendo seguidos;
r) treinamento de administradores e usuários em métodos, procedimentos e segurança;
s) controles que garantam proteção contra *software* malicioso;
t) requisitos para registro, notificação e investigação de incidentes e violações da segurança;
u) envolvimento de prestadores de serviços com subcontratados.

4.6 Gerência da Continuidade

Os controles visam a gerenciar a continuidade dos processos de segurança da informação, dando base para uma auditoria e um acompanhamento quantitativo de quão segura a empresa está.

Segundo ABNT (2003, p. 2), os controles considerados como melhores práticas para a segurança da informação incluem:
a) documento da política de segurança da informação;
b) definição das responsabilidades na segurança da informação;
c) educação e treinamento em segurança da informação;
d) relatório dos incidentes de segurança;
e) gestão da continuidade do negócio.

ABNT (2003, p. 2) ainda coloca alguns controles considerados essenciais para uma organização, sob o ponto de vista legal:
a) proteção de dados e privacidade das informações pessoais;
b) salvaguarda de registros organizacionais;
c) direitos de propriedade intelectual.

Já SÊMOLA (2003, p. 73) cita exemplos de ferramentas metodológicas:
a) formulário para mapeamento de vulnerabilidades;
b) formulário para mapeamento de processos de negócio críticos;
c) formulário para orientação na condução de entrevistas;

d) planilha para identificação de ativos físicos, tecnológicos e humanos;
e) planilha para estudo de sensibilidades à quebra de segurança;
f) instrumento para mapeamento topológico;
g) matriz de criticidade para priorização de ações;
h) matriz de tolerância à paralisação

KOVACICH (1998, p. 128) enfatiza o que deve ser levado em consideração na construção dos controles:

a) Por que coletar estas estatísticas?
b) Quais estatísticas específicas deverão ser coletadas?
c) Como coletar as estatísticas?
d) Quando coletar as estatísticas?
e) Quem coletará as estatísticas?
f) Onde (qual ponto do processo) as estatísticas serão coletadas?

KOVACICH (1998, p. 130) ainda expõe que deve-se ter em mente que a utilização de métricas e controles é uma ferramenta para suporte à decisão, mas não são perfeitas. Entretanto podem ser utilizadas como estatísticas para a tomada de decisão, auxiliando com ações bem informadas gerando decisões bem informadas.

4.7 Auditoria

Nenhum controle ou métrica definida pela organização tem valor se não há uma auditoria periódica pelo menos por amostragem em torno deles.

ABNT (2003, p. 51) ressalta que convém que sistemas de informação sejam periodicamente verificados em sua conformidade com as normas de segurança implementadas. Verificação de conformidade técnica envolve a análise dos sistemas operacionais para garantir que controles de *hardware* e *software* foram corretamente implementados. Esse tipo de verificação de conformidade requer a assistência de técnicos especializados. Convém que sejam executados manualmente (auxiliado por funções de *software* apropriadas, se necessário) por um engenheiro de sistemas experiente ou por funções de *software* que gerem relatórios técnicos para interpretação subseqüente por um técnico especialista.

Verificação de conformidade também engloba, por exemplo, testes de invasão, que podem ser executados por especialistas independentes contratados especificamente para este fim. Isto pode ser útil na detecção de vulnerabilidades do sistema e na verificação de quanto os controles são eficientes na prevenção de acessos não autorizados devido a estas vulnerabilidades. Convém que cuidados sejam tomados em testes de invasão cujo sucesso pode levar ao comprometimento da segurança do sistema e inadvertidamente explorar outras vulnerabilidades.

4.8 Norma e Metodologia

Conforme citações anteriores, já há normas internacionais no mercado ditando como devem ser feitos os controles de segurança, mas o mais importante é garantir que uma metodologia seja aplicada, de acordo com os interesses da empresa. Sêmola descreve a diferença entre norma e metodologia no texto a seguir:

> "O fato de já existirem normas nacionais e internacionais – apesar de estarem em estágio de absorção e amadurecimento – que rezem sobre o código de conduta para o gerenciamento da segurança da informação, não soluciona por completo o desafio que as empresas enfrentam. Isso acontece porque a norma tem o nítido papel de apenas apontar os aspectos que merecem atenção, indicando O QUE fazer para o adequado gerenciamento, sem, no entanto, indicar com precisão metodológica COMO se devem realizar as atividades". SÊMOLA (2003, p 72).

