ISAÍAS DE QUEIROZ RAMOS

Contribuição da Ciência da Informação para criação de um Plano de Segurança da Informação

Campinas - SP

2007

ISAÍAS DE QUEIROZ RAMOS

Contribuição da Ciência da Informação para criação de um Plano de Segurança da Informação

Dissertação apresentada ao Curso de Pós-Graduação, em Ciência da Informação, da Pontifícia Universidade Católica de Campinas, como requisito parcial à obtenção do título de Mestre.

Orientador: Prof. Dr. Orandi Mina Falsarella

Campinas - SP

2007

Ficha Catalográfica
Elaborada pelo Sistema de Bibliotecas e
Informação - SBI - PUC-Campinas

T020 RAMOS, ISAÍAS DE QUEIROZ.

R175c Contribuição da ciência da informação para criação de um plano de segurança da informação / Isaías de Queiroz Ramos. - Campinas: PUC-Campinas, 2007.
117p.

Orientador: Orandi Mina Falsarella.
Dissertação (mestrado) - Pontifícia Universidade Católica de Campinas, Centro de Ciências Sociais Aplicadas, Pós-Graduação em Ciência da Informação.
Inclui bibliografia.

1. Ciência da informação. 2. Ciência da informação - Sistemas de segurança. 3. Ciência da informação - Processo decisório. 4. Planejamento estratégico. 5. Pesquisa bibliográfica. 6. Tecnologia da informação. I. Falsarella, Orandi Mina. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Sociais Aplicadas. Pós-Graduação em Ciência da informação. III. Título.

22.ed.CDD – t020

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Autor (a): RAMOS, Isaías de Queiroz

Título: "CONTRIBUIÇÃO DA CIÊNCIA DA INFORMAÇÃO PARA CRIAÇÃO DE UM PLANO DE SEGURANÇA DA INFORMAÇÃO" .

Orientador (a): Prof. Dr. Orandi Mina Falsarella

Dissertação de Mestrado em Ciência da Informação

Este exemplar corresponde à redação final da Dissertação de Mestrado em Ciência da Informação da PUC-Campinas, e aprovada pela Banca Examinadora.

Data: 27/02/2007.

BANCA EXAMINADORA

Prof. Dr. Orandi Mina Falsarella

Prof. Dr. Marco Antonio Silveira

Profª. Dra. Angela de Mendonça Engelbrecht

DEDICATÓRIA

À minha esposa Vânia que acompanhou cada momento durante esse percurso, inclusive sugerindo, apoiando-me com palavras, ombro, carinho e incentivando-me a não desanimar.

À minha querida filha Rebeca, um presente de Deus, que nasceu bem próximo ao fim deste trabalho, mas, ainda no ventre da minha esposa, participou dos momentos de correria.

AGRADECIMENTOS

A Deus, por ter-me concedido força, saúde e perseverança nos momentos em que minhas forças física, emocional e intelectual chegavam ao limite, Ele, com suas mão poderosas, me ajudava.

À minha família, pela compreensão que teve quanto à minha ausência em alguns finais de semana.

Ao meu orientador Prof. Dr. Orandi Mina Falsarella, pelo incentivo e sábios conselhos.

À Pontifícia Universidade Católica de Campinas por fornecer bolsa de estudo e suporte, muito obrigado!.

À coordenação do programa de mestrado, na pessoa do Prof. Dr. Raimundo Nonato, pelas palavras de incentivos.

A todos os professores do programa que sempre se mostraram acessíveis e compassivos nas aulas ministradas.

Ao pessoal da secretaria acadêmica, pelas informações e paciência.

À banca examinadora, que é formada por pessoas que trouxeram grandes contribuições para este trabalho e minha formação.

RAMOS, Isaías de Queiroz. **Contribuição da Ciência da Informação para criação de um Plano de Segurança da Informação.** 2007. Dissertação de Mestrado em Ciência da Informação – Pontifícia Universidade Católica de Campinas, Campinas – SP.

RESUMO

As organizações lidam diariamente com informações que têm assumido valores distintos no mundo dos negócios. As informações consideradas estratégicas e de apoio às tomadas de decisão necessitam de gerenciamento e garantia de confidencialidade, integridade e disponibilidade. Sendo assim, este trabalho teve como objetivo analisar a contribuição da Ciência da Informação para criação de um Plano de Segurança da Informação. Para isso, utilizou-se de uma pesquisa bibliográfica, analisando os conceitos de organização, informação, Ciência da Informação, Planejamento Estratégico e segurança da informação. E, ao avaliar os fluxos de informações nas organizações, foi possível extrair as necessidades de informações, como também a aplicação das características e domínio de proteção, a geração da necessidade de informações qualificadas e priorizadas e a utilização da norma NBR/ISO 17799:1 no ambiente organizacional. Assim constaram-se, com esse estudo, subsídios necessários para criação de um Plano de Segurança da Informação que seja integrado com as formas de tratamento das informações, concebidas pela Ciência da Informação e pelas técnicas de gestão utilizadas no processo de Planejamento Estratégico.

Palavras-chave: Informação, Ciência da Informação, Segurança da Informação, Planejamento Estratégico.

RAMOS, Isaías de Queiroz. **Contribution of Information Technology to the creation of the Information Security Plan.** 2007. Abstract for Master's Degree in Science Technology – Pontifícia Universidade Católica de Campinas, Campinas – SP.

ABSTRACT

Every day companies deal with information which has different values in the business world. Both, the strategic information and the information that supports decision-making need management and confidentiality warranty, integrity as well as availability. Therefore, the aim of this paper was to analyse the contribution of Information Technology to the creation of the Information Security Plan. A bibliographic research analysing the concepts of organization, information, Information Science, Strategic Planning and information security was used to carry out this paper. By evaluating the information flow in the organizations, it was possible to extract not only the information needs but also the application of the characteristics and protection domain, the generation of the need of qualified and high-priority information as well as the use of the norm NBR/ISSO 17799:1 in the organizational environment. This study certified the need of subsidies to the creation of an Information Security Plan which must be integrated with ways of dealing with information conceived by Information Technology and by management techniques used in the process of Strategic Planning.

Key Words: Information, Information Science, Information Security, Strategic Planning.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

Neste capítulo será feito uma contextualização do problema, onde se analise em primeira instância os aspectos da chamada explosão informacional, a valorização da informação e a evolução das organizações, paralelo aos impactos das tecnologias de informação e comunicação. Apresenta o surgimento da Ciência da Informação, a necessidade de proteção das informações e sobre o Planejamento Estratégico como forma de conhecer as informações estratégicas organizacionais. Na seqüência, apresenta o objetivo do trabalho, justificativa, o método de pesquisa e a estrutura do trabalho.

1.1 Contextualização do problema

A valorização da informação evidenciou-se de forma mais clara após a segunda guerra mundial, na denominada "explosão informacional" (Saracevic, 1996, p. 2), em que a quantidade de informações resultantes das pesquisas realizadas antes, durante e após a guerra necessitavam de uma nova forma de tratamento e facilidade em seu manuseio.

Um dos primeiros escritos que contribuiu para a análise e discussão dessa problemática foi o artigo do pesquisador americano Vannevar Bush (1945), que, preocupado com o número crescente das publicações ou materiais úteis para a pesquisa e desenvolvimento, pensou em um recurso que facilitasse aos cientistas e à sociedade em geral acesso a estas informações. Com objetivo de organizar e recuperar as informações de forma ágil, propôs a criação de uma máquina, MEMEX (Memory Extension). A proposta de Bush era que este dispositivo idealizasse uma

memória humana estendida que, através de associações, pudesse recuperar informações rapidamente, facilitando assim a sua utilização. Lembrando que o mecanismo de recuperação da época era baseado em sistemas manuais de indexação através de palavras-chaves.

Entretanto, a idéia de Bush não apresentou somente os recursos visionados especificamente no MEMEX, mas despertou nas comunidades científicas, governos e empresários, interesses nas questões do tratamento, armazenamento, disseminação da informação, como também, incentivou a busca de novas ferramentas ou meios automáticos que fornecessem suporte a esses requisitos. Tais interesses foram se concretizando com o surgimento de diversas Tecnologias de Informação e Comunicação (TIC), visto principalmente, a partir da segunda metade do século XX (Saracevic, 1996).

No entanto, revisando as literaturas percebe-se que, paralelamente ao surgimento e evolução da TIC, houve também um progresso evolutivo no âmbito organizacional, provocando, dessa forma, mudanças singulares na sociedade.

Hampton (1981) define organização como “uma combinação intencional de pessoas e tecnologia para atingir um determinado objetivo”. Como decorrência desse fato, não há como deixar de relacionar a origem e o progresso tecnológico dos momentos evolutivos das abordagens organizacionais. A TIC e as organizações são elementos que se relacionam e integram entre si. Em determinado momento, a tecnologia atuou como uma simples ferramenta de automatização das operações nas organizações, em outro, como recurso imprescindível de suporte ao tratamento de informações para negócios.

Um dos primeiros impactos de mudanças nas organizações ocorreu, inicialmente, no ambiente operacional, pois, no processo de produção,

todas as atividades envolvidas eram executadas pelo mesmo profissional ou artesão. Devido à necessidade de uma maior escala de produção, esse ambiente se transformou e adequou às tarefas segmentadas e compartilhadas. De forma geral, essa carência por aumento de produtividade foi a força motriz para a criação dos conceitos de Administração Cientifica de Taylor, a idéia de uma linha de produção de Ford e a estruturação de um ambiente organizacional de Faylor, no inicio do século XX (Maximiano, 2004).

No entanto, esses conceitos que representam os fundamentos básicos da Administração e que impactaram empresas e pessoas, contribuem para verificar o primórdio dos estudos focalizados nas organizações e a origem do tratamento das informações estratégicas de maneira que resultem em fator decisório e diferencial competitivo.

Sendo assim, fica explícita a valorização do objeto informação no suceder dos anos, com o avanço tecnológico e organizacional. Segundo Ferreira (2003) “a informação é um ativo, como qualquer outro ativo importante”, que merece cuidado e atenção especial dentro das organizações. Conforme Robredo (2003), essa informação apresenta algumas características:

> “Registrada (codificada) de várias formas, duplicada e reproduzida, transmitida por diversos meios, conservada e armazenada em suportes diversos, medida e quantificada, adicionada a outra informação, organizada, processada e reorganizada segundo diversos critérios, recuperada quando necessário segundo regras preestabelecidas” (p.9).

Dentro desse contexto, a Ciência da Informação surge como uma Área interdisciplinar - Biblioteconomia, Ciência da Computação, Ciência Cognitiva e Comunicação, entre outras - tendo a informação como seu objeto de estudo. Conforme Saracevic (1996), a Ciência da Informação teve sua origem na revolução

técnica e científica após a segunda guerra mundial. Acrescenta ainda, que a Ciência da Informação apresenta-se na atualidade como:

> "Um campo dedicado às questões cientificas e à prática profissional voltadas para os problemas da efetiva comunicação do conhecimento e de seus registros entre os seres humanos, no contexto social, institucional ou individual do uso e das necessidades de informação. No tratamento dessas questões são consideradas de particular interesse as vantagens das modernas tecnologias informacionais" (Saracevic, 1996, p.47).

Com o crescente uso da informação como um ativo estratégico e de valor nas organizações, um ponto que merece destaque é saber como as empresas desempenham o papel de proteger as informações contra acesso não autorizado, modificação e indisponibilidade. Segundo Ariosto (apud Holanda, 2006) "a informação está, de modo crescente, exposta a um elevado número de ameaças e vulnerabilidades". Para Geus e Nakamura (2003) as empresas estão sujeitas a possíveis ataques, métodos, técnicas e ferramentas que aumentam os riscos de segurança. Sendo assim, instituições (privadas ou públicas), grupos de pesquisas ou gestores de segurança, trabalham e incentivam a implementação de procedimentos para a Segurança da Informação.

