FACULDADE DE TECNOLOGIA E CIÊNCIAS SOCIAIS APLICADAS – FATECS
CURSO: ADMINISTRAÇÃO
ÁREA: TECNOLOGIA DA INFORMAÇÃO
PROFESSORA ORIENTADORA: MARIÂNGELA ABRÃO

Segurança da Informação nas Organizações

Rodrigo de Oliveira Carvalho
RA: 2040083/5

Brasília, Junho de 2009

RODRIGO DE OLIVEIRA CARVALHO

Segurança da Informação nas Organizações

Trabalho apresentado à Faculdade de Tecnologia e Ciências Sociais Aplicadas, como requisito parcial para a obtenção ao grau de Bacharel em Administração do UniCEUB – Centro Universitário de Brasília
Profa. Orientadora: MSc. Mariângela Abrão

Brasília, Junho de 2009

Carvalho, Rodrigo de Oliveira
Segurança da informação nas organizações / Rodrigo de Oliveira Carvalho. - - Brasília: UniCEUB, 2009.
39 f. : il. ; 29,7 cm.
Orientadora: MSc Mariângela Abrão
TCC (graduação) – Centro Universitário de Brasília, FATECS, Administração, 2009.
1. Segurança da Informação. 2. Política de Segurança da Informação. 3. Security Officer. 4. CSO. 5. NBR ISO/IEC 27001. I. Abrão, Mariângela. II. UniCEUB, FATECS, Graduação em Administração. III.Título.

RODRIGO DE OLIVEIRA CARVALHO

Segurança da Informação nas Organizações

Trabalho apresentado à Faculdade de Tecnologia e Ciências Sociais Aplicadas, como requisito parcial para a obtenção ao grau de Bacharel em Administração do UniCEUB – Centro Universitário de Brasília
Profa. Orientadora: MSc. Mariângela Abrão

Brasília, Junho de 2009

Banca Examinadora

_____
Profª. Mariângela Abrão, MSc.
Orientadora

_____
Prof(a) _____
Examinador(a)

_____
Prof(a) _____
Examinador(a)

A Deus.

“E vos vivificou, estando vós mortos em ofensas e pecados. Em que noutro tempo andastes segundo o curso deste mundo, segundo o príncipe das potestades do ar, do espírito que agora opera nos filhos da desobediência. Entre os quais todos nós também antes andávamos nos desejos da nossa carne, fazendo a vontade da carne e dos pensamentos; e éramos por natureza filhos da ira, como os outros também. Mas Deus, que é riquíssimo em misericórdia, pelo seu muito amor com que nos amou. Estando nós ainda mortos em nossas ofensas, nos vivificou juntamente com Cristo (pela graça sois salvos). E nos ressuscitou juntamente com ele e nos fez assentar nos lugares celestiais, em Cristo Jesus” (Efésios 2.1-6).

AGRADECIMENTO

Aos meus pais que, apesar de todos os percalços, não desistiram de mim.

Aos amigos Dimitri, Juliano e Antônio Carlos, que me ajudaram na confecção deste trabalho.

Às amigas Flavia e Janne, pelo apoio e intercessão constantes.

Aos mestres, devido sua paciência e doação. Em especial aos professores Mariângela Abrão e Homero Reis, a quem também posso chamar de amigos.

“Porque brotará um rebento do tronco de Jessé, e das suas raízes um renovo frutificará. E repousará sobre ele o Espírito do SENHOR, o espírito de sabedoria e de entendimento, o espírito de conselho e de fortaleza, o espírito de conhecimento e de temor do SENHOR”. (Isaías, 11.1-2)

RESUMO

Esta pesquisa visou melhorar a compreensão, por parte do Administrador de empresas, da realidade da Segurança da Informação. O objetivo não foi propor melhores princípios ou práticas para a proteção dos ativos de informação da organização. A proposta foi de metodologia mais clara, de forma que o Administrador – gerente e/ou executivo – que deve participar do processo de Segurança da Informação, compreendesse melhor todo o processo. O trabalho provocou o Administrador e o CSO a ampliarem suas competências imediatas, de forma a tornar toda a rotina conhecida. Em nenhum momento houve a intenção de que as partes envolvidas dominassem detalhes da Política de Segurança da Informação ou mesmo do Sistema de Gestão de Segurança da Informação. Entretanto, para a efetiva implementação, tanto da Política, quanto do Sistema, faz-se necessário o conhecimento e comprometimento de toda sua estrutura. Nenhum passo para o desenvolvimento da Política e do Sistema foi omitido ou mesmo simplificado. Esperou-se que, com abordagem menos técnica, houvesse melhor inserção e atuação do Administrador em todo seu processo. É claro que a cultura organizacional precisa ser alcançada e atualizada para a realidade onde a base é a tecnologia de forma que se compreendam os aspectos da gestão de risco, integre-se a visão técnica com a visão do negócio e se alcance as melhores definições e abrangências dos profissionais envolvidos. A pesquisa, bibliográfica, deu ênfase à literatura renomada e atual mas, infelizmente, não foi implementada na prática. O trabalho baseou-se na norma NBR ISO/IEC 27001.

Palavras-chave: Segurança da Informação. Política de Segurança da Informação. Security Officer. CSO. NBR ISO/IEC 27001.

ABSTRACT

This research aimed to improve understanding by the Administrator of companies, the reality of information security. The goal was not proposing principles and best practices to protect the information assets of the organization. The proposed methodology was clear, so that the Administrator – Manager and/or Executive – to participate in the process of Information Security, to better understand the process. The work caused the Administrator and the CSO to broaden their skills immediately in order to make the whole routine known. At no time was the intention of the parties that dominate the Information Security Policy or the Information Security Management System (ISMS). However, for the effective implementation of both Policy and System, it is necessary knowledge and commitment of all its structure. Any step in the development of Policy and the System has been omitted or simplified. It is hoped that with less technical approach, there was better integration and performance of the Administrator in its entire process. It is clear that organizational culture must be obtained and updated to the reality where the base is the technology so that it understands the issues of risk management, to integrate technical vision with the vision of the business and to reach the best settings and range of professionals involved. The research, literature, emphasized current and renowned literature, but unfortunately it was not implemented in practice. The work was based on standard NBR ISO/IEC 27001.

Descriptors: Infosec. Information Security Policy. Information Security Management System. Security Officer. CSO. NBR ISO/IEC 27001.

LISTA DE ILUSTRAÇÕES

Figura 1 Ciclo de vida da informação, 18

Figura 2 Interação entre os componentes básicos, 19

Figura 3 SGSI baseado em PDCA, 25

Figura 4 Fluxo de PSI, 35

Figura 5 Relação empresa e área de tecnologia, 36

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANSI	American National Standards Institute
BSI	British Standards Institution
CEN	Comité Européen de Normalisation
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and related Technology
CSO	Chief Security Officer
ETSI	European Telecommunications Standards Institute
IEC	International Electrotechnical Comission
IEEE	Institute of Electrical and Electronics Engineers
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunications Union,
NIST	National Institute for Standards and Tecnology,
PSI	Política de Segurança da Informação
ROI	Return Over Investiment (Retorno sobre o Investimento)
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança da Informação
SOX	Sarbanes-Oxley Act of 2002
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO 11

2 DESENVOLVIMENTO 13
2.1 Mitigando Riscos 14
2.2 Contextualização 16
2.2.1 O que é Informação 17
2.2.2 Ciclo de Vida da Informação 17
2.2.3 Segurança da Informação 18
2.2.4 Conseqüências da Política de Segurança da Informação 20
2.2.5 CSO, CISO e *Security Officer* 20
2.3 Política de Segurança da Informação 21
2.3.1 Tendências 21
2.3.2 Legislação e Instituições Padronizadoras 22
2.3.3 Normas e Metodologias 23
2.3.4 Antes de definir a PSI 26

3 METODOLOGIA 28

4 DISCUSSÃO 29
4.1 Retorno sobre o Investimento (ROI) 31
4.2 Definindo a PSI baseada na Norma NBR ISO/IEC 27001 32

5 CONSIDERAÇÕES FINAIS 37

REFERÊNCIAS 38

1 INTRODUÇÃO

Desde os primórdios da civilização, antes mesmo da linguagem escrita, a informação era adquirida, tratada, armazenada e transferida entre pessoas. O ser humano vivia determinada situação, tirava conclusões sobre as sensações vividas, pintava em alguma parede ou caverna sua percepção e contava sobre ela. Seja na forma cultural, de geração em geração, seja na forma de instrução, dos mais velhos aos mais novos. E transmissão de informação é cíclico.