CARUSO, Carlos (2002) enfatiza que embora a empresa tenha despendido esforços para implantar alguns itens, esses não estejam de acordo, far-se-á necessária uma revisão total dos processos, contando com um diagnóstico inicial, um projeto de adequação e com o desenvolvimento de mecanismos de controle. De qualquer forma, esteja ou não implantada a segurança de forma adequada, essas normas trarão uma oportunidade de uma revisão abrangente no âmbito empresarial. Além disso, podemos concluir que essa análise consumirá recursos e exigirá pessoas experientes nesse trabalho, o que tende a causar uma grande procura pelo mercado de profissionais gabaritados e conhecedores das normas mencionadas.

4.9 Comitê Estratégico de Segurança

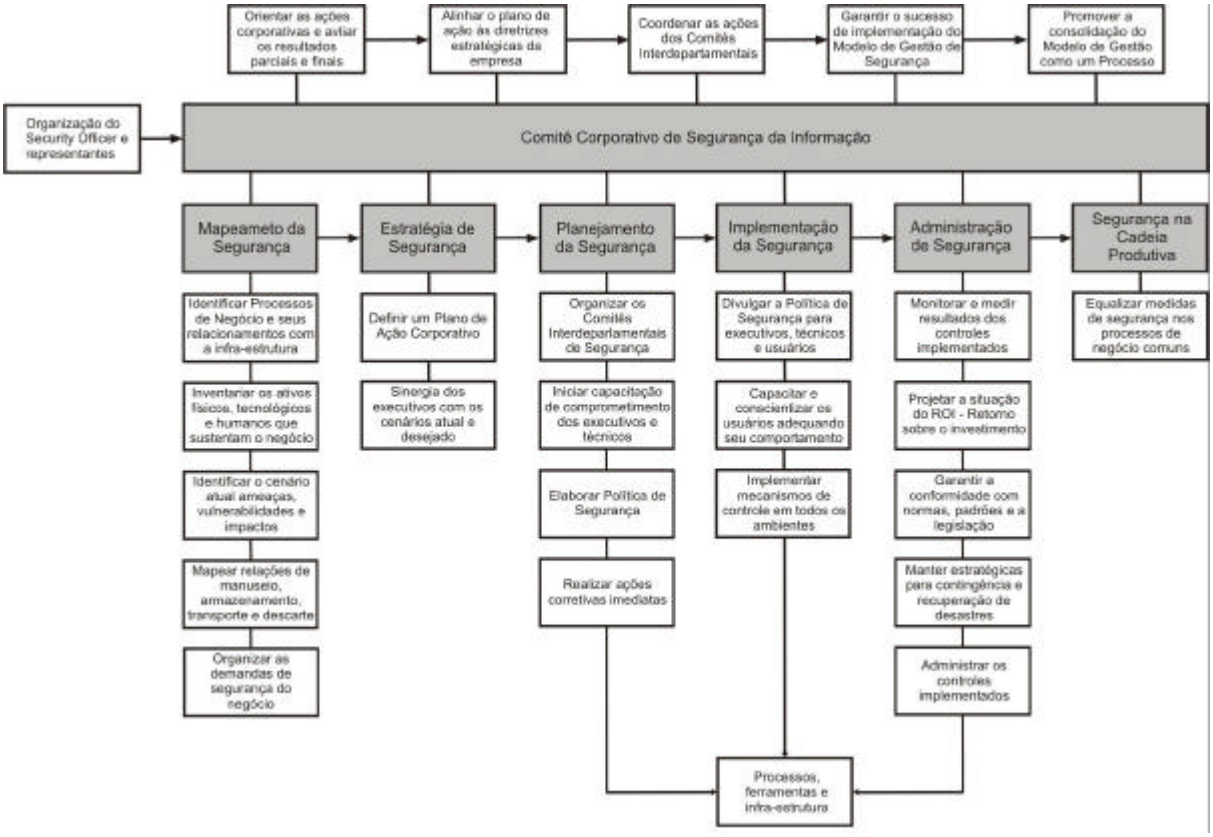
Vários autores apontam como imprescindível a criação de um comitê estratégico de segurança, onde deverão ser definidas todas as questões relativas à política de segurança, sobretudo os casos omissos, entre outros objetivos.

> “A segurança da informação é uma responsabilidade de negócios compartilhada por todos os membros da equipe da direção. Convém que seja considerada a criação de um fórum de gestão para garantir um direcionamento claro e um suporte de gestão visível dos envolvidos para as iniciativas de segurança. Convém que esse fórum promova a segurança dentro da organização através do comprometimento apropriado e dos recursos adequados. O fórum pode ser parte de um corpo administrativo existente” ABNT (2003, p. 5).