Sêmora (2003) define Segurança da Informação como "uma Área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". Ferreira (2003) acrescenta que a Segurança da Informação protege a informação de diversos tipos de ataques que surgem no ambiente organizacional, garante a continuidade dos negócios, reduz as perdas e maximiza o retorno dos investimentos e das oportunidades.

Segundo os autores, há preocupação com algumas mudanças que levam as organizações a estarem atentas com a proteção da informação. São elas:

- Crescimento sistemático da digitalização de informações;
- Crescimento exponencial da conectividade da empresa;
- Crescimento das relações eletrônicas entre as empresas;
- Crescimento exponencial do compartilhamento de informações;
- Baixo nível de identificação do usuário no acesso gratuito à Internet;
- Acesso a conexões Internet em banda larga;
- Disponibilidade de grande diversidade de ferramentas de ataque e invasão;
- Associação equivocada entre Inteligência Competitiva e Espionagem Eletrônica;
- Crescente valorização da informação como principal ativo de gestão das empresas.

Segundo a norma NBR ISO/IEC 17799:1, Segurança da Informação tem como objetivo proteger um bem que tem tornado cada vez mais importante dentro das organizações, a informação, em suas várias formas de representação - escrita, falada, visual, eletrônica, entre outras.

Dentro desse contexto, existem três pilares ou focos que devem sustentar a informação:

- Confidencialidade;
- Integridade;

- Disponibilidade.

A confidencialidade está relacionada em garantir que a informação seja acessada somente pelas pessoas que tenham a devida autorização para isso. Em um ambiente compartilhado, a informação deve possuir dispositivos ou instrumentos de controle que permitam somente quem tem permissão, acessá-la.

A integridade engloba a exatidão da informação, da origem ao destino, sem qualquer tipo de modificações. A informação se torna íntegra se, no destino, no momento de resgate, ela estiver fiel ao seu estado original.

A disponibilidade é a garantia sem falhas de obter acesso às informações importantes sempre que delas se necessite.

Tendo em vista esses pilares, antes de definir estratégias, método ou planos de segurança da informação, é importante saber como as organizações tomam suas decisões, formulam suas estratégias, integram as TI e estabelecem procedimentos. Nesse sentido, é preciso conhecer as estratégias organizacionais, provenientes do Planejamento Estratégico (PE).

Segundo Maximiano (2004) PE “é um processo intelectual, que consiste em estruturar e esclarecer a visão dos caminhos que a organização deve seguir e os objetivos que deve alcançar”.

Ao final do seu desenvolvimento o PE gera produtos que representam toda estrutura do planejamento. São eles:

- Visão;
- Missão;
- Objetivos;

- Estratégias.

A visão de uma organização é caracterizada pelos anseios ou perspectivas quanto ao futuro da mesma. Seria como visualizar, em um período de tempo estabelecido, o destino da empresa.

A missão organizacional é verificada e/ou estabelecida no conhecimento da proposta ou razão de existência de uma organização (Certo, 1993). A missão expressa os valores, as competências e a vocação existente dentro da instituição que norteia objetivos claros e finalidades comuns (Maximiano, 2004).

Os objetivos são extraídos da missão da organização, de maneira que, em uma análise de prós e contras, vantagens e desvantagens, oportunidades e ameaças, se estabelece um foco para o futuro.

As estratégias são os caminhos ou meios que serão trilhados para se chegar aos objetivos visionados.

Assim, conhecendo as necessidades estratégicas das organizações por meio do PE e, decorrente deste, as necessidades informacionais, é possível pensar que existem elementos para criar um Plano de Segurança de Informação.

1.2 Objetivo do trabalho

O objetivo deste trabalho é apresentar uma proposta como a Ciência da Informação - CI pode contribuir para a criação de um Plano de Segurança de Informação (PSI) e sua dinâmica no ambiente organizacional.

1.3 Justificativa

Um dos ativos mais importantes para o bom desenvolvimento das organizações é, sem dúvida, a informação. Segundo Davenport (1998), a informação é o que reduz a incerteza, ou seja, ela auxilia o processo de tomada de decisão tanto na esfera organizacional como individual. Partindo dessa perspectiva, o estudo sobre segurança da informação tem sido uma realidade não somente brasileira, como no mercado globalizado e, por isso requer um maior aprofundamento teórico.

É de grande relevância o estudo desta temática, pois possibilita uma visão sistêmica da gestão organizacional, proporcionando não somente subsídios teóricos para os executivos, gerentes e administradores, mas também para profissionais que atuam em diversos setores das organizações, levando-os, assim, a compreender que a responsabilidade de garantir a confidencialidade, a integridade, a disponibilidade da informação, em termos de segurança envolve todos na organização.

Para os profissionais que atuam direta ou indiretamente com os sistemas de informações, este assunto é de grande relevância, pois com evolução dos diversos tipos de ameaças que rondam estes ambientes - vírus, *hackers*, espionagem industrial, engenharia social, entre outros - surge necessidade dos profissionais acompanharem atentamente essa evolução e estarem capacitados para combatê-las o mais rápido possível. Acrescenta-se ainda, a existência de demanda por profissionais para atuarem na área de Segurança da Informação.

1.4 Método de pesquisa

O método de pesquisa a ser utilizado será a pesquisa bibliográfica.

Pesquisa bibliográfica segundo Gil (2002, p.44), consiste em desenvolver o trabalho "com base em material já elaborado, constituído principalmente de livros (de leitura corrente e de referência) e artigos científicos (publicações e periódicos)".

Diante disso, pretende-se, a partir da discussão dos conceitos de Planejamento Estratégico e dos produtos gerados no desenvolvimento deste plano, analisar quais informações são relevantes para a organização e, a partir disso, como, do ponto de vista da confidencialidade, integridade e disponibilidade, o Plano de Segurança de Informação pode ser desenvolvido.

1.5 Estrutura do trabalho

Este trabalho está estruturado em cinco capítulos. O capítulo 1 apresenta a contextualização do problema, o objetivo do trabalho, a justificativa, o método de pesquisa e a estrutura do trabalho.

No segundo capítulo apresenta-se uma revisão dos conceitos existentes de informação em diversas áreas do conhecimento e sua importância para as organizações. Encerra o capítulo analisando o conceito de Segurança da informação, como sua necessidade mediante uma analise da Norma NBR ISO 17799:1, que trata das práticas de segurança da informação.

O capítulo 3 traz os principais conceitos de Planejamento Estratégico e descreve seus produtos - visão, missão, objetivos e estratégias. Observa-se, também, o fluxo de informação nesse processo e a sua necessidade

de informação.

O capítulo 4 mostrará como a Ciência da Informação pode contribuir para a criação de um Plano de Segurança de Informação, mediante a extração das necessidades de informações, aplicação das características e domínios de proteção, geração da necessidade de informação qualificada e priorizada e utilização da Norma NBR/ISO 17799:1

Finalmente, o capítulo 5 descreve as conclusões e as sugestões para novos trabalhos.

2. INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO

O termo informação é bastante amplo e possui diversos significados. O presente capítulo conceitua-o em algumas áreas do conhecimento, descreve sobre segurança da informação, mostrando a importância do profissional de segurança da informação, assim como os tipos de ataques às redes de computadores e sobre a norma NBR/ISO 17799:1.

2.1 Informação

O termo informação, etimologicamente, se origina do latim *formatio*, no sentido "de representar, apresentar, criar uma idéia ou noção" ou "dar forma, aparência, pôr forma, formar" (Zeman, 1970, apud Pinheiro, 2004). Com esta definição fica claro o território multifacetado que este termo percorre em suas diferentes abordagens. Segundo Kobashi e Tálamo (2003, p.10), a informação tem sido "objeto de estudo de várias disciplinas".

A informação influencia a vida das pessoas, pois ela "afeta e é afetada pelo contexto do indivíduo que inclui valores éticos, políticos, sociais e religiosos" (McGarry, 1984). Esta apresenta um impacto nas organizações, sendo uma arma estratégica indispensável para obtenção de vantagens competitivas (Porter, 1985).

Estudos denotam a complexidade de conceituar este termo, visto que, segundo Schrader (apud Capurro, 1991), na década de 1980, foram encontradas 134 definições para informação dentro da Área da Ciência da Informação. Um outro estudo do mesmo autor constatou em uma pesquisa, considerando um período maior (1900 a 1981), que são 700 as definições para o

termo nas diversas Áreas do conhecimento (apud Capurro e Hjorland, 2003).

Para Demo (2000), há valores diferentes no objeto informação que precisam ser observados:

> "A informação é em si ambivalente, tanto em quem a pronuncia, quanto em quem recebe. Em todos os momentos passa pelo filtro da subjetividade, além de sua dimensão estar limitada pelo aparato perceptor e conceitualizador. Mas é esta ambivalência que resgata sempre a possibilidade de criar, inventar. Se tudo fosse apenas lógico, seria apenas repetitivo. O mundo da informação é agitado, conturbado, porque é, ao mesmo tempo, intrinsecamente manipulado e impossível de ser totalmente manipulado" (p.41)

Partindo desta perspectiva, fica claro compreender a ampla definição de Wilden (2000) que descreve a informação como:

> "Estruturas, formas, modelos, figuras e configurações, em idéias, ideais e ídolos; em índices, imagens e ícones; no comércio e na mercadoria; em continuidade em descontinuidade; em sinais, signos e significantes; em gestos, posições e conteúdos; em freqüências, entonações, ritmos e inflexões; em presença e ausências; em palavras, em ações e em silêncios; em visões e em silogismos. É a organização da própria variedade" (p.11).

Tendo em vista as características apresentadas acima, alguns autores denominam e consideram a informação como "camaleão intelectual". Entende-se, com essa expressão, que a informação possui um alto grau de adaptabilidade ao ambiente no qual se encontra inserida ou contextualizada. As multifaces da informação são tão presentes que Wersig e Nevelling, 1975 (apud Pinheiro, 2004, p.2) aconselham, "se não tem como evitar o termo informação, a melhor forma é sempre que usá-lo deixar claro, todo instante, o que significa", ou

seja, a informação como um objeto que está presente em diversas áreas, exige sempre na sua apresentação a necessidade de contextualização. Araújo (1995, p. 56) acrescenta, ainda, que a informação "não é na verdade um conceito único, singular, mas sim uma série de conceitos conectados por relações complexas".

Na opinião de Buckland (1991), a informação pode ser expressa como um processo, um conhecimento ou como coisa. Como processo, a informação é apresentada como o ato de informar e proporciona modificações do saber. A informação como conhecimento, segundo o autor , está relacionada com o ato de agregar algo novo ao individuo, ou seja, diminuir a incerteza. Já a informação vista como coisa, está relacionada a alguma representação física, por exemplo, os sinais em uma comunicação e textos em geral, entre outros. O objetivo do autor no artigo *information as thing* (informação como coisa) é mostrar que o processo de informar não está limitado somente às características intangíveis e subjetivas - informação-como-conhecimento e informação-como-processo -, mas, como algo que é representado fisicamente.

A utilização da palavra informação sempre esteve presente na vida do ser humano como elemento que não se deve ignorar. Para Fontes (2006), a informação é um recurso que move o mundo e está presente em todo ciclo de desenvolvimento humano e em diversas Ciências existentes.

Como no parágrafo citado acima, em relação ao ciclo de desenvolvimento humano, significa dizer que, em todas as fases da vida, a informação se faz presente, seja na redução de qualquer incerteza ou no processo de agregação do conhecimento. A fim de exemplificar esta idéia, Silva (1998) trabalha apresentando as diferentes faixas etárias da vida humana e como ocorre o processo de obtenção do conhecimento e da informação. Mostra que, do berçário

ao jardim da infância (1-5 anos) a aprendizagem é adquirida pelos sentidos, curiosidades e imaginações, através da informação como figuras e imagens. No primário (6-8 anos) a aprendizagem ocorre mediante informações observáveis. Nos juniores (9-11 anos) é a fase da investigação e o porquê das coisas; assim, a busca do conhecimento se dá por meio de informações existentes em literaturas. Na fase da adolescência (12-17 anos) é o momento de expansão, surge a razão, a mais alta das faculdades humanas, idade das dúvidas, da lógica, período em que o aprendizado é motivado por informações amplas do mundo. Já os jovens (18-24 anos) possuem uma forte imaginação construtiva e planejada. As informações facilmente associadas proporcionando invenção ou novas descobertas em alguns casos. A fase adulta (25-60) é estágio de aplicação, realização e reflexão e assim por diante.