Com a invenção da escrita, o tratamento da informação passou a ser mais fidedigno. Também foi possível aumentar sua quantidade porque tinha-se mais acesso e, conseqüentemente, armazenava-se mais informação.

A civilização evoluiu, cada qual à sua maneira, e desenvolveu métodos próprios de superar os obstáculos que surgiam. Com o processo evolutivo, percebeu que o crescimento dependia, também, de conquistas – terra, comida, habitat, ou de prevalecer sobre outros grupos. Às vezes, não se tratava apenas de força, mas técnicas – caça, cultivo, fogo, êxodo, construção, armamento, guerra.

Como as guerras marcaram as grandes evoluções, principalmente tecnológicas, surgiu a necessidade de se definir quem teria acesso a que tipo de informação.

O tratamento da informação como ativo mais importante da organização é decorrente do desenvolvimento da Tecnologia da Informação (TI) e conseqüente desenvolvimento da rede mundial de computadores – *Internet*.

Veiga (2004) afirma que as preocupações relativas à estabilidade e à segurança das redes e dos Sistemas de Informações[1] são inerentes ao seu uso ou demanda. Ou seja, a Internet só será mais utilizada se os níveis de segurança e qualidade dos serviços oferecidos forem maiores. Entretanto, quanto mais a sociedade utilizar a Internet, mais susceptível estará aos riscos – descontinuidade do funcionamento, furto/roubo ou destruição de informação. Para tanto, há o desenvolvimento científico-tecnológico de ferramentas de segurança, além da correta utilização das tecnologias, a fim de diminuir os riscos.

[1] Entende-se por sistema de informação uma infra-estrutura que suporta o fluxo de informação interno e externo a uma organização. Suas funções são receber, armazenar, processar, apresentar e distribuir a informação. (GOUVEIA e RANITO, 2004, p. 24, tradução nossa).

Este desenvolvimento possibilitou às organizações disponibilizar e acessar o maior número possível de informações sobre os clientes, concorrentes, fornecedores, parceiros e seus funcionários. O acesso a estas informações passou a criar diferencial entre as organizações na conquista de mercado e de novos clientes.

Manipular a informação com a devida consideração que merece, disponibilizando-a a qualquer tempo e para quem de direito, protegendo sua integridade contra alterações e roubos, mantendo a confiabilidade sobre a mesma é a preocupação da Segurança da Informação (SI).

O objetivo deste trabalho é descrever o assunto Segurança da Informação e apresentar, de forma simplificada, um Sistema de Gestão de Segurança da Informação (SGSI), de forma que profissionais da área de Administração de empresas compreendam seu processo, sem a necessidade de conhecimentos técnicos aprofundados.

A confecção deste justifica-se com a exploração de um novo viés deste assunto, que deve ser continuamente estudado e atualizado, devido à grande volatilidade das tecnologias envolvidas. Para tanto, identifica-se como problema: É possível tornar a linguagem utilizada nos Sistemas de Gestão de Segurança da Informação de fácil interpretação?.

As características da metodologia adotada e utilizada são: bibliográfica, já que os dados foram pesquisados/coletados em diferentes meios em que o assunto encontra-se publicado; exploratória, porque visa esclarecimento do assunto abordado; e qualitativa, pois trata-se da interpretação de informações técnicas.

O trabalho está dividido em três partes principais. A informação é contextualizada na introdução, o processo de Segurança da Informação e os conceitos inerentes são descritos no desenvolvimento e a conclusão conecta a descrição do processo com sua real implementação, às vistas das normas vigentes.

2 DESENVOLVIMENTO

Com a expansão da rede mundial de computadores – *Internet* – no mundo e do desenvolvimento e melhoria dos processos de comunicação de dados, que facilitam a disponibilização e troca de informações entre pessoas, organizações, filiais, parceiros, fornecedores e clientes, faz-se necessária a adoção de práticas voltadas para a preservação, manutenção e disponibilidade destas. Uma conseqüência é o surgimento diário de novas vulnerabilidades nos sistemas operacionais, aplicativos e ferramentas utilizadas pela *Internet*.

Uma tendência mundial é que toda organização que tenha a informação como um de seus ativos, adote Políticas de Segurança da Informação (PSI) baseadas em normas nacionais e internacionais.

A aplicação de normas de Segurança da Informação agrega valor ao produto ou ao serviço prestado, apesar de não garantir que a organização não esteja susceptível a roubos ou perdas, diminui consideravelmente os riscos das organizações.

Desenvolver e implementar uma Política de Segurança da Informação torna-se necessária para que as organizações disponibilizem mais serviços e informações a seus usuários, de forma confiável, segura, controlada e atualizada.

Para Sêmola (2003, p. 1):

> (...) é inegável o papel fundamental da informação. Em todas as empresas, independente de seu segmento de mercado, *core business*[2] e porte, nas fases de sua existência, sempre fizeram uso da informação, objetivando melhor produtividade, redução de custos, ganho de *market share*[3], aumento de agilidade nos negócios, competitividade e principalmente, apoio à tomada de decisão e gerenciamento dos riscos em função dessas decisões.

O diferencial competitivo está diretamente relacionado com a continuidade do negócio e ligado à forma como a informação é tratada, armazenada, gerida e disponibilizada no momento da realização de negócios numa organização.

---

[2] Entende-se por *core business* a parte central de um negócio ou de uma área de negócios, que é geralmente definido em função da estratégia da organização o mercado, ou seja, é o cerne das atividades do negócio (CERTO, 2003).

[3] Entende-se por *market share* a participação no mercado, a fatia de mercado detida por uma organização. Sua medida quantifica a quantidade do mercado dominado por uma organização (*idem*).

Com isso, houve a necessidade do surgimento de:

(i) Redes internas de computadores e portais de colaboração interna – *Intranets* – para agilizar o acesso às informações, que passaram a ser compartilhadas rapidamente, e descentraliza os processos administrativos e de negócios nas organizações;

(ii) Computadores e dispositivos portáteis (*notebooks* e *pdas*), pois quebra-se o paradigma do acesso local às informações, cuja troca passa a ser instantânea, e pode-se ter acesso em qualquer lugar do mundo, através da *Internet – Extranets, VPNs*.

Simultaneamente, as tecnologias de rede se desenvolvem, ganhando performance e pulverizando mais ainda a informação. A *Internet* passa a representar o principal canal de distribuição de informações, sejam elas internas ou externas. Possibilita também a interligação de organizações (filial e matriz), ambientes, processos e parceiros, que formam a cadeia produtiva das organizações. Prometem melhor planejamento dos processos de negócio, fazendo com que a organização, vislumbre o *digital marketplace*[4], ou seja, as bases de informação dos elementos da cadeia produtiva, como fornecedores, parceiros, clientes e o governo se integram, gerando diferencial de mercado para as organizações envolvidas (DIAS, 2000).

2.1 Mitigando[5] Riscos

Toda e qualquer decisão relacionada à proteção deve ser realizada levando em consideração “o que deve ser protegido”, “o quanto se está sujeito a um problema”, o “quanto vale” e “quanto risco deixa-se de correr após a implementação da medida de proteção”. Contudo, como as metodologias propostas possuem elevado grau de profundidade e a maioria dos profissionais do país não estão preparados para segui-las, além do que, a qualidade da especialização das empresas brasileiras desobriga-os a serem menos especialistas, acarretando na utilização indevida das

[4] Entende-se por *digital marketplace* o mercado baseado na economia digital, ou seja, há exclusivamente a troca de informações e não de itens tangíveis como bens mão-de-obra ou mesmo moeda (ALDRICH, 1999).

[5] À luz da Segurança da Informação, mitigar diz respeito à redução do impacto, enquanto reduzir refere-se à redução da probabilidade de ocorrer um evento (N. A.).

metodologias propostas. Sendo assim, um processo crucial para a tomada de decisões acaba por não ser seguido. (YU, 2002)

Não obstante, a atual realidade brasileira é que os profissionais que atuam no mercado são, normalmente, advindos de TI ou auditoria e, como tais, tendem a ter uma visão estritamente técnica do assunto. Sob essa visão, são capazes de realizar análise de vulnerabilidades e acabam adotando-a como análise de riscos. A falta da variável “o quanto vale” na equação de riscos é sutil, mas é crucial para a compreensão dos reais riscos corridos (SÊMOLA, 2002).