ABNT (2003, p. 5) define a responsabilidade do comitê de segurança:

a) análise crítica e aprovação da política da segurança da informação e das responsabilidades envolvidas;
b) monitoração das principais mudanças na exposição dos ativos das informações às principais ameaças;
c) análise crítica e monitoração de incidentes de segurança da informação;
d) aprovação das principais iniciativas para aumentar o nível da segurança da informação.

Sêmola tenta descrever todos os processos tangentes ao comitê na figura seguinte:



Fonte: SÊMOLA (2003, p. 32)

Na ilustração podemos concluir os objetivos do comitê:

a) Orientar as ações corporativas e avaliar os resultados parciais e finais, onde fica claro a supervisão do comitê quanto à operacionalidade da segurança;
b) Alinhar o plano de ação às diretrizes estratégicas da empresa, no qual mostra o vínculo estreito entre o negócio e às estratégias de segurança;
c) Coordenar as ações dos comitês interdepartamentais, em que Sêmola propõe que sejam divididas as responsabilidades entre departamentos;
d) Garantir o sucesso da implementação do Modelo de Gestão da Segurança, que conseguiremos fazer por meio de auditorias periódicas;
e) Promover a consolidação do Modelo de Gestão como um processo, frisando a necessidade de se criar um único processo de segurança.

CAZEMIER (2003, p. 59), em uma decomposição interessante, divide as responsabilidades da segurança entre duas funções: *Security Manager* e *Security Officer*. A primeira, segundo ele, tem a função do gerenciamento do processo de segurança internamente na área e a segunda com as seguintes responsabilidades externas à área:

- agir como um intermediário entre o *Security Manager* e o negócio;

- coordenar a comunicação no caso de incidentes de segurança (específicos);
- coordenar as medidas de segurança a ser implementadas pelo “lado do usuário”;
- atuar como intérprete da política de segurança e como intermediário entre a política e as unidades de negócio.

Para que se cumpram os objetivos da função do *Security Officer*, SÊMOLA (2003, p. 60) sugere um modelo que descreva a estrutura, funções e responsabilidades do comitê:

a) Coordenação Geral de Segurança:

- Mobilizar corporativamente as áreas associadas;
- Deliberar medidas e contramedidas corporativas;
- Definir índices, indicadores e metas estratégicas.

b) Coordenação de Segurança:

- Coordenar as subfunções do Coordenador Geral de Segurança;
- Avaliar os resultados alcançados;
- Propor mudanças;
- Propor medidas e contramedidas;
- Mobilizar os gestores críticos associados.

c) Planejamento e Avaliação:

- Elaborar relatórios gerenciais sobre os resultados alcançados;
- Elaborar propostas de projetos específicos de segurança;
- Promover palestras de conscientização e manutenção do conhecimento;
- Apoiar consultivamente o Coordenador Geral.

d) Controle:

- Conduzir ações de auditoria e monitoramento;
- Analisar métricas dos índices e indicadores;
- Realizar análises de risco;
- Treinar a função de Execução no manuseio dos índices e indicadores.

e) Execução:

- Cumprir e fazer cumprir a Política de Segurança nos ambientes associados;
- Informar à função Controle os resultados dos índices e indicadores;
- Responder a questões de auditoria;
- Registrar ocorrências de quebra de segurança reportando-as à função Controle;
- Executar medidas e contramedidas de segurança.

Para que o comitê, em termos práticos, tome decisões a respeito dos processos da empresa, fica claro que esse comitê deve ser independente, com recursos alocados e permaneça em uma área de *staff* à diretoria da empresa.

4.10 Resposta aos Incidentes de Segurança

Os incidentes de segurança (ocorrências de alguma violação de segurança) devem ser controlados para serem respondidos e mitigados em tempo hábil.

ABNT (2003, p. 12) defende o registro de incidentes de segurança e expõe o objetivo de minimizar os danos originados pelos incidentes de segurança e mau funcionamento e monitorar e aprender com tais incidentes.

A associação enfatiza também que convém que todos os funcionários e prestadores de serviço estejam conscientes dos procedimentos para notificação dos diversos tipos de incidentes (violação da segurança, ameaças, fragilidades ou mau funcionamento) que possam ter impactos na segurança dos ativos organizacionais. Urge que eles sejam solicitados a notificar quaisquer incidentes ocorridos ou suspeitos, tão logo quanto possível, ao ponto de contato designado. É necessário que a organização estabeleça um processo disciplinar formal para tratar com os funcionários que cometam violações na segurança.