Na Teoria Matemática da Comunicação, a informação é apresentada como "uma noção quantitativa, referindo-se sempre à quantidade de informação e não a sua qualidade" (SHANNON, C. E.; WEAVER, W, 1963). Nessa teoria da informação, o que importa é a medida do conteúdo de informação, ou melhor, o teor ou taxa de informação (Pignatari, 1969, apud Messias, 2002).

Nas Ciências Biológicas, a informação aparece como um componente totalmente presente no corpo humano. Elas classificam os seres humanos como seres informacionais.

> "No corpo humano, as informações são transmitidas sob forma de pulsos que caminham ao longo das fibras nervosas. O sistema nervoso humano dirige os movimentos através da transmissão de sinais que partem dos centros controladores e caminham através dos músculos, os quais se contraem e executam o movimento ordenado" (Edwards, 1964, p.13).

No campo do desenvolvimento cientifico, Aguiar (1991) categoriza os vários tipos de informação: informação científica, informação em ciência e tecnologia, informação para indústria e informação industrial.

Informação científica “é todo conhecimento que resulta – ou está relacionado com o resultado – de uma pesquisa científica,” envolvendo a divulgação do conhecimento que esta pesquisa apresenta; construir insumo para um novo projeto de pesquisa científica; apresentar a metodologia empregada na execução (Aguiar, 1991, p.10).

Enquanto a informação em ciência e tecnologia engloba:

> “As informações que, além de cumprirem as funções relacionadas como específicas da informação científica ou da informação tecnológica, servem ainda para cumprir e apoiar a atividade de planejamento e gestão em ciência e tecnologia: avaliar o resultado do esforço aplicado em atividades científicas e tecnológicas e subsidiar a formulação de políticas, diretrizes, planos e programas de desenvolvimento científico e tecnológico”. (Aguiar, 1991, p.12)

Aguiar adota uma terminologia proposta por Klintoe de informação para a indústria como o conjunto de conhecimentos em que a empresa deve dispor a fim de:

- Facilitar a execução de operações correntes de natureza administrativas, de produção e de controle;
- Possibilitar o acompanhamento da dinâmica de mercado, para detecção de oportunidades e ameaças;
- Permitir a implementação de estratégias emergenciais para enfrentar problemas conjunturais;

- Subsidiar as atividades de planejamento estratégico;
- Contribuir para o desenvolvimento tecnológico (Aguiar 1991, p.12).

Ainda segundo Aguiar, há uma distinção entre informação para indústria, definido acima, e informação industrial que, em sua colocação, representa:

> "O esforço de coletar, avaliar e tornar disponíveis informações sobre o setor industrial e suas operações produtivas, gerando dados técnico-econômicos, informações sobre tecnologias utilizadas, a estrutura industrial, a produtividade setorial, estudos de viabilidade, dados de investimento e retorno, implantação de indústrias, transferência de tecnologia, dentre outros" (p.13).

Uma outra expressão utilizada é informação para negócio que segundo Vernon (apud Borges e Campello, 1997), representa:

> "Dados, fatos e estatísticas publicados, necessários à tomada de decisão nas organizações de negócios, públicas ou privadas, bem como governo. Inclui informações mercadológicas, financeiras sobre bancos, empresas, leis e regulamentos de impostos, informações econômicas e comerciais, bem como informação factual sobre o ambiente no quais os negócios se realizam" (p.150).

Tendo em vista essas definições relacionadas ao ambiente empresarial ou de negócio, acrescenta-se a colocação de Moresi (2000) que a informação é utilizada em muitas organizações como um fator estruturante e um instrumento de gestão, considerando seus valores e os sistemas de informação.

Apesar de estas terminologias - informação para a indústria,

informação industrial, informação para negócio -, serem mais utilizadas em países como Estados Unidos e Reino Unido, no Brasil o termo já é utilizado por diversos autores (Jannuzzi e Montalli, 1999, Borges e Campello, 1997, Aguiar, 1991, entre outros).

Para Robredo (2003), sem perder a universalidade do termo, dentro da documentação a informação é suscetível de ser:

> ○ Registrada (codificada) de diversas formas,
>
> ○ Duplicada e reproduzida *ad infinitum,*
>
> ○ Transmitida por diversos meios,
>
> ○ Conservada e armazenada em suportes diversos,
>
> ○ Medida e quantificada,
>
> ○ Adicionada às outras informações,
>
> ○ Organizada, processada e reorganizada segundo diversos critérios e recuperada quando necessário segundo regras preestabelecidas (p.9).

Acrescente-se ainda a necessidade de entender as diferenças entre dado, informação e conhecimento, que são termos que estão intrinsecamente relacionados.

Dados são definidos como uma série de observações, medidas ou fatos nas formas de números, palavras, sons e/ou imagens. Os dados não têm significado próprios, mas fornecem a matéria prima a partir da qual é produzida a informação. Dados na forma plural da palavra latina “datum” significa “coisas que podem ser dadas” (Buckland, 1991, p.5).

Para Oliveira (2003), dado é qualquer elemento identificado em sua forma bruta que por si só não conduz a uma compreensão de determinado fato ou situação. Considera-se, portanto, dado como o possível precursor da informação, isto é, se trabalhado de modo que venha criar um significado ou resolver um problema, reconhece-o como informação. Já o conhecimento é o ato ou estado de conhecer, percepção clara dos fatos. O mais alto grau das faculdades especulativas, campo de interesse da informação, competência e ciência.

Conforme Davenport (1998), não é tão trivial distinguir, na prática, dados, informação e conhecimento. Segundo ele, o que se pode fazer é elaborar um processo que inclua os três. No entanto, a dificuldade se embate nos dois elementos, informação e conhecimento. Não há um consenso entre os especialistas sobre onde termina a informação e onde começa o conhecimento. A informação serve para propagar o conhecimento.

Urdaneta (apud Moresi, 2000) acrescenta à tríade (dado, informação e conhecimento) o elemento, inteligência, como um nível a mais na hierarquia de representação da informação (vide figura 1). Sua abordagem alcança o contexto das organizações, apresentando estes níveis e suas diferenças como sendo relevantes no processo decisório.

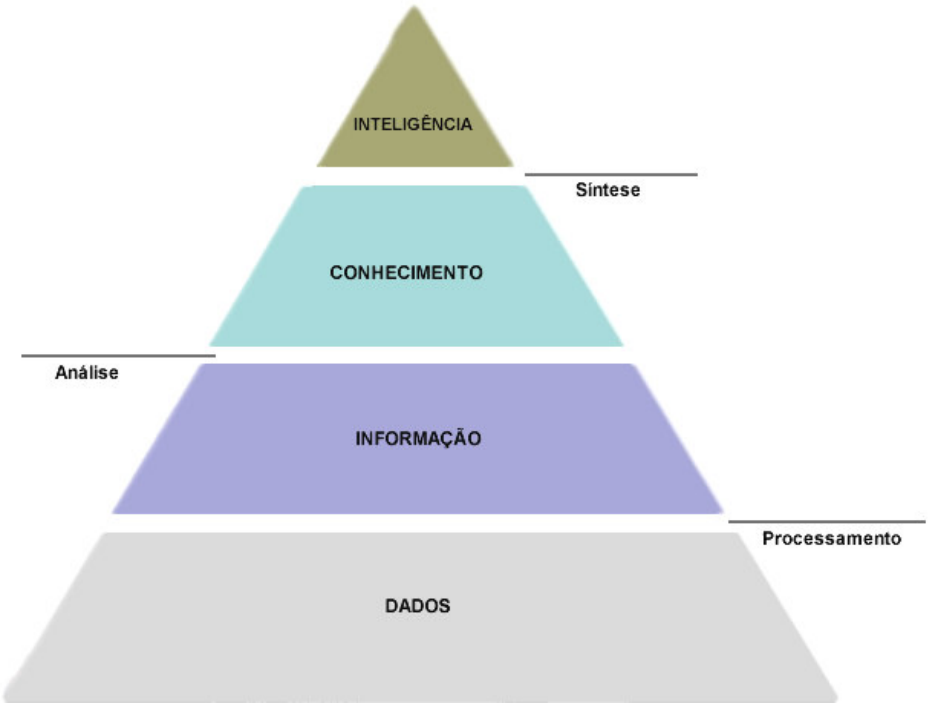

Figura 1: Os níveis hierárquicos da informação. **Fonte:** Adaptada de Moresi (2000, p.18).

A figura 1 representa as quatro fases diferentes da informação, considerando suas características e funções dentro da organização. A apresentação em forma de pirâmide é proposital, pois busca demonstrar o dinamismo e a importância progressiva da informação. De acordo com Moresi (2000, p.18), a classe dados significa "sinais que não foram processados, correlacionados, integrados, avaliados ou interpretados de qualquer forma; como, fatos, sons, imagens estáticas etc.". Ele considera o item dados, como a base ou substância fundamental na fabricação da informação.

Quanto à informação, é resultante de um processamento dos dados na sua forma bruta para um estágio inteligível por parte das pessoas que irão trabalhá-la ou usá-la. Para o autor, o processamento dos dados exemplifica as "transmissões de rádio transformadas em um formato de relatório padronizado, a exibição de arquivos de computador como texto ou gráfico em uma tela, a grade de

coordenadas em um mapa, entre outros", transformando-os em um relatório ou documento significante que tenha valor para organização.

O próximo nível é o do conhecimento "que pode ser definido como sendo informações que foram analisadas e avaliadas sobre a sua confidencialidade, sua relevância e sua importância" (Moresi, 2000, p.19). Segundo sua definição, o conhecimento auxilia os responsáveis por ações decisivas a resolverem os problemas nas organizações e a entenderem melhor as causas das situações adversas no ambiente. Deixa de ser uma informação que informa e reduz a incerteza ou esclarece algo, e passa a desempenhar um papel ativo nas soluções de problemas.

O nível mais alto desta hierarquia é a inteligência, que Moresi (2000, p.19) ressalta como sendo a "informação como oportunidade, ou seja, o conhecimento contextualmente relevante que permite atuar como vantagem no ambiente considerado".

Além dos conceitos e importância da informação apresentados acima, percebe-se a necessidade das organizações em tratá-la de modo que resulte em valor comercial, maximização dos processos de produção e desenvolvimento. O valor de uma informação é determinado pela sua utilidade nas organizações e para as pessoas. A maximização dos processos relaciona-se com a utilização de sistemas de informação que automatizam e respondem com maior produtividade.

Battaglia (1999, p. 207) classifica quatro tipos de informações que geram produtos e proporcionam desenvolvimento em algum momento: informação científica, técnica, tecnológica e técnico-econômica.

Segundo a mesma autora, a informação científica é aquela gerada e tramitada principalmente no meio acadêmico. Ela possui representação nas pesquisas básicas e aplicadas, e, geralmente, aparece em documentos como revistas científicas, teses, anais de congressos, entre outros. São informações que se originam em experimentos de laboratórios em Universidade ou empresas que investem em pesquisas. Já a informação técnica representa, especificamente, produtos e serviços que estão disponíveis no mercado. São aquelas que saíram do experimento inicial e se tornaram produtos de interesse para o mercado; por exemplo, documentos de patentes. Estes dois primeiros tipos de informações, na opinião da autora, são geralmente estruturados em bases de dados como Dialog, Quest-Orbit, SNT, portanto, são mais organizadas e de fácil acesso. (Battaglia,1999).