Para aumentar a complexidade do problema, os profissionais de TI tendem a decidir por “fazer segurança por nota fiscal”, que quer dizer, implementar ferramentas tecnológicas de detecção e correção. Esses profissionais de TI não levam em consideração a necessidade de utilizar métodos de prevenção de problemas utilizando processos. Exemplos desses processos são: a análise de pessoas no momento de contratação, a segregação de tarefas, o estabelecimento de políticas e procedimentos de Segurança da Informação, políticas de classificação da informação, a realização de campanhas de divulgação e treinamento, o estabelecimento de métricas, dentre outros (SPAFFORD, 2005, tradução nossa).

Em todas as regulamentações há um fator comum: a qualidade das informações. De acordo com o Código de Boas Práticas da Gestão de Segurança da Informação (NBR ISO/IEC 27002, 2007), as informações estão seguras desde que sejam preservadas a sua:

(i) confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
(ii) integridade: salvaguarda da exatidão e completa da informação e dos métodos de processamento;
(iii) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Quaisquer falhas que comprometam a confidencialidade, a integridade ou a disponibilidade das informações terão reflexo direto no índice de riscos operacionais da empresa (BRASIL, 2006).

A área de Segurança da Informação da empresa deve assumir o compromisso de assegurar as melhores técnicas e práticas a fim de possibilitar o menor risco possível ou mantê-lo em níveis aceitáveis (ABREU, 2007).

Ainda segundo Abreu (2007, p. 51):

> De acordo com a NBR/ISO/IEC 27001, para isso, a área deve utilizar três fontes principais, na ordem:
> 1) A primeira 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.
> 2) A segunda 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.
> 3) 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.

Os resultados na análise do item 1, se não implementado, acarretaram ausência de *Due Dilligence*[6] e/ou *Due Care*[7]. A análise do item 2 é a probabilidade entre a ocorrência e as perdas decorrentes do riscos analisados e o custo do controle a ser implementado. O item 3 refere-se à Política de Segurança da Informação, propriamente dita. Vale ressaltar que a norma NBR ISO/IEC 27001 afirma que os requisitos para efetiva segurança provêm das leis específicas e resultados das análises dos riscos (ABREU, 2007).

Em todo o processo, a análise deve ser orientada pelo profissional de Segurança da Informação, contudo, a responsabilidade pelo resultado final é do gestor da área de negócio, visto ser o único que pode determinar quais seriam os impactos resultantes de um desastre. Este deve ser orientado a prover uma classificação de graus de impacto.

2.2 Contextualização

Já que esta obra destina-se aos profissionais de Administração, faz-se necessária a explanação de terminologia técnica, para fins de tornar mais clara e objetiva as nomenclaturas adotadas. Os termos conceituados são os difundidos e adotados pelos profissionais de Segurança da Informação. Por isso, alguns termos em língua estrangeira serão mantidos, mas sua devida tradução e explicação os seguirão.

---

[6] *Due dilligence* – termo ainda sem tradução precisa para o português que define as análises mínimas que devem ser realizadas em um ambiente para garantir que não houve negligência quanto ao conhecimento deste (N. A.).

[7] *Due care* – termo ainda sem tradução precisa para o português que define os controles mínimos que devem ser realizados em um ambiente para garantir que não houve negligência quanto aos cuidados deste (idem).

2.2.1 O que é Informação

Por informação deve ser entendido, segundo Ramos (2008, p. 287):

> (...) todo patrimônio que se refere à cultura da empresa ou ao seu negócio, podendo tais informações ser de caráter comercial, técnico, financeiro, legal, de recursos humanos, ou de qualquer natureza, que tenha valor para a organização e que se encontrem armazenadas em recursos computacionais da empresa, com tráfego dentro da sua infra-estrutura tecnológica.

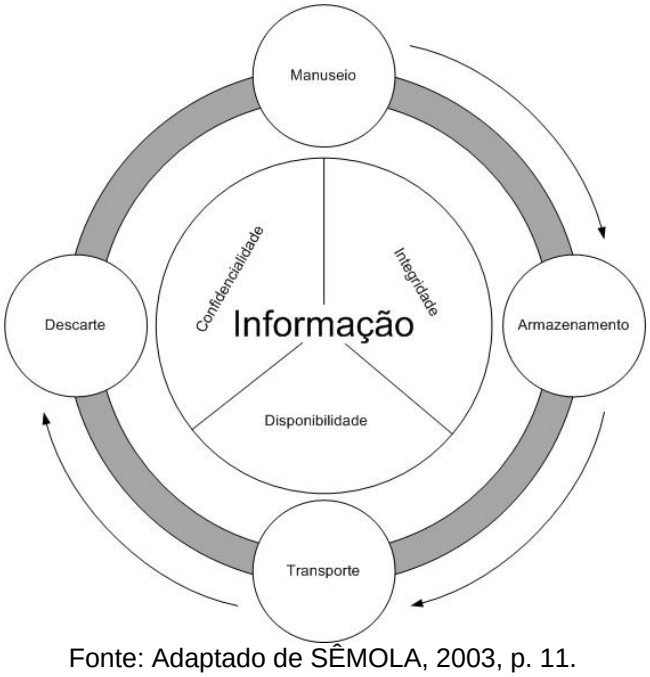
Cabe ressaltar que o termo “dado” é erroneamente utilizado como sinônimo de informação. Dado, nada mais é, do que algo bruto, sem significado individual. Sua manipulação e tratamento resultam na informação (NORTON, 1996).

2.2.2 Ciclo de Vida da Informação

Para melhor entender o objeto da segurança é importante conhecer os momentos que fazem parte do ciclo de vida da informação.

Sêmola (2003) afirma que o ciclo da vida da informação é composto e identificado pelos momentos vividos pela informação e que a colocam em risco. Esses momentos acompanham os ativos físicos, humanos e tecnológicos que fazem uso, alteram ou descartam a informação.

FIGURA 1 – CICLO DE VIDA DA INFORMAÇÃO



Fonte: Adaptado de SÊMOLA, 2003, p. 11.

Os quatro momentos do ciclo de vida da informação, segundo Sêmola (2003) são:

(i) Manuseio.

(ii) Armazenamento.

(iii) Transporte.

(iv) Descarte.

Toda a preocupação com a segurança está focada nestes quatro momentos, para que não haja comprometimento da confidencialidade, integridade e disponibilidade.

2.2.3 Segurança da Informação

Segundo a Norma ABNT NBR ISO/IEC 27002 (2007, p.ix), "a Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

A Segurança refere-se aos ativos de informação[8] da empresa porque é resultado de instrumentos como diretrizes, normas, bens, em conjunto com outros processos da gestão do negócio.

Devem-se diferenciar os ativos da Tecnologia da Informação – *hardware* e *software*, basicamente – dos ativos que fazem parte do escopo da Segurança da Informação. Normalmente, os ativos de TI são equivocadamente avaliados como sendo os mesmos da SI (RAMOS, 2008).

Devido à diversidade dos sistemas, o aumento nos números de usuários e das aplicações, e conseqüente aumento das ameaças, a Segurança da Informação vem se tornando um processo cada vez mais importante dentro das organizações.

Antes de adotar procedimentos de aquisição de sistemas ou equipamentos, faz-se necessária a avaliação do objeto da segurança. Há a necessidade de se verificar o ROI, ou seja, se o valor do investimento é condizente com o ativo que se quer investir.

---

[8] "Ativos de informação são definidos como aqueles que produzem, processam, transmitem ou armazenam informações" (RAMOS, 2008, p.16).

Sêmola (2003) diz que é primordial a análise dos riscos inerentes ao negócio da empresa, para identificação das ameaças e vulnerabilidades. Apenas através desta análise será possível estimar a probabilidade da ocorrência de uma ameaça e qual impacto causará ao negócio.