Para ser capaz de lidar com os incidentes de forma apropriada, há que se coletem evidências o mais rapidamente possível após a sua ocorrência. Com essa demanda, deve-se possuir uma função específica de resposta aos incidentes em que sejam todos registrados e tratados de forma adequada.

4.11 Fatores Críticos de Sucesso

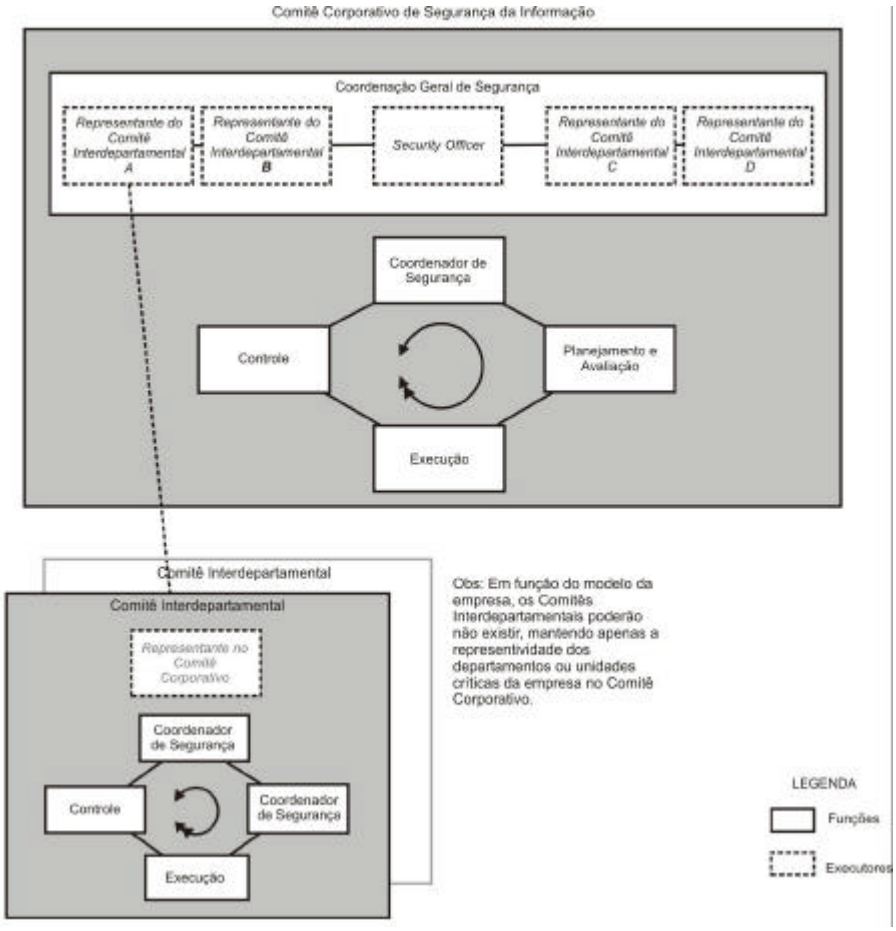
Há alguns fatores que, se não forem observados, podem levar a falhas no processo de segurança e a um possível descrédito da gestão por parte dos colaboradores da empresa.

> “Muitos sistemas de informação não foram projetadas para serem seguros. A segurança que pode ser alcançada por meios técnicos é limitada e convém que seja apoiada por gestão e procedimentos apropriados. A identificação de quais controles convém que sejam implantados requer planejamento cuidadoso e atenção aos detalhes. A gestão da segurança da informação necessita, pelo menos, da participação de todos os funcionários da organização. Pode ser que seja necessária também a participação de fornecedores, clientes e acionistas. Consultoria externa especializada pode ser também necessária.” ABNT (2003, p. 2).

ABNT (2003, p. 2) aponta de forma direta os fatores críticos de sucesso para a implementação da segurança da informação dentro de uma organização:

a) política de segurança, objetivos e atividades que reflitam os objetivos do negócio;
b) um enfoque para a implementação da segurança que seja consistente com a cultura organizacional;
c) comprometimento e apoio visível da direção;
d) um bom entendimento dos requisitos de segurança, avaliação e gerenciamento do risco;
e) divulgação eficiente da segurança para todos os gestores e funcionários;
f) distribuição das diretrizes sobre as normas e política de segurança da informação para todos os funcionários e fornecedores;
g) proporcionar educação e treinamento adequados;
h) um abrangente e balanceado sistema de medição, que é usado para avaliar o desempenho da gestão de segurança da informação e obtenção de sugestões para a melhoria.