A informação tecnológica é o resultado prático das pesquisas desenvolvidas que visam a “colocar em operação as unidades industriais, mediante construção de protótipos, de unidade piloto”. E, a informação técnico-econômica “refere-se aos dados macroeconômicos, estratégias, cooperação, parcerias, produtos, unidades de produção e mercados” (Battaglia, 1999, p. 208). A autora apresenta uma figura extraída do livro de Jakobiak (1995), que visualmente apresenta as diferenças nos diversos tipos de informação, conforme figura 2.

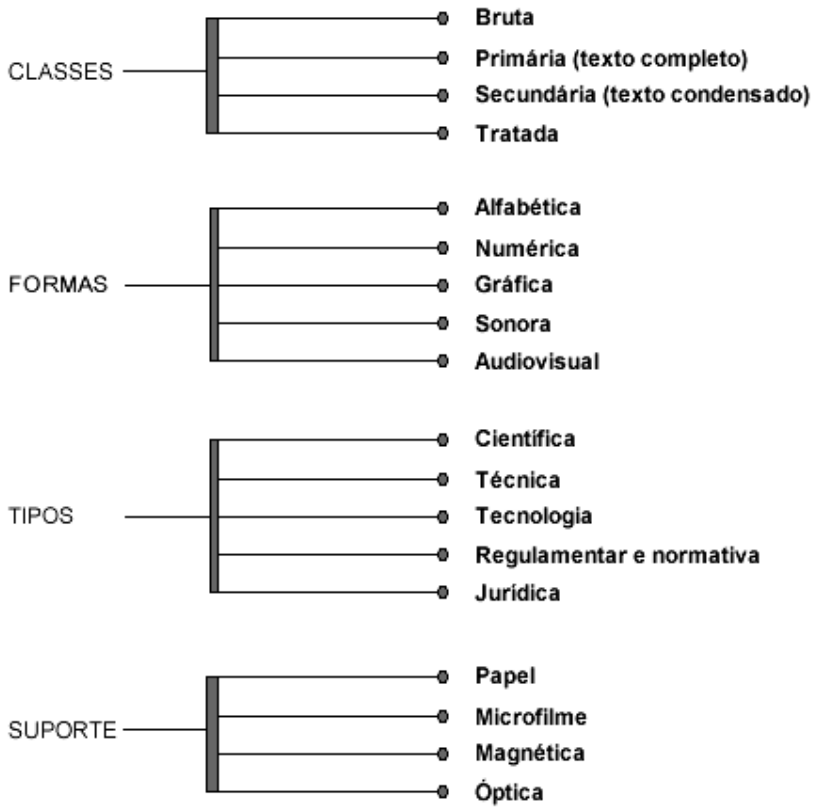

Figura 2: Tipologia de informação. **Fonte:** Battaglia (1999, p. 207)

Essa figura ilustra as características em que uma informação se apresenta em cada estágio do seu fluxo. Uma determinada informação pode ser classificada como bruta e sua forma de apresentação e divulgação se dá mediante um texto escrito; representa uma pesquisa científica e o meio de disseminação é digital ou óptico.

Basicamente estas informações estão estruturadas, armazenadas e disponíveis em fontes que, segundo Montalli, 1987 (apud Montalli, 1997) são representadas da seguinte forma: fontes de informação técnica, fontes de informação para negócio e fontes de informação científica.

A primeira fonte, **de informação técnica**, é baseada em documentos formais e legais que estão disponíveis como normas técnicas,

documentos patentes, legislação e publicações oficiais das diversas áreas. A segunda, **informação para negócios**, são os relatórios anuais de companhias, relatórios de pesquisas de mercado, levantamentos industriais, revistas técnicas, revistas de negócios, estáticas e manuais. Acrescenta-se que as organizações, associações comerciais e agências de consultores são pontos de referências para tais informações.

Em sua dissertação, Damásio (2001), faz um levantamento das informações utilizadas pelo setor industrial e percebe que, entre as informações sobre mercado, estatística sobre produto, financeira e companhia, as que mais causaram interesse para a indústria foram as relacionadas aos produtos em primeiro lugar, e a informação sobre empresas, em segundo lugar. Com isso, concluiu que as empresas estão preocupadas com o dinamismo dos produtos e quem são seus concorrentes. Enquanto a terceira fonte, **informação científica,** está relacionada à pesquisa, como monografias, dissertação, periódicos de pesquisas, artigos, índices e anais de conferências, congressos e eventos científicos.

Já Cendón (2003) compilou diversas fontes de informação para negócio, descrevendo-as como origem das seguintes informações: jurídicas, financeiras, sobre empresas e produtos, estatísticas, indicadores econômicos, oportunidades de negócios, entre outras. Seu principal objetivo neste estudo foi selecionar, descrever, compilar e avaliar fontes brasileiras de informação no contexto empresarial, especificamente armazenadas em bases de dados.

A autora ressalta que esses procedimentos de busca das informações em bases de dados para tomada de decisão nas empresas, ainda é recente no Brasil. No entanto, a sua pesquisa encontrou um total de 134 bases de

dados voltadas ao contexto de informação para negócios, como mostra a tabela 1 abaixo (Cendón, 2003).

Tabela 1: Bases de dados por categoria de informação

Categoria de informação		Dados confirmados	Dados não confirmados	Total
Bibliográficas		02	06	08
Empresas e produtos		03	10	13
Financeiras		0	04	04
Estatística e indicadores		09	04	13
Oportunidades de negócios		01	03	04
Biográfica		00	01	01
Vocabulário		00	01	01
Investimento		00	04	04
Área Jurídica	Doutrina	03	06	09
	Legislação	27	17	44
	Jurisprudência	13	13	26
	Tramitação	02	02	04
	Vocabulário	00	03	03
Total		**60**	**74**	**134**

Fonte: Cendón (2003, p. 22).

Apesar de que o número de dados não confirmados aparece maior que os confirmados, pode-se verificar a crescente utilização desse recurso pelas organizações brasileiras. Uma outra observação é em relação às informações jurídicas que aparecem representando 64% do total de bases encontradas, enquanto as informações sobre empresas e produtos notificam 13 bases de dados

com referência às informações como, fornecedores, produtos, entidades de apoio à micro e pequenas empresas, entre outras (Cendón, 2003).

Acrescentam-se, ainda, alguns tipos de informações que são geradas no dia-a-dia das organizações e são diferenciadas quanto (Falsarella et al 2003, p.146):

- Ambiente de origem;
- Formatação;
- Uso ou aplicação

Segundo os autores, existem dois ambientes que geram informações nas organizações, o interno e o externo. As informações geradas no ambiente interno compreendem aquelas que estão limitadas e controladas pelos processos e pessoas internas; por exemplo, folha de pagamento, controle de estoques, conta a pagar, entre outras. Enquanto as informações que são geradas no ambiente externo, são as que não estão no controle da organização; porém elas são importantes, pois podem demonstrar às organizações oportunidades como também ameaças no segmento atuante, como relatório de índices econômicos, informações dos concorrentes, e outros.

Quanto ao aspecto formatação, os autores classificam dois tipos de informações: informação estruturada e informação não estruturada. Informação estruturada “é a informação codificada, sistematizada, dentro de uma estrutura pré-estabelecida” (Falsarella et al, 2003, p.147). Entende-se que, devido essa informação possuir facilidades em sua recuperação, manuseio e interpretação, ela agrega valor e significado e se torna importante nos momentos de decisões. Por outro lado, a informação não estruturada é a informação “não contextualizada, que

por si só não contribui para a leitura de uma determinada situação". Compreende-se como dados que podem ou não se transformar em uma informação estratégica, mas que, no momento, se encontra em sua forma bruta sem qualquer estruturação.

Com relação ao uso ou aplicação da informação, os autores apresentam dois tipos de informações: as estratégicas e as transacionais.

As informações estratégicas são as que atingem a organização em um todo, pois possuem uma visão macro. Ela foi estruturada compreendendo análises do ambiente interno, como pontos fortes e fracos, e do externo, como oportunidades e ameaças. Enquanto as informações transacionais são "informações referentes à operacionalização e controle das atividades imprescindíveis ao funcionamento harmônico da instituição, subsidiando a tomada de decisão do corpo técnico das unidades organizacionais" (Falsarella et al, 2003, p.147).

Para exemplificar os tipos e formatos de informações com que as organizações lidam frequentemente, Miranda (1999) apresenta algumas informações estratégicas dentro das organizações, conforme quadro 1.

Quadro 1: Tipos de informações estratégicas.

Tipos de informações	**Descrição**
Cliente	Envolve conhecer as suas necessidades quanto aos produtos ou serviços oferecidos, nos aspectos de: qualidade exigida, demanda, resistências, preferências etc.

Concorrente	Compromete-se em ter informações como: características dos concorrentes, sua reputação no mercado, preços praticados, prazos administrados, participação no mercado, serviços e produtos ofertados, entre outros.
Cultural	Informações sobre o publico alvo, no que tange a educação, aos meios de comunicação, hábitos culturais como, teatro, cinema, exposições, pinturas etc.
Demográfica	São informações sobre a quantidade de pessoas que estão sendo alcançadas, distribuição da população (idade, sexo, raça, área geográfica, nível de renda, crença), etc.
Ecológica	Informações sobre as leis de preservação do meio ambiente (áreas verdes, matas, recursos hídricos), normas como a ISO 14000, por exemplo, que trata das questões de preservação do ambiente, e são estratégicas.
Econômica ou financeira	Relacionam-se as informações de índices estratégicos financeiros, conjuntura econômica nacional e mundial, segmentos de mercado, incentivos fiscais, tributos, entre outros.
	Sobre seu perfil, ações, localização, condições de transporte, preços, prazos de pagamento,

Fornecedor	descontos, disponibilidade quanto a formação de parcerias etc.
Governamental ou política	Envolvem-se as informações do Poder Executivo no que se refere às regulamentações, ação social, as políticas fiscais, exportação e importação, planas de governo etc.
Legal	Compreende as informações dos Poderes Legislativo e Judiciário que envolve legislação tributária, fiscal, trabalhista, sindical, comercial, propriedade autoral e tecnológica.
Sindical	Informações sobre capacidade de mobilização, acordos trabalhistas, integração como outros sindicatos, tendências ideológicas, representação parlamentar etc.
Social	Informações sobre tendências dos segmentos socioeconômico, diferenças entre as classes sociais, poder aquisitivo, estrutura política e ideológica, atuação das ONGs.
Tecnológica	Representa informações sobre pesquisas em andamento, tendências de pesquisas, desenvolvimento nacional e internacional, impactos de mudanças tecnológicas.
	Outras informações surgem diariamente a cada

Outras	dia no âmbito organizacional.

Fonte: Miranda (1999, p. 5).

Observa-se a informação no contexto organizacional como um elemento chave para dar base e consistência às diversas decisões que surgem. No entanto, é importante que essas informações estejam organizadas e classificadas dentro de parâmetros de valores e utilidade nas organizações. Para tanto, Amaral (1994) e Moresi (2000) apresentam um quadro ilustrativo que estabelece as classes da informação.

- Informação crítica;
- Informação mínima;
- Informação potencial;
- Informação sem interesse.

Com relação à informação crítica, esta significa a própria sobrevivência da organização (Moresi, 2000). Ela é imprescindível na luta por vantagens competitivas e deve estar presente no momento certo para as tomadas de decisões.

Quanto à informação mínima, diz respeito àquela que é necessária para o funcionamento normal das organizações. Ela representa as exigências legais, as características de seus produtos ou serviços, o foco de atuação, seus clientes, entre outras.

Com relação à informação potencial considera-se aquela que fornece ou cria vantagens competitivas nas empresas. Conforme Araújo (1995, p.2), essa informação geralmente está presente em sistemas de informação como

documentos e são “organizadas, processadas e recuperadas com a finalidade de maximizar o uso”. Apesar de a autora estar preocupada com a forma como os sistemas de informação se comportam em relação ao processamento das informações, demonstra a existência de uma classificação da informação e que as mesmas possuem diferentes níveis de prioridade em seu gerenciamento.