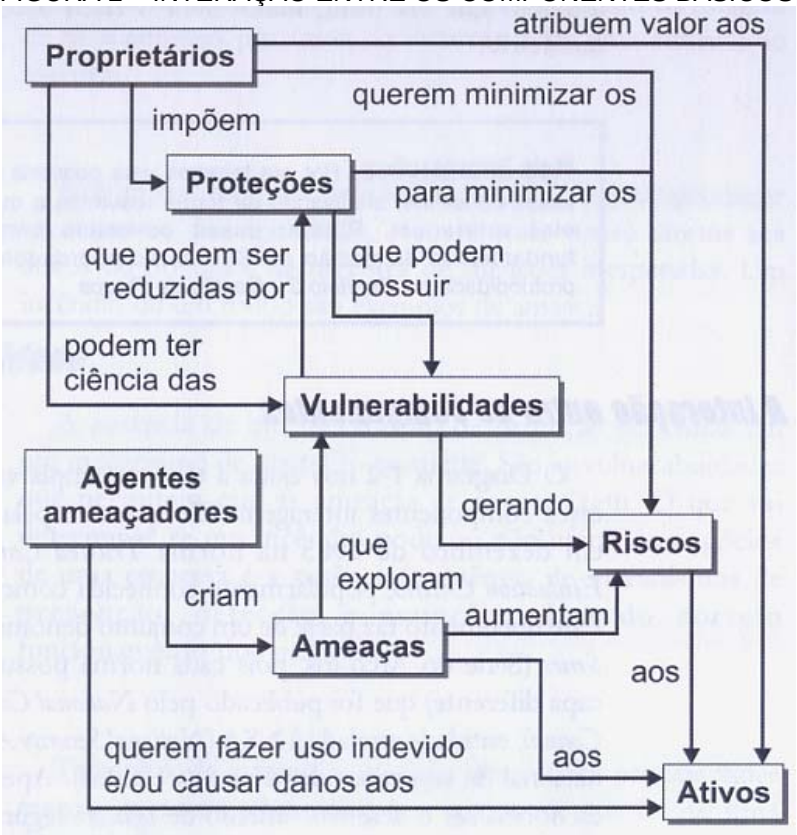
Alguns aspectos devem ser compreendidos a fim de proceder com a correta avaliação de quais riscos ou ameaças à quais a empresa pode estar exposta.

(i) Ameaças: segundo Sêmola (2003), ameaças são possibilidade que podem comprometam as informações e seus ativos.

(ii) Vulnerabilidades: para Sêmola (2003, p.48), “são as fragilidades existentes ou associadas a ativos que processam ou armazenam informações e que, ao serem exploradas por uma ameaça, podem comprometer a Segurança da Informação.”

(iii) Riscos: na visão de Baraldi (2004), riscos são todos os eventos e expectativas que impedem as organizações de atingirem os seus objetivos trazendo possíveis prejuízos financeiros e mesmo outros não tangíveis como a imagem da organização.

FIGURA 2 – INTERAÇÃO ENTRE OS COMPONENTES BÁSICOS



Fonte: RAMOS, 2008, p. 26.

2.2.4 Conseqüências da Política de Segurança da Informação

O fato de haver uma Política de Segurança da Informação já é considerado motivo de sucesso, porque sua elaboração deve estar em consonância com os objetivos e atividades do negócio. Além disso, deve levar em conta a cultura organizacional da empresa, comprometimento e apoio de todos os níveis gerenciais e da alta administração, para que sua implementação seja efetiva e possa contar com devido apoio financeiro.

Divulgar a PSI também é fator essencial e deve alcançar todos os colaboradores, sejam eles gerentes, funcionários ou terceirizados, para que seja efetiva, no todo. Após a formalização da PSI, faz-se necessário treinamento/qualificação, diferenciado para cada grupo para que haja entendimento correto dos requisitos de Segurança da Informação, da análise de riscos e da gestão de riscos.

Com o estabelecimento de um eficiente processo de gestão de incidentes de segurança, aliado à constante medição e aprimoramento de sua gestão – isto é, identificação dos riscos e tratamento de forma sistemática e contínua – é que poderá se tomar decisões levando em consideração os componentes do risco e buscar os objetivos para que as ações garantam para que estes mesmos riscos encontrem-se em patamares aceitáveis.

2.2.5 CSO, CISO e *Security Officer*

Chief Security Officer (CSO), *Chief Information Security Officer* (CISO) e *Security Officer* são as designações do profissional responsável pela Segurança da Informação da empresa. A melhor nomenclatura, em português, para este profissional seria Analista de Segurança.

2.3 Política de Segurança da Informação

A Política de Segurança da Informação (PSI) é um documento produzido pelo *Security Officer* em conformidade com o código de ética da empresa, o conjunto de leis vigentes no país, as melhores práticas e padrões de segurança reconhecidos internacionalmente e a cultura da empresa.

O objetivo da PSI é registrar os princípios e diretrizes da segurança adotadas pela organização, que (deveria) ser seguida por todo seu corpo integrante. Na PSI encontram-se a implementação da Segurança da Informação, a formalização para proteção, controle e monitoramento das informações e dos ativos de informação. Também é na PSI que encontra-se o comprometimento da alta administração com a proteção da informação, o que embasa a colaboração de todos os integrante no ciclo de vida da informação (BEAL, 2005).

Ferreira (2003) define que o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas são compreendidos pelo Sistema de Gerenciamento de Segurança da Informação (SGSI), ou *Information Security Management System (ISMS*). A organização que implemente um SGSI abrangerá os ativos que estão sendo protegidos, o gerenciamento de riscos, os objetivos de controles e controles implementados.

2.3.1 Tendências

As redes de computadores, em especial a Internet, rede pública que conecta milhões de computadores em todo o mundo, chegaram para democratizar o acesso às informações, porém, atrelado a isto, há que se considerar os requisitos de segurança envolvidos neste processo. Neste sentido, é importante que se tenha muito bem definido os critérios para bom uso e proteção das informações. A política de segurança é justamente a formalização destes critérios (KUROSE e ROSS, 2003).

Com o aparecimento do padrão NBR ISO 9000[9], desenvolveu-se entre os empresários a consciência de padronização como diferencial de mercado, gerando mais credibilidade e confiança nas organizações. A Política de Segurança da

[9] A norma NBR ISO 9000 traz parâmetros cujas aplicações objetivam a melhora no desempenho da organização que a adota (N. A.).

Informação também está nesse caminho e é o mais novo movimento no meio corporativo em busca da padronização e conformidade e, conseqüentemente, a certificação com base na NBR ISO/IEC 27001. A tendência é que após as principais organizações do mercado se adaptarem a essa nova norma, as demais empresas também verão e identificarão essa necessidade e se adequarão gradativamente, repassando toda essa necessidade de conformidade para os demais parceiros da cadeia produtiva (SÊMOLA, 2003).

Neste mundo globalizado onde as informações atravessam fronteiras com velocidade espantosa, a proteção do conhecimento é de vital importância para a sobrevivência das organizações. Os negócios passam a ser influenciados diretamente e, uma falha, uma comunicação com informações falsas, um roubo ou uma fraude de informações podem trazer graves conseqüências para a organização, tais como a perda de mercado, de negócios e conseqüentemente, perdas financeiras. Desse modo, informações, infra-estruturas de rede e capital intelectual devem ser protegidos e tratados com a devida importância que merecem. Conhecimento é o principal capital da organização, protegê-lo significa proteger o próprio negócio. Com isso pode-se dizer que atualmente, nos processos de negócio das organizações, a segurança das informações é fundamental (NAKAMURA e GEUS, 2003).

2.3.2 Legislação e Instituições Padronizadoras

Em função da grande importância da segurança de informação na sociedade moderna, vários grupos iniciaram pesquisas que resultaram em padrões de segurança. Há também projetos legislativos que visam o tratamento legal das situações de troca de informações através da Internet, protegendo os direitos da sociedade e definindo sanções legais aos infratores (DIAS, 2000).

As organizações precisam manter-se atualizadas durante todo o processo de implantação da segurança de informações. Elas devem pesquisar as legislações em vigor e em andamento e os padrões de segurança definidos por organismos nacionais e internacionais.

No Brasil é a Associação Brasileira de Normas Técnicas (ABNT) quem estabelece os padrões a serem seguidos por produtos e serviços de várias áreas.

No âmbito internacional, existem outras instituições que também têm a mesma função. Dentre elas, destacam-se, segundo Beal (2005), Ferreira (2003) e Sêmola (2003):

(i) *American National Standards Institute*, ANSI.
(ii) *British Standards Institution*, BSI.
(iii) *Comité Européen de Normalisation*, CEN;
(iv) *European Telecommunications Standards Institute*, ETSI;
(v) *Information Systems Audit and Control Association*, ISACA
(vi) *Institute of Electrical and Electronics Engineers*, IEEE;
(vii) *International Electrotechnical Comission*, IEC;
(viii) *International Organization for Standardization*, ISO;
(ix) *International Telecommunications Union*, ITU;
(x) *National Institute for Standards and Tecnology*, NIST;

2.3.3 Normas e Metodologias

Uma política de segurança é a formalização de todos os aspectos considerados relevantes por uma organização para a proteção, o controle e o monitoramento de seus recursos computacionais e, conseqüentemente, das informações por eles manipuladas. Em outras palavras, de uma forma mais prática, a política de segurança deve contemplar, de forma genérica, todos os aspectos importantes para a proteção lógica e física das informações e dos recursos computacionais.