SÊMOLA (2003, p. 61), em figuras, acrescenta que os controles da segurança devem ser feitos de forma departamental, seguindo as diretrizes do comitê de segurança:



Fonte: SÊMOLA (2003, p. 61)

Não há uma forma padrão para se inserir no organograma da empresa o departamento de segurança. Existem somente algumas funções descritas que devem ser exercidas dentro da empresa. Quanto maior o poder no organograma, maior a efetividade das ações decorridas deste departamento.

Não existe uma fórmula para que se construa uma segurança eficiente, mas estes fatores críticos de sucesso podem servir de base para todas as políticas a serem desenvolvidas.

5 CONCLUSÕES

Realizar um estudo abrangente com uma visão estratégica da forma que melhor se conduz um processo de segurança da informação organizacional é, sem dúvida, enriquecedor. Conhecer profundamente as formas de proteção utilizadas atualmente e tentar identificar seus pontos falhos visando a uma melhora em cada um deles seria uma enorme pretensão possivelmente jamais alcançada. Essas formas de proteção já possuem uma extensa literatura disponível no mercado. A experiência adquirida com os meios de proteção trouxe à tona algumas questões relevantes e nos possibilitou identificar conflitos entre autores, cada um com vantagens e desvantagens distintas.

A exposição superficial das formas de proteção conduziu-nos a uma abordagem, conforme esperado, holística e conseqüentemente a uma definição do modelo de gestão da segurança da informação. A intenção foi definir diretrizes a serem aplicadas a cada empresa, seguidas de um extenso estudo particular sobre a forma de implantação.

A falta de literatura com pressupostos teóricos e a recente “explosão” de textos sobre o assunto nos levou a utilizar uma bibliografia baseada em poucos livros e alguns artigos de revista, mas devido à redundância de informações foi possível confirmar alguns itens considerados essenciais ao desenvolvimento do trabalho. Algumas normas internacionais ajudaram concretizando a real necessidade de uma gestão integrada.

Conseguimos descrever, embora indiretamente, o escopo, objetivo e benefícios da segurança da informação corporativa em um contexto mais amplo, e demonstramos muito pouco o que já está sendo feito no Brasil e no mundo, pois a literatura encontrada era demasiadamente teórica. Mas foi possível citar várias formas de controle para a redução do risco. Porém a forma de condução dos meios de proteção baseadas em uma gestão estratégica foi bem exemplificada.

As formas de proteção citadas, como classificação da informação, política de segurança e plano de continuidade de negócios, confirmaram a abrangência do escopo da segurança corporativa e o porquê da necessidade da gestão estratégica ao longo de todo o processo, pela sua abrangência e

complexidade. A análise de risco evidenciou igualmente a política estratégica conforme apresentada.

Em nossa opinião, grandes benefícios podem ser atingidos com uma gestão estratégica de segurança da informação. Demonstrou-se que sem esta chamada gestão estratégica pouco se pode aproveitar das formas de proteção, pois em sua maioria dizem respeito à corporação como um objeto único. Todas as formas de proteção citadas visam a um ganho significativo para a organização, e, se não representarem ações corporativas, suas vantagens são mínimas.

A palavra estratégica deve ser utilizada para que se consiga estabelecer metas de curto, médio e, principalmente, longo prazo. Sem uma visão do mercado pouco poderemos definir para a área de segurança, e se não houver um comprometimento de todos os esforços podem ser em vão.

Esperamos que, com este trabalho, gestores empresariais possam mudar o foco de atuação da segurança em suas corporações, visualizando o problema de forma globalizada, não gastando recursos desnecessários tampouco diminuindo os recursos com segurança.

6 BIBLIOGRAFIA

ABNT. **NBR ISO/IEC 17799: Tecnologia da Informação – Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2003.

ABNT. **NBR 11515: Critérios de Segurança Física Relativos ao Armazenamento de Dados – Procedimento**. Rio de Janeiro: ABNT, 2001.

BAIENSE, Carla. Risco Gerenciado. **e-Manager**. nº 39, p. 14-17. São Paulo: TB Editora, mai. 2003.