A informação sem interesse é a que, após uma analise de sua origem, formatação e uso ou aplicação, percebe-se que a mesma não representa valor de decisão ou estratégico no processo decisório (Moresi, 2000). Conforme Amaral (1994, p.29) essa informação é considerada como nada e deve ser reconhecida como lixo. Moresi (2000, p.15) salienta, ainda, o cuidado de não desempenhar esforços para tal tipo de informação, evitando assim desperdício de recursos em seu tratamento.

Em decorrência das classes de informação apresentadas e seus impactos no processo de decisão, verifica-se a necessidade das organizações que pretendem prevalecer no ambiente competitivo vigente, conhecer bem o seu ambiente interno e externo, via um processo que Oliveira (2003) chama de “diagnóstico estratégico” que, basicamente, significa ter conhecimento dos fatores que podem influenciar direta ou indiretamente a empresa, envolvendo a busca e o gerenciamento de diversos tipos de informações.

Conclui-se que a garantia e a certeza de que estas informações estão circulando adequadamente sem perturbações que alteram sua real forma de ser, só é observável através de análises, adoção de normas e políticas de segurança da informação.

2.2 Segurança da Informação

Segundo Aurélio (1975), a palavra segurança envolve o “ato ou efeito de segurar, afastamento de todo perigo, condição do que está seguro, confiança e prevenir-se”. A palavra segurança vem do latim *securitas,* significa garantia de integridade tanto de pessoas, como bens e instituições. Porém há uma diversidade de contextos para o uso da palavra segurança, como seguranças empresariais, físicas, patrimoniais, públicas, entre outras.

Na verdade, desde o primórdio da raça humana, todos buscam, de alguma forma, algum tipo de segurança. Porém, o termo Segurança da Informação tornou-se mais notável a partir da valorização da informação como um bem decisório e peça fundamental nas estratégias organizacionais, como também da configuração de um ambiente que Castell (1999) chamou de “era da informação”.

Tendo em vista que o termo informação transcende e possui significado em diversos segmentos sociais, econômicos, políticos e organizacionais, resta visualizá-la como um ativo especial dentro das organizações e que merece a atenção de todos (profissionais, acionistas, executivos, clientes, fornecedores) no tocante a sua proteção.

Conforme Fontes (2006):

> “Informação é um recurso que move o mundo, além de nos dar conhecimento de como o universo está caminhando (...). É um recurso crítico para realização do negócio e execução da missão organizacional” (p.2).

Portanto, à medida que as organizações possuem suas informações em ambientes informatizados e compartilhados, percebe-se a

necessidade de protegê-la da melhor forma possível. Sendo assim, o principal objetivo da Segurança da Informação é garantir que a informação não seja de forma alguma adulterada ou sofra qualquer tipo de uso indevido e não esteja indisponível quando necessário.

A necessidade de uma maior conscientização com relação à Segurança de Informação tem levado as organizações proverem as mais diversas táticas e métodos, seja na divulgação ou no estabelecimento de padrões de segurança. Os envolvidos neste processo deixam de ser somente a alta administração e os funcionários internos, mas estendem-se para os fornecedores, os terceirizados ou outras pessoas e entidades que tenham acesso direto ou indireto às informações.

Tem-se observado, na prática, que os alvos principais em um programa de conscientização da Segurança de Informação limitam-se aos que estão de forma visível em contato direto com as informações, como os executivos e funcionários, por exemplo. Porém, para um funcionamento adequado, as políticas de segurança devem alcançar os envolvidos nos processos organizacionais, ou seja, o conceito de integridade, confidencialidade e disponibilidade das informações, é um dever de todos, como acionistas, fornecedores, terceirizados e/ou quaisquer prestadores de serviços diretos ou indiretos nas organizações. Por isso, autores como Ferreira (2003, p.1) e Alves (2006) esclarecem que a Segurança da Informação “visa proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios”.

Partindo dessa perspectiva, com o crescente uso das Tecnologias da Informação e Comunicação (TIC) e suas facilidades de acesso, existem diversos

riscos que ameaçam as organizações. Por um lado está o conforto que as novas tecnologias propiciam, por exemplo, de um determinado ponto do planeta ter-se acesso à informação em lugares que estão geograficamente muito distante, realizar transações comerciais instantâneas e compartilhar conhecimento. Do outro, as novas tecnologias estão sujeitas às diversas vulnerabilidades que são propagadas imediatamente às suas descobertas, tendo como resultado a proliferação de técnicas e possíveis "profissionais" que podem causar altos prejuízos em diversas empresas.

As literaturas que tratam sobre as questões de ameaças e técnicas de segurança os classificam de diversas maneiras. Para Geus e Nakamura (2003), existem os chamados *Script kiddies*, *Cyberpunks*, *Coders*, *White hat*, *Black hat* e *Gray hat, Insiders* e Engenheiro social. São nomenclaturas que designam as funções desses grupos. Conhecer suas metodologias de ataques, como também suas verdadeiras funções, é essencial para melhor se proteger.

Numa tradução literal, os garotos dos scripts (*Script Kiddies*), são geralmente novatos na arte de explorar vulnerabilidades. Muito embora possam ser pessoas que tenham um bom conhecimento de programação, sistemas operacionais e redes de computadores, eles são verdadeiros aventureiros que "vasculham" *sites* que fornecem scripts prontos, sem mesmo entenderem em profundidade os códigos e metodologias em execução. Os *scripts kiddies* têm causado grandes prejuízos em organizações que não tem adotado os princípios básicos de Segurança da Informação ou consideram os procedimentos de SI como algo secundário.

Cyberpunks é um grupo que, além do profundo conhecimento do que realmente eles estão fazendo, caracterizam-se também como um grupo étnico

que tem sido objeto de estudo da Ciência Social há alguns anos. Mas sua verdadeira função é descobrir vulnerabilidades em sistemas e aplicativos, por pura diversão ou *hobby* e liberam essas informações na Internet ou até mesmo para as empresas responsáveis (Geus e Nakamura 2003).

Segundo os autores, os *Coders* são profissionais que já tiveram uma experiência no mundo dos *hackers* e usam essas experiências para escreverem artigos de revistas, manuais e livros. Eles também proferem palestras, seminários, aulas em Universidades e são consultores de segurança. Há o exemplo de Kevin Mitnick, considerado um dos maiores *hackers* nas últimas décadas do século 20. Ainda na sua infância já praticava fraudes na escola em que estudava, fazia ligações telefônicas gratuitas e andava de graça no sistema de transporte do Los Angeles. Depois de várias infrações, foi preso em 1995 e solto em 2000 e, durante o período de três anos, em liberdade condicional, trabalhou como consultor de segurança e lançou dois livros na área (Geus e Nakamura 2003).

Os chapéus brancos (*White hat*) são considerados os "*hackers* do bem", pois prestam serviços de teste de segurança nas organizações. Suas funções são reconhecer os pontos frágeis e vulneráveis e aplicar correções. A grande questão é até que ponto as empresas podem confiar os seus ambientes corporativos para acessos e testes por uma equipe de possíveis "*hackers*"?

Os chapéus pretos (*Black hat*) são os "*hackers* do mal". Seus principais objetivos são roubar informações confidencias das organizações e as venderem para as mesmas ou para outras empresas ou pessoas interessadas. Todo esse processo envolve uma quantia considerável de dinheiro. Um exemplo, os *hackers* invadiram o sistema de banco de dados da empresa Creditcards.com e roubaram 55 mil números de cartões de créditos e exigindo 20 mil dólares para não

tornar pública essa informação (Geus e Nakamura, 2003). Como todas as organizações se preocupam com o fator reputação, este tipo de “crime” tem-se alastrado no ambiente virtual. São comuns os dados ou informações importantes serem vendidas para concorrentes, imprensa ou empresas especializadas em chantagem empresarial.

Os chapéus cinzas (*Gray hast*), são *Black hat* com aparência de *White hat*. Na verdade, eles se apresentam como “*hackers* bonzinhos” para se infiltrarem nas organizações como consultores de segurança, mas com segundas intenções. Há exemplos de diversas empresas que os contrataram, porém eles tornaram públicos diversas vulnerabilidades dessas organizações sem terem o mínimo cuidado de preservarem a confidencialidade das informações. Os meios usados para divulgação destas informações são geralmente boletins em sites de *hackers (*Geus e Nakamura 2003).

Em uma entrevista, Gray (2004), um dos agentes de segurança mais reconhecidos na atualidade, informou que cerca de 70% dos casos de invasões causadas por *hackers*, têm, como ponto de vulnerabilidade nas redes corporativas, os seus próprios funcionários. É neste cenário que surge a figura dos *Insiders*, que podem ser funcionários, ex-funcionários ou terceirizados. Como decorrência desse fato, os *Insiders* muitas vezes não são fáceis de serem detectados, devido aos acessos dentro das organizações, como também ao tempo disponível para verificar mesas, salas dos servidores e até mesmo os lixos.

Esses atacantes tornaram-se para as empresas, motivo de preocupação no momento da adoção de normas e políticas de segurança da informação. Há vários exemplos de empresas que sofreram grandes prejuízos por um funcionário facilitar o acesso a informações, ou ex-funcionários que, ao se

sentirem injustiçados, praticam más ações. Geus e Nakamura (2003), no seu livro Segurança de Redes, citam exemplo de um ex-funcionário que pegou 41 meses de prisão por instalar uma "bomba lógica"[1] no seu antigo emprego. Esse procedimento causou o prejuízo de 10 milhões de dólares.

Outro agente comum na atualidade é engenheiro social que desenvolve a habilidade de conseguir informações confidenciais através da persuasão ou manipulação, uma vez que o elo mais fraco dentro de qualquer política de segurança é o ser humano. Mitnick (2003), em seu livro "A arte de enganar", cita o trabalho do psicólogo Robert B. Cialdini, que aborda seis tendências para o ser humano se entregar a um pedido de informação.

A primeira tendência é **autoridade** que exerce uma forte influência no comportamento das pessoas subordinadas, ou seja, uma pessoa que contata o departamento de processamento de dados e se apresenta como diretor do departamento de marketing, por exemplo, terá maiores chances de obter informação de um novo produto que a empresa está para lançar. A segunda tendência é a **afabilidade**; nessa, as pessoas se apresentam de forma prestativa, criando assim um ambiente amigável. Já a terceira tendência fala da **reciprocidade** e diz respeito a sentir-se inclinado(a) a ajudar ou fornecer informações, simplesmente por ter sido favorecido em algum momento. A quarta tendência é a **consistência**, por meio da qual os indivíduos se comprometem em cumprir suas promessas declaradas. A quinta tendência é a **validação social**, dá importância àquilo que é aceito pela maioria, tornando-se, assim, em um padrão de comportamento. Por último, a sexta tendência é a **escassez**. As pessoas tendem a

---

[1] Bomba lógica é um programa que tem como objetivo destruir dados ou hardware de computadores,

sentir-se bem quando detêm informações que estão em “falta” ou restritas a poucos e orgulham-se de as apresentarem.

Diante disto, percebe-se a necessidade de adoção de um Plano de Segurança da Informação nas organizações. Para tanto, este trabalho deve ser desenvolvido por um profissional que esteja atento às mudanças organizacionais, tecnológicas e pessoais.

2.3 Profissional de Segurança da Informação

As técnicas de ataques utilizadas no mundo virtual são renovadas e sofisticadas rapidamente. Os profissionais responsáveis pelo planejamento de segurança da informação devem conhecer as possíveis vias de ataques e se precaver ou, no mínimo, estabelecer algumas práticas básicas de segurança da informação. No entanto, podem surgir as seguintes perguntas: quem é o profissional responsável pela Segurança da Informação dentro de uma organização? Qual o seu perfil? É um profissional de origem tecnológica?

Há um consenso de que o perfil desse profissional envolva não somente um conhecimento técnico, mas também um conhecimento de negócio. Com a globalização e mudanças nas estruturas organizacionais, desaparece o profissional especialista e entra em cena o profissional que conhece um pouco de cada área. As funções fundem-se como se não houvesse barreiras ou limites entre si, tendo como resultado um profissional multitarefa.