A existência de normas nacionais e internacionais e o estágio de absorção e amadurecimento destas a respeito dos procedimentos para o gerenciamento da Segurança da Informação, não resolvem inteiramente os problemas das organizações. O problema ocorre porque as normas definem, apontam e determinam apenas o que fazer para o melhor gerenciamento da segurança das informações, não apontando de, forma precisa, como desenvolver essas atividades e procedimentos (SÊMOLA, 2003).

Portanto, de nada adiantará estar ciente dos controles e aspectos apontados por uma norma de segurança, se não for utilizada uma metodologia eficiente, eficaz e condizente, que oriente e transforme as atividades em resultados que reflitam na diminuição dos riscos. À medida que os riscos, as ameaças e os impactos se tornam

mais mensuráveis e representativos, além da percepção mais apurada de que a segurança não mais está limitada à tecnologia, mas abrange também os aspectos físicos e humanos, cresce então o volume de vulnerabilidades encontrado nas organizações. As ações a este respeito se tornaram mais profundas e, com o aumento dos ativos críticos, este processo de análise e gestão ficou ainda mais complexo. Diante disto, adotar uma metodologia passou a ser fator crítico de sucesso, subsidiando a Política de Segurança da Informação nas organizações (NAKAMURA e GEUS, 2003).

A Segurança da Informação e sua política não são resolvidas somente através do desenvolvimento de *softwares* e *hardwares* para a segurança. Sua abrangência vai além. Ela deve ser tratada como um conjunto de mecanismos que, integrados, interage e determina o que deve ser protegido, contra o que será necessária proteção e como será feita essa proteção. Além disso, deve-se também determinar o nível de segurança que se deseja e avaliar a relação custo x benefício. A análise dessa relação consiste em verificar se o investimento para proteger determinado ativo será mais alto do que seu valor para a organização, tornando inviável o investimento.

Dentre essas normas e metodologias, atualmente destacam-se, segundo Beal (2005), Ferreira (2003) e Sêmola (2003):

(i) BS 7799: *British Standard of Information Security Management Systems, parts* 1 *and* 2.

(ii) ISO/IEC 17799: *Information Technology – Code of practice for information security management*.

(iii) ISO/IEC 27001: *Information technology – Security techniques – Information security management systems – Requirements.*

(iv) ISO/IEC 27002: *Information technology – Security techniques – Code of practice for information security management.*

(v) ABNT NBR ISO/IEC 27001: Tecnologia da Informação – Técnicas de Segurança – Sistema Gestão da Segurança da Informação – Requisitos.

(vi) ABNT NBR ISO/IEC 27002: Tecnologia da informação – Técnicas de segurança – Código de práticas para a gestão da segurança da informação.

(vii) SAS70: *Reports on the Processing of Transactions by Service Organizations*.

(viii) SOX (*Sarbanes-Oxley Act of 2002*): *Public Company Accounting Reform and Investor Protection Act of 2002*.

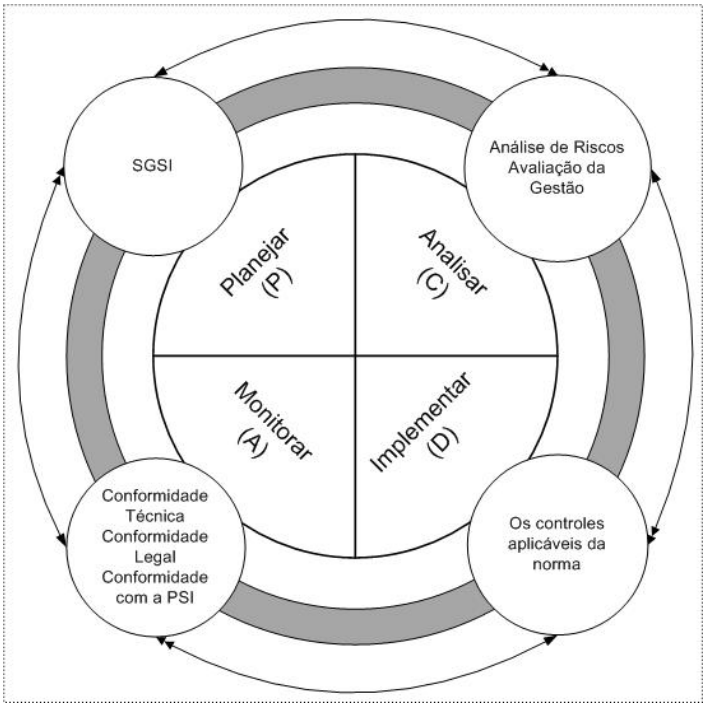
(ix) ITIL: *Information Technology Infrastructure Library*.

(x) COBIT: *Control Objectives for Information and related Technology.*

A história das políticas de Segurança da Informação começa com o BSI (*British Standard Institute*), responsável pela criação da norma BS 7799 Parte 1, em dezembro de 1995. Considerado o mais completo padrão para o gerenciamento da Segurança da Informação no mundo, pode-se implementar com ele um sistema de gestão de segurança baseado em controles e práticas definidos por normas e práticas internacionais. Com sua Parte 1, a BS 7799 se tornou norma oficial da ISO sob o código ISO/IEC 17799. No Brasil, após sua tradução, virou a NBR ISO/IEC 27001.

Já a Parte 2 da BS 7799 foi lançada somente em 1998 e introduz o modelo PDCA (*Plan-Do-Check-Act*), como parte do sistema de gerenciamento, preparando o desenvolvimento e a implementação, e melhorando a eficiência dos Sistemas de Gerenciamento de Segurança das Informações (SGSI) das organizações. A Parte 2 virou, no Brasil, NBR ISO/IEC 27002

FIGURA 3 – SGSI BASEADO EM PDCA.



Fonte: SÊMOLA, 2003, p. 142, adaptado.

Outra norma internacional, muito adotada a partir de 2002 pelas instituições financeiras é a lei Sarbanes-Oxley ou SOX, como também é conhecida. Ela foi aprovada em 2002 pelo congresso americano, como resposta aos grandes escândalos contábeis e financeiros de empresas como Enron, WordCom e Tyco, que abalaram o mercado de capitais. Ela é composta por 1107 artigos e estabelece severas punições para os executivos que burlarem suas determinações, estabelecendo multas de até US$ 5 milhões e prisão de até 20 anos aos infratores. As instituições financeiras são as que mais utilizam essa norma.

2.3.4 Antes de definir a PSI

A Política de Segurança define um padrão de segurança a ser adotado por toda organização, pessoal técnico, gerencial, operacional e usuários internos e externos. É um mecanismo preventivo de proteção dos dados e processos mais importantes de uma organização. Ela deve estabelecer como a manipulação das informações e de seus recursos computacionais será protegida, monitorada e controlada dentro e fora da organização. É importante ainda que a política estabeleça princípios institucionais e responsabilidades para as funções relacionadas com segurança, como também discrimine as principais ameaças, riscos e impactos envolvidos (DIAS, 2000).

Para Nakamura e Geus (2003, p. 171), a Política de Segurança é de suma importância para a organização no tratamento de suas informações, pois:

> (...) é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações. A necessidade de estabelecer uma política de segurança é um fato realçado unanimemente em recomendações provenientes tanto do meio militar (...), como no meio técnico (...), e mais recentemente, no meio empresarial (...).

A informação será sempre o alvo das ameaças e a mesma não está mais confinada somente aos ambientes físicos ou a processos isolados. Ela provê todos os processos de negócio e está em toda a organização, ficando sujeita a várias ameaças, vulnerabilidades e é sensível a impactos específicos. Com o desenvolvimento da tecnologia, as informações ficaram entrelaçadas, compartilhadas e distribuídas num mesmo fluxo, estando sujeitas a vulnerabilidades que agora transcendem os aspectos tecnológicos, sendo alvo também de interferências físicas e humanas (SÊMOLA, 2003).

O desenvolvimento de uma Política de Segurança é o primeiro e o principal passo relacionado com estratégia de segurança de informação nas organizações. É através dela que são definidos os procedimentos de proteção dos ativos organizacionais existentes.