BAIENSE, Carla. Risco Calculado. **e-Manager**. nº 38, p. 16-20. São Paulo: TB Editora, abr. 2003.

BAIENSE, Carla. Siga os Líderes. **e-Manager**. nº 38, p. 21. São Paulo: TB Editora, abr. 2003.

CAMPANA, Carlos. Segurança: Você se Preocupa com Isso?. **NewsGeneration**. v. 1, n. 1, p. 1-3. São Paulo, 30 mai. 1997. Disponível em: <http://www.rnp.br/newsgen/9705/n1-3.html>. Acesso em: 07 abr. 2004.

CARUSO, Carlos. **Gestão da Segurança da Informação**. São Paulo, 6 mar. 2002. Disponível em: <http://www.securenet.com.br/artigo.php?artigo=112>. Acesso em: 7 abr. 2004.

CAZEMIER, Ing. Jacques e A., OVERBEEK, *et al*. **ITIL – Security Management**, Londres: The Stationery Office, 2003.

FONTES, Edison. **Segurança da Informação:** Investimento ou Custo Operacional?. São Paulo, 9 nov. 2001. Disponível em: <http://www.securenet.com.br/artigo.php?artigo=108>. Acesso em: 7 abr. 2004.

ITGI – IT Governance Institute, **COBIT® Framework.** EUA: ISACA, 2000.

KOVACICH, Gerald L. **Information Systems Security Officer's Guide**. EUA: HB, 1998.

MARTINS, José Carlos Cordeiro. **Gestão de Projetos de Segurança da Informação**. Rio de Janeiro: Brasport, 2003.

McCARTHY, Mary Pat. **Transformação na Segurança Eletrônica**. São Paulo: Pearson Education do Brasil, 2003

MENEGOTTO, Victor Hugo. **O Poder da Análise de Riscos:** A análise que pode alavancar grandes investimentos na área de TI. São Paulo, 10 set. 2003. Disponível em: <http://www.axur.com.br/artigo.php?id=64>. Acesso em: 7 abr. 2004.

MITNICK, Kevin D. **A Arte de Enganar**. São Paulo: Pearson Education do Brasil, 2003.

MOREIRA, Stringasci Nilton. **Segurança Mínima:** uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

NBSO - NIC BR Security Office. **Estatísticas dos Incidentes Reportados ao NBSO**. Brasília, 10 set. 2003. Disponível em: <http://www.nbso.nic.br/stats/>. Acesso em: 13 out. 2003.

OLIVA, Rodrigo Polydoro. **Política de Segurança Como Estratégia Competitiva**. São Paulo, 8 ago. 2003. Disponível em: <http://www.secline.com.br/view_inpress.asp?codmateria=120>. Acesso em: 7 abr. 2004.

PALMA, André. **Classificação de Informações:** Além da Confidencialidade. São Paulo, 6 abr. 2004. Disponível em: <http://www.axur.com.br/artigo.php?id=70>. Acesso em: 7 abr. 2004.

PRADO, Larissa. **Quatro Passos no Gerenciamento de Riscos**. São Paulo, 12 mar. 2002. Disponível em: <http://www.securenet.com.br/artigo.php?artigo=114>. Acesso em: 7 abr. 2004.

PROJECT MANAGEMENT INSTITUTE. **A Guide to the Project Management Body Of Knowledge (PMBOK® Guide)**. EUA: Automated Graphic Systems, 2000.

RAMOS, R. R. **Calculando o ROI em Projetos de Segurança da Informação**. São Paulo, 19 dez. 2001. Disponível em: <http://www.axur.com.br/artigo.php?id=39>. Acesso em: 7 abr. 2004.

RAMOS, R. R. **Análise de Risco:** O que se diz, o que se faz, e o que realmente é. São Paulo, 11 mai. 2002. Disponível em: <http://www.axur.com.br/artigo.php?id=41>. Acesso em: 7 abr. 2004.

RAMOS, R. R. **O Fator Humano na Segurança da Informação**. São Paulo, 26 abr. 2002. Disponível em: <http://www.axur.com.br/artigo.php?id=40>. Acesso em: 7 abr. 2004.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**. Rio de Janeiro: Campus, 2003.

SNHNEIDER, Charles. **Desmistificando a Continuidade do Negócio:** Uma análise do cenário brasileiro. São Paulo, 2 out. 2003. Disponível em: <http://www.axur.com.br/artigo.php?id=65>. Acesso em: 7 abr. 2004.