Segundo a 2ª Pesquisa Nacional sobre o perfil do profissional de Segurança da Informação (*Modulo*, 2004), mais da metade dos entrevistados classificaram os cargos de *Securty Officer,* Consultor de Segurança e Gerente ou

---

de forma programada.

Coordenador de Segurança, como os mais próximos para atuarem nesta função. A pesquisa apresenta também uma corrida pela especialização por parte desses profissionais.

O *Security Officer* ou Consultor de Segurança é a pessoa responsável pela implementação e cuidado com a segurança nas organizações. Segundo Sêmora (2003), é um executivo com várias especialidades, com uma visão completa e profunda da Segurança da Informação, com um conhecimento amplo de gerenciamento de projetos, coordenação de equipes e liderança. Ele ressalta a importância de esse profissional ter, como fator primordial, o alinhamento dos planos de segurança com as necessidades de negócio ou estratégias da empresa. Segundo o autor ele, deve: conhecer o negócio da empresa, o segmento de mercado, o plano de negócio da empresa e as expectativas da organização. Na visão de Ferreira (2003), este profissional é responsável pelo gerenciamento das políticas de Segurança da Informação.

Suas funções se dão na:

> "Área de segurança e da infra-estrutura organizacional para tratamento da segurança da empresa; Planejamento dos investimentos para a segurança da informação; Definição dos índices e indicadores para análise do retorno do investimento; Definição, elaboração, divulgação, treinamento, implementação e administração do plano de segurança, da política de segurança, análise de risco, plano de auditoria de segurança, relatórios de diagnóstico do nível de segurança, conformidade e atendimento a legislação vigente e investigação sobre incidentes de segurança".

Ferreira (2003) acrescenta às funções desse profissional, além da necessidade de conhecimento dos negócios como apresentado por Sêmora (2003),

a constante carência de atualização e acompanhamento das novas tecnologias que surgem, ou seja, o profissional de segurança deve estar atento para as rápidas mudanças que ocorrem e possíveis vulnerabilidades que elas podem apresentar. Na verdade, este profissional, além do perfil apresentado pelos autores acima, pode-se descrevê-lo como uma pessoa pró-ativa, ou seja, alguém que tem uma habilidade de trabalhar e antecipar futuros problemas, ser ágil e competente. Pode ser descrito como uma profissional da informação que Valentim (2000) definiu como "observador, empreendedor, atuante, flexível, dinâmico, ousado, integrador, pró-ativo".

Na estrutura organizacional, Ferreira (2003) sugere que esse profissional esteja em um departamento ligado direto com a diretoria ou presidência da empresa, ou seja, que não esteja ligado ao setor de informática ou auditoria simplesmente, como é comum nas empresas.

Propõe ainda a criação de dois comitês, o comitê corporativo e o interdepartamental. O comitê corporativo se constitui de diversos executivos dos vários departamentos da empresa, formando, assim, visões distintas. Seu principal papel é "organizar, concentrar e planejar as ações de segurança". Já o comitê interdepartamental se posiciona em ambientes específicos, porém respondendo às diretrizes definidas pelo comitê corporativo.

Contudo, com o crescimento e surgimento de diversas empresas que trabalham com auditoria, implementação e treinamento em segurança da informação, as organizações podem optar pela não criação de comitês e sim por contratarem serviços de terceiros. Entretanto, são inegáveis os riscos na escolha e contrato destas empresas, pois afinal são ativos importantes que as organizações estarão disponibilizando para elas, sendo necessária uma atenção especial às

cláusulas de responsabilidade de ambas as partes na formulação do contrato.

2.4 Tipos de ataques

Existem alguns conhecidos ataques a que os profissionais de segurança devem estar atentos no momento da elaboração de um Plano de Segurança da Informação (PSI). Até agora foram descritas algumas denominações dadas para os “profissionais” que atuam no mundo dos *hackers*; no entanto, é necessário conhecer alguns modelos de ataques usados para obter as informações confidenciais ou para causar algum tipo de prejuízo às organizações.

2.4.1 Dumpster diving ou trashing

Este tipo de ataque é um pouco diferenciado dos demais que utilizam tecnologias ou elementos psicológicos. Ele consiste em procurar, no lixo, papéis ou qualquer outro meio onde constem informações confidenciais que venham a comprometer a confidencialidade e integridade da empresa ou de pessoas individuais. Muitas informações importantes têm sido descartadas de forma errada. Às vezes, são informações que, aparentemente, não são tão importantes no momento, porém nas mãos de uma pessoa mal intencionada, servem de complemento e suporte para um plano de ataque. Por exemplo, muitos utilizam senhas de acesso a um servidor importante da empresa, conta de banco eletrônico, conta de e-mail, gravadas em pedaços de papéis. Ao passar dos tempos, os papéis são desgastados e precisam ser substituídos por outros. Nesse momento, a lixeira mais próxima recebe estas informações sem o mínimo de cuidado de picotá-las ou eliminá-las. Os *insiders* são os atacantes que utilizam com uma maior freqüência este tipo de técnica, pois, geralmente, como descrito anteriormente, são os próprios funcionários da empresa, ex-funcionários ou fornecedores que possuem acesso a locais “privilegiados” das organizações. Eles podem também estar inseridos no

departamento de limpeza das organizações, sendo eles próprios responsáveis pelo recolhimento dos lixos (Geus e Nakamura, 2003).

2.4.2 Ataque físico

Há uma tendência de acreditar que a maioria dos ataques aos sistemas informacionais ocorrem somente via ambiente lógico, vias de bits e bytes e Internet. Porém, no mundo da "violência virtual", as origens dos ataques podem partir de diversas maneiras envolvendo acessos físicos.

O cuidado com a segurança física dos sistemas é primordial num PSI. Pois de nada valeria investir em softwares de segurança, altas tecnologias, se o acesso físico aos equipamentos representa a maior vulnerabilidade (Geus e Nakamura, 2003).

2.4.3 Informações livres

As informações livres são, na verdade, os meios utilizados para um ataque. Com uma gama enorme de informações produzidas, principalmente, pela Internet, tem-se facilitado o acesso a dicas, como fazer e fóruns de discussões, que são fontes utilizadas especialmente pelos *scripts Kiddies.*

Classificam-se, também, como informações livres, aquelas que, aparentemente, não têm nenhum significado no fornecimento ou por algum descuido. Por exemplo, as pessoas que participam de fóruns, descrevem suas verdadeiras tipologias de redes, versão de sistemas operacionais, seus endereços reais e os meios de contato (telefones e e-mails). Essas informações são vitais aos atacantes (Geus e Nakamura, 2003).

2.4.4 Packet Sniffing

Este tipo de ataque se caracteriza pelo uso de programas que

fazem varredura na rede e capturam pacotes. Muitas informações que circulam nas intranets e Internet, não possuem nenhum tipo de criptografia ou códigos de segurança que dificultem a sua visualização em caso de uma interceptação. Exemplificando esta ação, pensa-se em laboratório de informática, que esteja interligado com *hubs* e, um atacante utilizando uma máquina dentro da mesma rede pode usar vários *softwares* de captura (*nmap, ethereal, tcpdump,* entre outros), para ter acesso a todo tráfico da rede. Se, neste momento, outro usuário estiver acessando um servidor qualquer com seu usuário e senha, sem os devidos cuidados ou com programas que não trabalham com nenhum tipo de criptografia nos dados, suas informações estão vulneráveis, podendo ser acessadas e visualizadas (Geus e Nakamura, 2003).

2.4.5 Port scanning

Este é um ataque comum e ainda muito utilizado. Ele acessa as portas e serviços disponíveis em um servidor e, com tais informações, verifica as versões dos serviços habilitados. Por exemplo, utiliza-se um programa que acessa um determinado servidor Apache ou ISS – servidores de WEB. Verifica-se que a porta padrão desse serviço está aberta (porta 80), e qual a sua versão. Com essas informações, uma simples busca no site Google, mostrará se para esta versão existe alguma vulnerabilidade, como também os procedimentos para um ataque. Este tipo de ataque é comum em Instituição de ensino, com a distribuição de pontos de redes em salas de aula, auditórios, diretórios acadêmicos, etc. (Geus e Nakamura, 2003).

2.4.6 Ataques às redes sem fio

Com o surgimento das tecnologias sem fio, outros tipos de ataques surgem para os ambientes que estabelecem estes padrões. Uma grande diferença é que os dados deixam de trafegar via redes cabeadas e, basicamente, apenas para o entendimento, passam a usar o espaço para seu fluxo, ou seja, por meio de ondas de rádio. O cuidado com o perímetro de segurança aumenta, pois envolve sinais que, facilmente, podem transpor barreiras físicas. No entanto, como envolve novas tecnologias, os ataques ocorrem com maior freqüência, devido a muitos usuários destas tecnologias, não ativarem a segurança mínima disponível.

2.4.7 Ataques de negação de serviços

Basicamente este ataque envolve uma sobrecarga de conexões em um servidor, ou seja, o número de conexões estabelecidas em um servidor WWW, por exemplo, excede a quantidade suportada. Na atualidade, esta técnica progrediu bastante. Utilizam-se ataques distribuídos, em que várias máquinas de diversas partes do mundo são programadas para executarem uma ação desse tipo em um dia, hora e minuto marcado. Pior, muitas dessas máquinas são de pessoas que não estão cientes de sua participação no ataque (Geus e Nakamura, 2003).

Como pode ser observado, são diversas as técnicas de ataques e, a cada dia, surgem novas formas que ameaçam as organizações, as pessoas e a sociedade. Sejam por novas tecnologias que entram no mercado, ou mesmo, por vulnerabilidades descobertas às existentes. Em decorrência desses fatos, as organizações estão cientes de que o investimento em normas e padrões de segurança da informação passa a ser um bem necessário, além de influenciar diretamente a sobrevivência do negócio, principalmente aqueles que trabalham com tecnológicas da informação tendo a informação como o fator competitivo. Dawel

(2005), escrevendo sobre a importância de se trabalhar esta temática, define Segurança da Informação como “redução e administração dos riscos relativos ao negócio, a fim de que a empresa continue no mercado por muito tempo, contribuindo para uma boa rentabilidade aos investimentos dos acionistas e evitando perdas desnecessárias”.

Percebe-se que as questões de segurança da informação envolvem um processo ou ciclos e que, se não houver atenção ou implementação de planos de segurança adequados, todas as áreas da empresa se tornam vulneráveis. Portanto, pensar em um Plano de Segurança da Informação é acreditar na própria sobrevivência da organização.

2.5 Norma ISO/IEC 17799:1

Existem padrões ou normas específicas em Segurança da Informação que, além de fornecer orientações práticas de segurança, também habilitam as empresas que adotam algumas certificações. A utilização de normas ou padronizações tem se tornado real em várias organizações. Essas normas são reconhecidas internacionalmente e são utilizadas como diferencial competitivo. Sêmora (2003) define normas como “regras, padrões e instrumentos de controle que dêem uniformidade a um processo, produto ou serviço”. Devido às exigências por qualidade nos serviços, produtos e operações, as organizações submetem-se a controles e outros tipos de auditorias. Este é um processo adicional nas empresas que implementam condições de confiança diante da sociedade. Exemplos de normalizações são a família ISO 9000, que trata da qualidade e ISO 14000 que trabalha com o meio ambiente.

Entre as mais conhecidas do mercado, tem-se a ITIL - *It infrastructure library* - que fornece uma documentação criada pelo governo do Reino

Unido, recomenda ações práticas em gestão de TI; o COBIT – *Control objectives for information and related technology* – possui parâmetros para gestão e auditoria no tocante a segurança da informação; ISO *Guide 73,* ISO 13335 (Beal, 2005), entre outras. Elas são exemplos de orientações concernentes às tecnologias da informação e sua proteção. Neste trabalho, dá-se atenção a ISO/IEC 17799:1, uma norma específica na parte prática da segurança da informação e adotada por diversas organizações.