A elaboração da Política de Segurança deve considerar os processos, os negócios, toda e qualquer legislação que os envolva, os aspectos humanos, culturais e tecnológicos da organização. Ela servirá de base para a criação de normas e procedimentos que especificaram as ações no nível micro do ambiente organizacional, além de ser facilitadora e simplificadora do gerenciamento dos demais recursos da organização (NAKAMURA e GEUS, 2003).

3 METODOLOGIA

A pesquisa adotada é a descritiva, pois o objetivo era descrever o processo de Segurança de Informação. Como dito, este trabalho adotou metodologia de pesquisa bibliográfica, exploratória e qualitativa (GIL, 2007).

A fonte de consulta/coleta foi, fundamentalmente, bibliográfica, além de bases de dados de conteúdo acadêmico e de artigos publicados. De forma mais específica, livros de leitura corrente, publicações periódicas e impressos diversos. Optou-se por este tipo de pesquisa pela possibilidade de melhor abranger o tema adotado (GIL, 2007).

Com o aprimoramento das idéias, consideram-se os mais variados aspectos relativos ao assunto abordado. Como conseqüência, familiarizam-se mais com tema. Portanto, a pesquisa é do tipo exploratória (GIL, 2007).

Já que este trabalho contextualiza o problema analisado e explica seus processos, a pesquisa é abordada de forma qualitativa, ou seja, interpretativa e semântica (ABRÃO, BORGES e GAGLIARDI, 2008).

4 DISCUSSÃO

Em função do que se pode chamar de miopia dos executivos, que normalmente somente enxergam os aspectos tecnológicos do problema, aqueles associados aos riscos às redes, computadores, vírus, *hackers*[10] e *Internet*, criando uma barreira para identificar o fator crítico de sucesso que é a anatomia do problema. Anatomia do problema é a identificação dos elementos internos e externos que interferem nos riscos à Segurança da Informação.

O desafio então para os administradores das organizações e para os responsáveis pela criação de uma Política de Segurança da Informação é realizar ações que mapeiem e identifiquem a situação da empresa, suas ameaças, vulnerabilidades, riscos, sensibilidades a impactos, para permitir um adequado dimensionamento e modelagem da solução (SÊMOLA, 2003).

Quanto às características pessoais e particulares que cada empresa possui, a aplicação de uma solução de segurança para a informação será personalizada e terá um nível de segurança também personalizado.

A política de segurança de informações deve ir além dos aspectos relacionados especificamente com sistemas de informação e os recursos computacionais, ela deve se integrar às políticas de segurança em geral, às metas de negócio e ao plano estratégico de informática da organização. Os projetos de informática são os primeiros a sentirem um impacto em relação a uma eficiente ou ineficiente política de segurança. Projetos como de desenvolvimento de novos sistemas, plano de contingências e planejamento de capacidade, são exemplos dessa influência. A política de segurança das informações envolve todas as áreas da organização onde as informações circulam, sejam elas internas ou externas a esta (DIAS, 2000).

Apesar da Política de Segurança da Informação envolver todas as áreas da organização e todos os níveis de postos de trabalho, seu desenvolvimento e aplicação podem ser realizados de forma modular, primeiramente e de preferência nos setores mais críticos e estratégicos da organização e depois nos demais setores.

---

[10] O termo *hacker* é erroneamente adotado para denominar quem invade computadores e/ou sistemas computacionais com objetivo da quebra de um sistema de segurança, de forma ilegal ou sem ética. *Hacker* é o indivíduo que modifica ou inventa algo para realizar funcionalidades que não as originais. O termo mais adequado para definir o indivíduo malicioso é *Cracker*. (N. A.)

Como toda política institucional, também a política de segurança dever ser apoiada pela alta gerência e divulgada a todos os funcionários envolvidos com segurança de informações e usuários de informática.

A partir do momento que a política de segurança é aprovada pela alta administração da organização e está bem difundida, todas as demais ações, controles e processos devem se basear por ela.

É notória a necessidade do envolvimento da alta direção, refletida pelo caráter oficial com que a política é comunicada e compartilhada junto aos funcionários. Este instrumento deve expressar as preocupações dos executivos e definir as linhas de ação que orientarão as atividades táticas e operacionais. Então, para a implantação de uma Política de Segurança da Informação viável, é necessário ter uma visão corporativa, ou seja, enxergar os problemas, ameaças, vulnerabilidades, riscos e impactos às informações de uma organização do ponto de vista tecnológico, físico e humano, para assim conseguir atingir um nível de segurança adequado à natureza do negócio da organização em questão. (SÊMOLA, 2003).

Por se tratar de uma questão que envolve toda a organização nos aspectos falados, que por sinal são a base de sustentação do negócio, torna-se imprescindível que a formulação de uma Política de Segurança da Informação seja iniciada no formato *top-down*, ou seja, que o envolvimento, o apoio e a mobilização ocorram do topo da pirâmide organizacional, executivos e diretores para depois atingir os demais nesta hierarquia. Esta condição é fundamental, pois sem este apoio, não é possível atingir simultaneamente, e com igualdade, as vulnerabilidades em todos os ambientes e processos distribuídos. O apoio referido está relacionado não só à sensibilização e percepção adequada dos riscos e problemas associados, mas também da conseqüente priorização e definição orçamentária à altura (SÊMOLA, 2003).

É preciso ser objetivo na política e dizer exatamente o que se quer proteger. É esse tipo de abordagem que permite a transparência e adesão do processo por todos os envolvidos, a saber, os usuários, a alta direção da organização e o pessoal responsável diretamente pela administração dos recursos. Os envolvidos precisam saber claramente quais são os seus direitos e deveres para que se possa garantir um real envolvimento de todos.

As mudanças organizacionais ocorrem para buscar melhorias que visam atingir resultados, métodos e procedimentos mais eficientes. Essas mudanças são

motivadas por fatores externos como concorrentes e mercados e internos, como a aquisição de máquinas e equipamentos mais modernos.

Ocorre que algumas organizações, por falhas na administração, não sabem passar para seus funcionários as mudanças que ocorrerão e nem a forma como elas ocorrerão. Para reduzir o processo de rejeição por parte dos funcionários aos processos de mudanças, estas organizações devem rever e aprender a forma como conduzir os processos de mudanças.

O problema de comunicação entre organização e funcionários e a deficiência técnica dos funcionários, são consideradas como fatores responsáveis pela resistência destes às mudanças.

4.1 Retorno sobre o Investimento (ROI)

Em função do alto grau de subjetividade encontrado nas ações relacionadas com a segurança das informações, fica difícil para o responsável por esse controle encontrar uma forma de diálogo com os executivos responsáveis pela administração dessas organizações para apresentar elementos que traduzam a necessidade de investimentos e, principalmente, os benefícios que a implementação de segurança trará. Isso porque se trata de um investimento que comumente não se materializa facilmente, mostrando retorno quando os mecanismos de segurança são postos a prova ou testados (SÊMOLA, 2003).

Esta, então, é a maior dificuldade. Um dos principais obstáculos para os profissionais que trabalham com Segurança da Informação é o orçamento que dispõem para implementação das práticas e mecanismos de segurança. Geralmente, os executivos não têm a visão necessária para enxergar esta necessidade e a importância desses investimentos. Para muitos, desenvolver procedimentos de segurança e controle das informações em suas organizações, não passa de gastos a mais e não de investimentos, como deveria ser encarada a questão. Quando essa barreira é superada, de preferência antes da ocorrência de algum incidente de segurança, o orçamento para esses investimentos melhora. Entretanto, aumenta a necessidade de mostrar o retorno desse investimento, que só é possível demonstrar depois de algum tempo através de relatórios sobre as ocorrências de segurança ou

quando de fato ocorre uma tentativa mal sucedida de invasão, roubo de informações ou indisponibilidade de serviços.

4.2 Definindo a PSI baseada na Norma NBR ISO/IEC 27001

A Política de Segurança da Informação exige uma visão macro para seu planejamento. Conforme descrito por NAKAMURA e GEUS (2003, p. 174):

> O inicio do planejamento da política de segurança exige uma visão abrangente, de modo que os riscos sejam entendidos para que possam ser enfrentados. Normalmente, a abordagem com relação à segurança é reativa, o que pode, invariavelmente, trazer futuros problemas para a organização. A abordagem pró-ativa é, portanto, essencial e depende de uma política de segurança bem definida, na qual a definição das responsabilidades individuais deve estar bem clara, de modo a facilitar o gerenciamento da segurança em toda a organização.