Com a crescente utilização dos meios tecnológicos e valorização das informações utilizadas, seguindo as diretrizes de normalização, a partir de 1995 iniciou-se no Instituto de Padrões Britânico a publicação de orientações para proteção e cuidado com as informações importantes. À primeira versão deu-se o nome BS 7799, um padrão que trata das questões da Segurança da Informação de forma prática. Em 1998, o mesmo instituto publicou a primeira versão BS 7799-2 que trata sobre a Gestão da Segurança da Informação – especificação e guia para o uso. Porém, somente no ano de 2000, a norma tornou-se internacionalmente conhecida, quando homologada pela International Organazation for Standardization – ISO, nomeada como ISO/IEC 17799:1.

A norma ISO/IEC 17799:1 é formada por dez domínios voltados para Segurança da Informação, que envolve os princípios básicos de segurança e/ou contribui para um ponto de partida na criação de políticas, normas e procedimentos de gestão em empresas de pequeno, médio e grande porte. A seguir são apresentadas tais práticas:

1.Política de segurança;

2.Segurança organizacional;

3.Classificação e controle de ativos de informação;

4.Segurança em pessoas;

5.Segurança física e do ambiente;

6.Gerenciamento das operações e comunicações;

7.Controle de acesso;

8.Desenvolvimento e manutenção de sistemas;

9.Gestão da continuidade do negócio;

10.Conformidade.

2.5.1 Política de segurança

É um domínio que tem como objetivo fornecer orientação de segurança da informação à direção da organização. É a formalização dos ativos importantes, como estão classificados e como serão protegidos. Para tanto, a adoção de políticas, regras, procedimentos e práticas, devem partir ou serem apoiadas, primeiramente, pela alta administração da empresa, de forma que a sua implementação alcance toda estrutura organizacional como os seus principais gestores e cooperadores (NBR ISO/IEC 17799:1, 2000).

Segundo Sêmora (2003, p. 105) uma política de segurança tem como objetivo estabelecer “padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa”. Ele acrescenta que a implementação destas diretrizes demonstra a importância que a empresa oferece às informações estratégicas e também o seu devido valor a todos os funcionários.

Para Geus Nakamura (2003, p. 173), a política de segurança é “a

base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações". Segundo os autores, a elaboração de uma política é a base que fundamentará todas as estratégias de proteção nas empresas, pois ela envolve aspectos humanos, culturais e tecnológicos alinhados aos processos, negócios e legislação existentes.

Sendo assim, após essas definições, a norma propõe a elaboração de um documento nomeado como "documento da política de segurança da informação", que tem como objetivo - além de descrever as informações como: definição da segurança da informação; resumo das metas e importância destas; o comprometimento da alta direção e definição das responsabilidades na gestão da segurança visando a registrar as políticas que todos deverão seguir apoiada e em conformidade com a legislação e cláusulas contratuais existentes.

Acrescenta-se a isso a necessidade de um gestor que seja responsável pela análise crítica do ambiente e manutenção periódica. Devido à dinâmica e mudanças que ocorrem rapidamente tanto nos processos de negócio, quanto no surgimento de novas tecnologias, afetando diretamente os aspectos de segurança, este profissional frequentemente analisa as seguintes necessidades (NBR ISO/IEC 17799:1, 2000, p. 5):

- A efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados;
- O custo e impacto dos controles na eficiência do negócio;
- Os efeitos das mudanças na tecnologia.

2.5.2 Segurança organizacional

Neste domínio, a NBR ISO/IEC 17799:1 apresenta recomendações

práticas de gerenciamento da segurança dentro da organização.

> "Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização. Convém que fóruns apropriados de gerenciamento com liderança da direção sejam estabelecidos para aprovar a política de segurança da informação, atribuir funções da segurança e coordenar a implementação da segurança através da organização" (Op.cit., p. 5).

A segurança organizacional é o processo de conscientizar as fontes decisórias da estrutura organizacional da necessidade de estabelecer políticas, regras, procedimentos de segurança da informação.

2.5.3 Classificação e controle dos ativos de informação

Este domínio da norma é de suma importância, pois, além de mapear todos os ativos existentes na organização, orienta a uma classificação das informações por prioridades. Esta classificação leva a organização a perceber quais são as informações mais importantes e o seu tratamento. Para tanto, é proposto um inventário de todos os ativos de informação para verificação se os mesmo estão sendo protegidos adequadamente.

Esta classificação da informação viabilizará qual o nível de proteção deverá ser adotado para cada ativo, pois as informações possuem características distintas em seus diversos contextos. A NBR ISO/IEC 17799:1 define este tópico assim:

> "A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém 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” (p. 10).

No que se refere às recomendações de classificação das informações a norma apresenta as seguintes orientações:

- Sejam consideradas as necessidades dos negócios para compartilhar ou restringir o acesso, além de avaliar os impactos nos negócios em caso de acesso indevido ou danos da informação;
- Os dados provenientes de sistemas que processam informações sejam rotulados de acordo com o seu valor, sensibilidade e criticidade para a organização;
- Freqüentemente a informação deixa de ser sensível ou crítica ao longo do tempo. Assim, isso precisará ser considerado e deverá ocorrer a previsão para a sua reclassificação, evitando uma classificação fixa. Isso evitará gastos desnecessários;
- Evite criar muitas categorias de classificação, pois o excesso poderá prejudicar o resultado final de sua aplicação;
- A responsabilidade pela definição da classificação de um item de informação fique como o autor ou com o proprietário responsável pela informação.

2.5.4 Segurança em pessoa

Tem como objetivo reduzir os riscos de erros humanos, fraudes, roubos e uso indevido das instalações. Para tal, é necessária uma documentação de procedimentos e políticas e que todos da organização tenham conhecimento, desde a alta administração até as áreas operacionais. Acrescentam-se aqui, as

determinações de responsabilidades de cada um e o grau de confidencialidade conforme a política de segurança adotada.

A norma esclarece de forma fácil este tema que atenta para os seguintes objetivos: “Reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações”, de forma que os profissionais, mesmo antes de se inserirem na organização, sejam orientados quanto às suas responsabilidades, os itens que compõem os contratos de segurança da informação e, dependendo do grau de relevância da informação em contato, é necessário que os funcionários, prestadores de serviços e outros usuários, assinem um acordo de sigilo (NBR ISO/IEC 17799:1, 2000, p. 10).

2.5.5 Segurança física e do ambiente

A norma apresenta como objetivo deste domínio prevenir as organizações quanto ao acesso não autorizado, dano e interferência às informações e instalações físicas.

> “Convém que os recursos e instalações de processamento de informações críticas ou sensíveis do negócio sejam mantidos áreas seguras protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso” (NBR ISO/IEC 17799:1, 2000, p. 13).

Preocupa-se com acesso a lugares não permitidos às instalações físicas da organização. Salienta que os recursos críticos devem ser mantidos em lugares com uma devida segurança onde se estabelece perímetro de segurança física. É necessário um controle de entrada e saída. Os equipamentos devem ser devidamente seguros.

2.5.6 Gerenciamento das operações e comunicações

A norma coloca a necessidade de elaborar uma documentação com procedimentos de atualização de sistemas, novas configurações, registro de incidentes, políticas de backup ou cópias de segurança, gerenciamento de rede, gerenciamento de funções e separação dos ambientes de desenvolvimentos e de produção.

> "O objetivo é garantir a operação segura e correta dos recursos de processamento da informação. Recomenda-se que se utilize a segregação de funções, quando apropriado, para reduzir o risco de uso negligente ou doloso dos sistemas" (NBR ISO/IEC 17799:1, 2000, p. 17).

2.5.7 Controle de acesso

Usa requisitos de segurança que envolve uma documentação explicita sobre todos os controles de acesso como identificação dos usuários e grupos, privilégio de acesso para cada usuário ou grupo, regras de acesso, responsabilidades de cada um, políticas de senhas, análise critica dos direitos, autenticação, entre outros.

> "Objetivo é controlar o acesso à informação e este acesso seja controlado na base dos requisitos de segurança e do negócio. Levando em consideração as políticas de autorização e disseminação da informação" (NBR ISO/IEC 17799:1, 2000, p. 27).

2.5.8 Desenvolvimento e manutenção de sistemas

Propõe que todos os requisitos de segurança sejam implementados no momento de desenvolvimento dos sistemas. Estão inclusos, a validação de dados de entradas, autenticação de mensagem, criptografia, assinatura digital,

entre outros. A NBR ISO/IEC 17799:1 tem definido o seguinte para este item:

> "Garantir que a segurança seja parte integrante dos sistemas de informação, incluindo a infra-estrutura, aplicações do negócio e aplicações desenvolvidas pelo usuário. O projeto e a implementação dos processos do negócio que dão suporte às aplicações e aos serviços podem ser cruciais para segurança. Convém que requisitos de segurança sejam identificados e acordados antes do desenvolvimento dos sistemas de informação" (p. 38)

2.5.9 Gestão da continuidade do negócio

Ressalta a importância de planos de contingência para que as atividades de negócio e processos críticos não sejam surpreendidas por falhas que podem ocorrer em qualquer momento nas organizações. Essas falhas estão relacionadas a desastres naturais, falhas de sistemas, problemas de hardwares ou ações intencionais.

> "Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos. Que os processos de gestão da continuidade sejam implantados para reduzir, para um nível aceitável, a interrupção causada por desastres ou falhas da segurança (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) através da combinação de ações de prevenção e recuperação" (NBR ISSO/IEC 17799:1, 2000, p. 45).

2.5.10 Conformidade

Este último domínio está relacionado à conformidade com as leis vigentes do país e do mercado, com o objetivo de evitar qualquer violação a estatutos, regulamentações ou obrigações contratuais, direitos autorais, privacidade

de informação pessoal, entre outros.

Sendo assim, a norma NBR ISO/IEC 17799:1 envolve todos os aspectos práticos de segurança de informação que se propõe implementar nas organizações. Para Fontes (2006), a Segurança da Informação “é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada”.

Para finalizar este capítulo, apresenta-se o Quadro 2 que procura sintetizar as características da informação agregando-se a elas os domínios de proteção descritos pela norma NBR ISO/IEC 17799:1.

Quadro 2: Características da informação e domínios de proteção

Tipos de informação	Classificação	Fonte	Relevância	Domínios de proteção
› Invenções e inovações › Sobre produtos e serviços › Tecnologias › Conhecimento das descobertas › Cliente › Concorrente › Fornecedor › Cultural › Demográfico › Econômico › Financeiro › Governamental › Legal › Social	Informação Científica Informação Tecnológica Informação Estratégica	✓ Bases e bancos de dados ✓ Bases de patentes e normas técnicas ✓ Literatura científica ✓ Relatório técnico ✓ Teses e pesquisas ✓ Documentos internos ✓ Leis e regulamentos	Informação Crítica Informação Mínima Informação Potencial	■ Política de segurança ■ Segurança organizacional ■ Classificação e controle das informações ■ Segurança em pessoas ■ Segurança física e do ambiente ■ Gestão de operações e comunicações ■ Controle de acesso ■ Manutenção e

‣ Tecnológica ‣ Monitoramento de mercado ‣ Tomada de decisão, entre outras.	Informação para negócio	✓ Estatísticas de indicadores econômicos e empresariais ✓ Publicações governamentais	Informação sem interesse	desenvolvimento de sistemas ■ Gestão da continuidade do negócio ■ Conformidade

A análise deste conjunto de elementos – tipos de informação, classificação, fonte e relevância da informação -, auxilia a determinar os níveis de proteção adequados, sendo possível detectar quais as informações apresentam graus de importância diferenciada, considerando desde a sua origem até sua utilização. O que realmente determinará essa valorização é a análise da sua utilidade.

Por exemplo, uma informação de novos produtos a serem lançados no mercado ou desenvolvidos por uma determinada organização, pode ser denominada como informação crítica, pois estabelece vantagens competitivas diante dos seus concorrentes. Pode ainda ser classificada como informação tecnológica, devido ao conhecimento técnico, econômico e mercadológico (Aguiar, 1991). Um relatório técnico pode representar a fonte com as descrições geral e específica do produto. Sendo esta informação de suma importância para a organização, demanda um nível de proteção alto.