A PSI orienta e apóia os gestores das organizações nas ações de prevenção da segurança. Ela é de grande importância para o sucesso dos negócios. Devido a sua grande abrangência ela é subdivida em três blocos: diretrizes e normas, procedimentos e instruções, todos destinados respectivamente às camadas estratégica, tática e operacional (NBR ISO/IEC 27001, 2006).

As diretrizes têm o papel estratégico de expressar a importância que a organização dá a informação, comunicando também aos funcionários seus valores e seu comprometimento com a aplicação e incorporação da segurança à cultura organizacional. Além disso, devem as diretrizes expressar as preocupações dos executivos e definir uma linha de ação orientando as atividades táticas e operacionais. Ela ainda define as responsabilidades dos detentores das informações, os índices e indicadores do nível de segurança, controles de conformidade legal, requisitos de capacitação de usuários, mecanismos de controle de acesso físico e lógico, registro de incidentes, auditorias e gestão da continuidade dos negócios (NBR ISO/IEC 27001:2006).

De acordo com Sêmola (2003, p. 106):

> Critérios normatizados para admissão e demissão de funcionários, criação e manutenção de senhas, descarte de informação em mídia magnética ou em papel, desenvolvimento e manutenção de sistemas, uso da Internet, acesso remoto, uso de notebooks, contratação de serviços terceirizados e classificação das informações, são alguns exemplos de normas de uma típica Política de Segurança da Informação.

A norma de classificação das informações é fundamental para o sucesso da política. Ela é responsável pela descrição dos critérios que avaliaram a importância e o valor das informações para a organização, que serve de baliza para a formulação de todas as demais normas. Para se definir corretamente essa classificação, é de fundamental importância conhecer o perfil do negócio da organização, além das características das informações utilizadas pelos processos organizacionais e que circulam no ambiente corporativo (NBR ISO/IEC 27001, 2006).

Procedimentos e instruções deverão estar presentes na política em maior quantidade por seu perfil operacional, onde é necessário descrever meticulosamente cada ação e atividade associada a cada situação distinta de uso da informação (NBR ISO/IEC 27001, 2006).

Padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança definido sob medida pela e para a organização, são estabelecidos pela política de segurança, pois ela deve ser personalizada ao ambiente organizacional no qual será aplicada (SÊMOLA, 2003).

O planejamento da política de segurança deve ser feito tendo como diretriz o caráter geral e abrangente de todos os pontos, incluindo as regras que devem ser obedecidas por todos. Essas regras devem especificar procedimentos e controles necessários para proteção das informações, quem pode acessar o que e como e quais sistemas poderão ser acessados. Esse caráter geral permite à política controlar, ou melhor, servir de referência para todas as demais ações relativas à Segurança da Informação (NBR ISO/IEC 27001, 2006).

A linha de conduta e ação na construção da política de segurança deverá obedecer e estar em conformidade com requisitos legais, envolvendo obrigações contratuais, direitos de propriedade intelectual, direitos autorais de software, e todas as possíveis regulamentações que incidam no negócio da organização (SÊMOLA, 2003).

A política de segurança deve ser escrita de forma clara, para que todos os envolvidos possam entendê-la e melhor praticá-la.

Objetivando êxito no processo de implantação de uma política de segurança, é fundamental investir num processo de conscientização dos funcionários, mostrando a importância de sua participação. Para mudar essa cultura na empresa, é fundamental que os funcionários estejam preparados sobre o assunto, através de avisos

(comunicação interna/*intranet*), reuniões constantes de conscientização, treinamentos direcionados e peças teatrais com exemplos sobre o assunto.

Segundo a NBR ISO/IEC 27001 (2006), a política de segurança deve seguir pelo menos as seguintes orientações:

(i) Definição de Segurança da Informação, resumo das metas, do escopo e a importância da segurança para a organização, enfatizando seu papel estratégico como mecanismo para possibilitar o compartilhamento da informação e o andamento dos negócios.

(ii) Declaração de comprometimento do corpo executivo, apoiando as metas e os princípios da Segurança da Informação.

(iii) Breve explanação das políticas, princípios, padrões e requisitos de conformidade de segurança no contexto específico da organização, como por exemplo:

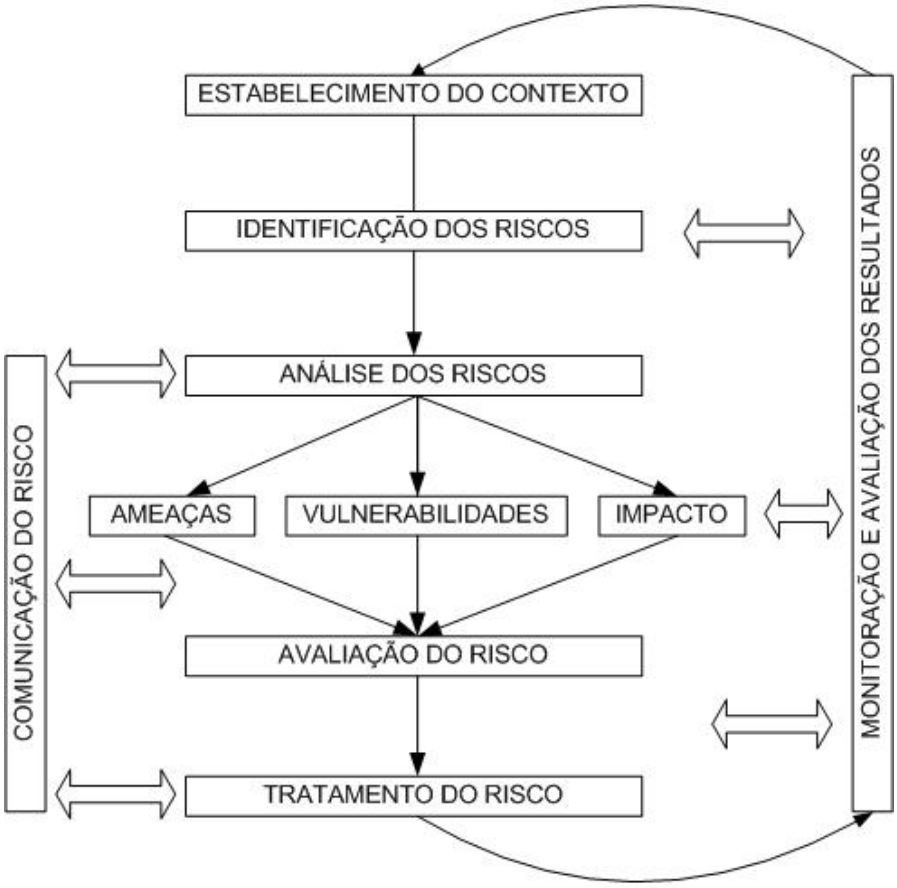
   a. conformidade com a legislação e eventuais cláusulas contratuais;
   b. requisitos na educação e treinamento em segurança;
   c. prevenção e detecção de vírus e programas maliciosos;
   d. gerenciamento da continuidade dos negócios;
   e. conseqüências das violações na política de segurança;
   f. definição de responsabilidades gerais e específicas na gestão da segurança de informações, incluindo o registro de incidentes de segurança;
   g. referências que possam apoiar a política, por exemplo, diretrizes, normas e procedimentos de segurança mais detalhados de sistemas ou áreas específicas, ou regras de segurança que os usuários devem seguir;
   h. classificação da informação de acordo com a prioridade definida pela organização para auxiliar na definição dos riscos.

Considerando o dinamismo e a velocidade da evolução tecnológica no século XXI, é possível perceber o quanto é complexo o desenvolvimento e, principalmente, a manutenção e atualização da Política de Segurança da Informação em toda a sua abrangência.

Nota-se, como diferencial proposto por esta pesquisa, não a proposição de nova PSI e sim a mudança na metodologia da implementação. Busca-se a

simplificação no sentido do entendimento, compreensão e não na adoção de PSI mais simplória.

FIGURA 4 – FLUXO DE PSI



Fonte: BEAL, 2005, p. 17, adaptado.

Na literatura técnica, as linguagem e terminologia são inacessíveis ao público leigo em TI, mas detentor de vasto conhecimento em áreas humanas, como, por exemplo, administradores. Este fato gera distanciamento entre áreas executivas e técnicas, a citar, gestores e TI.

Comprova-se tal colocação quando autores diversos confirmam que é papel do CIO abrir canal entre a infra-estrutura tecnológica da empresa e seus dirigentes, a fim de que uma PSI seja efetivamente implementada. Ele, o CIO, deve demonstrar o que é a PSI, bem como o SGSI, traduzindo e tornando-os de comum entendimento a todos.

Mas a responsabilidade de tradução simultânea do CIO não acaba aí. Cabe a ele, também, tornar-se um canal de comunicação, identificando qual a melhor forma

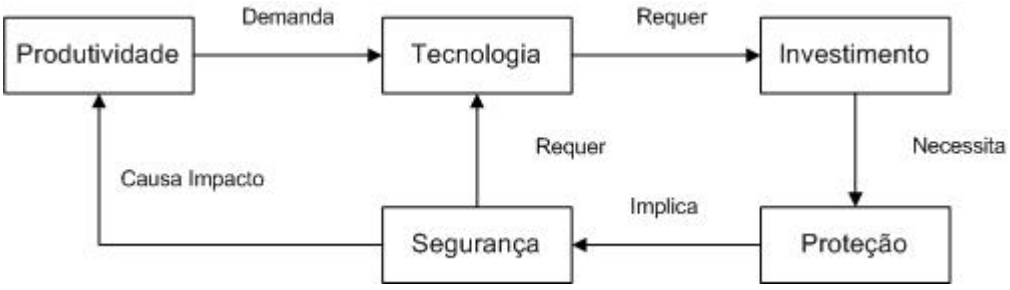
de atuação da SI e, conseqüentemente, ter entendimento abrangente do negócio (BALDO, 2006).

Vive-se um momento onde o CIO deixa de ser simplesmente um executivo de segurança e passa a ser um analista de negócios, pois, quanto mais ampla sua visão da estratégia da empresa, melhor será sua eficiência. “Os problemas de segurança são muito mais abrangentes do que se pensava. A questão ultrapassa produtos básicos e atinge processos e pessoas” (ROSSI apud BALDO, 2006, p. 25).

Cada vez mais, questões essencialmente técnicas afastam-se do foco da SI. O que está acontecendo com SI na moderna administração é o mesmo que aconteceu com TI no passado. Deixou de ser algo eventual ou oportunista para tornar-se uma questão de negócios (BALDO, 2006).

De fato, a tendência organizacional é ser fundamentada na área de TI. Entretanto, apesar de se ter avanço tecnológico, dinamismo e visibilidade, a organização cria uma dependência que, inteligentemente, deve ser acompanhada pelo fomento da SI, a fim de se reduzir ou mesmo evitar ameaças, vulnerabilidades e riscos.

FIGURA 5 – RELAÇÃO EMPRESA E ÁREA DE TECNOLOGIA



Fonte: DAWEL, 2005, p. 68.

5 CONSIDERAÇÕES FINAIS

O objetivo do trabalho foi alcançado no que se trata da convergência das teorias. Em nenhum momento houve a intenção de comparar os autores abordados, certificar um ou desacreditar outro. A pesquisa deu-se com a intenção de se obter as melhores definições que satisfizessem a solução do problema proposto.

Após a reflexão criteriosa sobre este trabalho, considerações devem ser feitas sobre algumas metas.

Quanto ao do objetivo, houve alcance da proposta inicial, ou seja, possibilitar acessibilidade do Administrador ao SGSI.

Quanto à limitação, infelizmente esta ferramenta não teve sua aplicabilidade comprovada na prática, devido limitação temporal. O desenvolvimento, implementação e análise dos resultados da PSI, mesmo que feita de forma modular ou setorizada, extrapolaria o tempo hábil de um semestre para o desenvolvimento deste trabalho.

Com relação à agenda futura, o autor sugere comparação entre duas realidades organizacionais, medindo o impacto da implementação de uma PSI tradicional numa organização e comparando como impacto da implementação da PSI sugerida neste trabalho. Além disso, será dada continuidade à pesquisa, porque o autor entende que esta obra é apenas o começo de uma série de trabalhos a serem realizados, a começar por certificações na área de SI e, por conseguinte, pós-graduação, mestrado, MBA e/ou afins.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:** Tecnologia da informação, técnicas de segurança, sistemas de gestão de segurança da informação, requisitos. Rio de Janeiro: ABNT, 2006.

_____. **ABNT NBR ISO/IEC 27002:** Tecnologia da informação, técnicas de segurança, código de práticas para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2007.

ABRÃO, M., BORGES, C., GAGLIARDI, M. **Resumo de Apoio:** metodologia da pesquisa científica. Apostila. Brasília, 2008.

ABREU, D. Política de Segurança: definir para Implementar**. Modulo Security News**, Rio de Janeiro, n. 247, jun. 2002. Disponível em: <http://www.myfreebsd.com.br/modules.php?name=Sections&op=viewarticle&artid=2&page=1>. Acesso em: 20 abr. 2009.

_____. Controle de Risco Operacional. **Risk Management Review**, São Paulo, n.13, p. 50-52, jul./ago. 2007. Disponível em: <http://www1.ideavalley.com.br/riskmanagement/flip/index.php?playerType=double&idEdicao=4bdf05beaabd709d3b2ea0527769a47e&idCaderno=5ef51c767af73d864f6b33c8884399c7&page2go=51>. Acesso em: 20 abr. 2009.

BALDO, W. Na Crista da Onda: executivos devem estar preparados para uma nova abordagem da segurança, que assume papel de destaque na formulação da estratégia de corporações e governo. **Information Week Brasil**, São Paulo, n. 154, p. 24-29, 09 fev. 2006

BARALDI, P. **Gerenciamento de riscos:** a gestão de oportunidades, a avaliação de riscos e a criação de controles internos nas decisões empresariais. Rio de Janeiro: Elsevier/Campus, 2004.

BEAL, A. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BRASIL. **Resolução 3.380, de 29 de junho de 2006**. Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional. Brasília, 2006. Disponível em: <http://www.bcb.gov.br>. Acesso em: 03 mai. 2009.

BRASILIANO. A. Método Brasiliano de análise de riscos. **Revista eletrônica Brasiliano & Associados:** estratégia e cenários, Luanda/Angola, n. 21, p. 19-34, nov./dez. 2005. Disponível em: <http://www.brasiliano.com.br/revistas/edicao_21.pdf?PHPSESSID=82346724aff2c89ec63763aa8e3fba59>. Acesso em: 16 mai. 2009.

CERTO, S. **Administração Moderna**. 9. ed. São Paulo: Prentice Hall, 2003.

DIAS, C. **Segurança e Auditoria da Tecnologia da Informação.** Rio de Janeiro: Axcel Books, 2000.

FERREIRA, F. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2003.

GIL, A. **Como Elaborar Projetos de Pesquisa.** 4. ed. São Paulo, Atlas: 2007.

GOUVEIA, L., RANITO, J. **Sistemas de informação de apoio à gestão.** Porto: SPI, 2004. Disponível em : <http://www2.spi.pt/inovaut/>. Acesso em: 18 abr. 2009

KUROSE, J., ROSS, K. **Redes de Computadores e a Internet**: Uma Nova Abordagem. São Paulo: Pearson, 2003.

NAKAMURA, E., GEUS, P. **Segurança de redes em ambientes cooperativos:** fundamentos, técnica, tecnologias, estratégias. São Paulo: Novatec, 2003.

NORTON, P. **Introdução à Informática**. São Paulo: Pearson Makron Books, 1996.

RAMOS, A. (Org.). **Security Officer 1:** guia oficial para formação de gestores em Segurança da Informação. 2. ed. Porto Alegre: Zouk, 2008.

SÊMOLA, M. **Você já fez uma análise de riscos de verdade?** Rio de Janeiro, n. 41, jun. 2002. Disponível em: <http://www.semola.com.br/disco/Coluna_IDGNow_41.pdf>. Acesso em: 03 mai. 2009.

_____. **Gestão da Segurança da Informação:** uma visão executiva. Rio de Janeiro: Elsevier, 2003.

SILVA, C., TRISTÃO, G. **Contabilidade básica**. 2. ed. São Paulo: Atlas, 2000.

SPAFFORD, G. **Enterprise should emphasize preventive controls.** 01 ago. 2005. Disponível em: <http://itmanagement.earthweb.com/netsys/article.php/3524221>. Acesso em: 03 mai. 2009

VEIGA, P. **Tecnologias e sistemas de informação, redes e segurança.** Porto: SPI, 2004. Disponível em : <http://www2.spi.pt/inovaut/>. Acesso em: 18 abr. 2009.

YU, A. Riscos de Investimentos em Tecnologia. **Bate-papo Programado.** 26 fev. 2002. Disponível em: <http://www.ipt.br/atividades/servicos/chat/?ARQ=27>. Acesso em: 18 abr. 2009.