Em contrapartida, uma informação da legislação que rege um determinado mercado ou país, pode estar dentro do contexto de informação mínima, que representa requisitos básicos e exigências estabelecidas para um funcionamento dentro das normalidades adotadas por governo ou entidades. É uma informação pública que está disponível para todos e, geralmente, se encontra disponível em base de dados da Internet. O nível de proteção para tal informação

pode ser classificado como baixo.

Portanto, para se definir um Plano de Segurança da Informação é importante saber a origem da informação, sua necessidade e contexto de uso e fazer análise de todos os elementos com o intuito de avaliar o adequado nível de proteção exigido.

3. PLANEJAMENTO ESTRATÉGICO

O tratamento das informações estratégicas nas organizações envolve diversos fatores, como sua classificação, forma de apresentação, modo de disseminação e sua adequada utilização no dia-a-dia da empresa, entre outros. Esses fatores demandam esforço e englobam toda a organização no processo de busca e análise das informações essenciais.

Para Calazans (2006, p.64), a informação estratégica "tem como principal objetivo o uso de dados, informação e conhecimento para agregação de valor a produtos e/ou serviços, garantindo a sobrevivência da organização aos desafios atuais". Dentro desse contexto, surge a necessidade de uma ferramenta de gestão como o Planejamento Estratégico (PE). Conforme Alday (2000), a razão pela qual as organizações devem se preocupar com a implantação do PE é devida a mudanças que ocorrem no ambiente econômico, social, tecnológico e político.

Sendo assim, o objetivo deste capítulo é conceituar planejamento, estratégia, PE e verificar a necessidade de informação que esses processos demandam e utilizam.

3.1 Conceito de planejamento

Segundo Maximiano (2004, p.138), dentro da administração de empresas, quando se fala em planejamento ou planejar é "pensar e agir em relação ao futuro; tomar decisões sobre o futuro; lidar com a incerteza do futuro ou antever eventos futuros com certa precisão"; ou seja, são ações pensadas, analisadas, calculadas e realizadas num momento presente, mas seus resultados se refletem em um período subseqüente ou futuro.

Pereira (2002, p. 28) acrescenta que, além da característica "pensamento" ou reflexão citado por Maximiano (2004), o planejamento representa uma atitude de "criação, adaptação e um controle" quanto ao futuro da organização dentro de uma perspectiva estratégica. Segundo ele, pode-se considerar o "planejamento como um processo formalizado para gerar resultados a partir de um sistema integrado de decisões". Ele ainda ressalta que este processo está completamente na direção oposta do que se chama improvisação - que se entende como atitudes repentinas, pouca reflexão e suas ações são imediatas.

Conforme Oliveira (2003, p.35), o planejamento não deve ser confundido com termos como, "previsão, projeção, predição, resolução de problemas e plano". Para o autor, a **previsão** está relacionada mais com ações probabilísticas do que um pensamento racional. O processo de planejamento, que envolve ações e atitudes de pensamento, não se pode confundir com métodos que utilizam análises de uma determinada amostragem e, dependendo dos acertos e dos erros prever-se o que poderá acontecer; nem sempre os resultados probabilísticos passados se refletem nas decisões futuras. Já a **projeção** diz respeito à análise detalhada de fatos passados para se ter uma perspectiva quanto ao futuro. Porém, devido às mudanças aceleradas em todos os âmbitos das empresas, não se pode ter certeza ou estabelecer seus objetivos com base exclusivamente nas informações passadas. Como relata Maximiano (2004, p.138), "uma das razões para planejar é lidar com a incerteza do futuro", ou seja, o mercado se modifica, os concorrentes também e daí surgem novas necessidades dos clientes e novos produtos, pois tudo isso é muito dinâmico e rápido. A **predição** seria a perda do controle organizacional devido ao fato de que mudanças ocorrem diferentemente das que aconteceram no passado. Resolução de problema

se resume como uma ação imediata, ou seja, a necessidade de uma resolução em curto prazo. E por fim, o **plano**, que corresponde a uma maneira formal de estabelecer os procedimentos dentro de uma organização, porém de forma rígida sem qualquer flexibilidade.

Sendo assim, Oliveira (2003) define como verdadeiro propósito do planejamento o:

> "Desenvolvimento de processos, técnicas e atitudes administrativas, as quais proporcionam uma situação viável de avaliar as implicações futuras de decisões presentes em função dos objetivos empresariais [...] de modo mais rápido, coerente, eficiente e eficaz" (p.36).

O autor ainda acrescenta três variáveis básicas que impactam o planejamento e devem ser influenciadas por ele: as pessoas, a tecnologia e os sistemas (Oliveira, 2003), conforme figura 3.

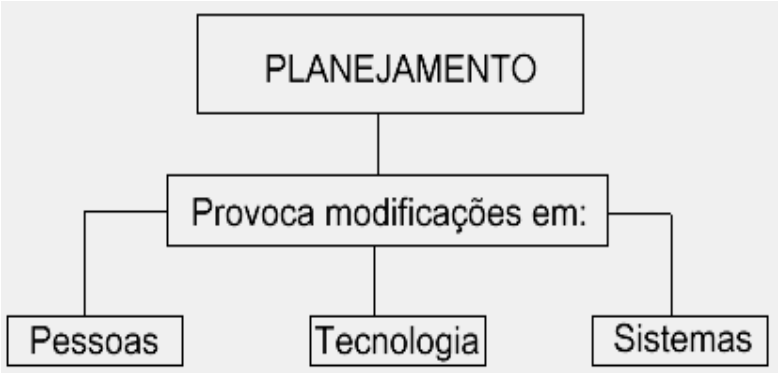

Figura 3: Modificações provocadas pelo planejamento.
Fonte: Oliveira (2003, p.38)

O impacto do planejamento nas pessoas pode acarretar mudanças do estado atual, de conforto e segurança, para um estado que, muitas vezes, envolve e exige o desenvolvimento de novas competências, a eliminação de certas

atividades, reeducação de funções e novas maneiras de controles. Ressaltam-se a importância e a influência que o fator humano desempenha no processo de planejamento. Pode-se influenciar de forma positiva ou negativa. Se as pessoas não forem convencidas das melhorias que o planejamento proporcionará, elas serão resistentes às mudanças. Porém, se convencidas dos benefícios, é um viés importante para o sucesso do planejamento.

Em tecnologia, os impactos se tornam mais evidentes, pois este segmento está em constante mudança. Novas ferramentas são adicionadas diariamente facilitando o suporte e a forma de executar determinadas tarefas. Menciona-se também, o próprio perfil das organizações atuais, que exigem um tratamento rápido e eficiente de diversas informações. Como o planejamento procura conhecer os possíveis ambientes futuros, este é um fator de grande impacto no momento de planejar.

Nos sistemas, está implícita a estrutura hierárquica organizacional, e os resultados podem ser direcionados a novas autoridades e responsáveis.

Portanto, segundo os argumentos de (Fichmann e Almeida, 1991; Pereira, 2002; Oliveira, 2003; Maximiano, 2004), pode-se considerar o planejamento como um processo dinâmico, racional e sistêmico, que fornece as diretrizes quanto às futuras ações com o máximo de antecedência possível.

3.2 Conceito de estratégia

Estratégia em grego é *strategos,* que significa literalmente “chefe do exército” (Fishmann e Almeida, 1991). Este termo tem sua gênese no ambiente militar, em que os exércitos vencedores eram aqueles que adotavam as melhores estratégias diante dos inimigos, sob a supervisão ou orientação de um capitão ou

comandante. Maximiano (2004) também descreve a origem do termo da seguinte forma: “o conceito de estratégia nasceu da guerra, em que a realização de objetivos significava superar um concorrente”. Desta forma, existia um determinado grupo com interesses comuns e, para a realização desses interesses, era necessário derrotar outro grupo que lutava pelo mesmo alvo. Segundo Ansoff (1997), estratégia “é quando a munição acaba, mas continua-se atirando para que o inimigo não descubra que a munição acabou”.

Tendo em vista a luta por interesses, objetivos, propósitos comuns que marcam as organizações atuais, houve uma transposição do termo que outrora se utilizava em um ambiente militar para a administração das empresas com os seguintes nomes: estratégia gerencial, estratégia organizacional, estratégia empresarial ou simplesmente estratégia (Maximiano, 2004).

Para Oliveira (2003), o que representa o verdadeiro propósito estratégico dentro da gestão administrativa é “estabelecer quais serão os caminhos, os cursos, os programas de ação que devem ser seguidos para serem alcançados os objetivos e desafios estabelecidos”. Independentemente do porte da organização, a maneira de gerenciamento dos recursos “físicos, financeiros e humanos” no intuito de maximizarem os seus desempenhos, é um exemplo de estratégias que tornam efetivos os objetivos propostos.

3.3 Planejamento Estratégico

Segundo Oliveira (2003, p.44), o Planejamento Estratégico se caracteriza por um “processo administrativo que proporciona sustentação metodológica para estabelecer a melhor direção a ser seguida pela empresa, visando ao melhor resultado de interação com o ambiente e atuando de forma inovadora e diferenciada”. Para se obter sucesso no desenvolvimento do PE, é

necessário que ele, primeiramente, seja reconhecido e aprovado pela alta administração da organização, independentemente do modelo aplicado: planejamento participativo, planejamento coordenado, planejamento integrado, planejamento permanente (Ackoff, apud Oliveira, 2003).

Para Almeida (2001, p.13), o PE é "uma técnica administrativa que procura ordenar as idéias das pessoas de forma que se possa criar uma visão do caminho que deve seguir. Depois de ordenar as idéias, são ordenadas as ações". A organização é uma instituição que deve ter objetivos claros e bem definidos, que deve seguir para um propósito exclusivo, envolvendo assim as pessoas que constituem elemento base de qualquer organização. Como componente dentro da organização, as pessoas possuem atribuições que devem ser combinadas a outros elementos (tempo, tecnologia, informação etc), para se alcançar de forma unânime uma direção certa. O trabalho do PE é, justamente, ordenar os interesses de maneira estruturada e eficaz.

De acordo com Fischmann e Almeida (1991, p. 25) o PE consiste em:

> "Uma técnica administrativa que, através da análise do ambiente de uma organização, cria a consciência das suas oportunidades e ameaças dos seus pontos fortes e fracos para o cumprimento da sua missão e, através desta consciência, estabelece o propósito de direção que a organização deverá seguir para aproveitar as oportunidades e evitar riscos".

Percebe-se, na definição de PE acima, a existência de termos como, oportunidades, ameaças, pontos fortes e fracos, missão e riscos. São fatores a que toda organização está sujeita e dos quais se pode beneficiar, considerando-

os positivamente (oportunidades, pontos fortes, missão) ou negativamente (ameaças, pontos fracos, riscos). Na verdade, esses fatores estão presentes independente do porte da organização, cujo conhecimento se torna fundamental na elaboração do planejamento estratégico.

Conforme Chiavenato (2000, p.148), ao se pensar em PE, deve-se considerá-lo como “um conjunto de tomada deliberada e sistemática de decisões, envolvendo empreendimentos que afetam ou deveriam afetar toda a empresa por longos períodos de tempo”. As ações e decisões que compõem o planejamento estratégico englobam toda estrutura organizacional como seus respectivos responsáveis.

Acrescenta-se, ainda, o conceito de Maximiano (2000) que considera o processo de PE como uma atividade de observação, ou seja, baseada na análise dos ambientes externos e internos da organização. Segundo o autor, este processo define objetivos que cria um vínculo entre os desafios e as oportunidades internas e externas. Dentro desse processo, existe uma seqüência de análise: “análise de situação estratégica, análise interna e externa e definição do plano estratégico, compreendendo os objetivos e a estratégias” (Maximiano, 2004, p.164).

3.3.1 Tipos de planejamento

Devido à grande quantidade de informações sobre planejamento nas organizações e, principalmente, quando se aprofunda nas teorias administrativas, segundo alguns autores, verifica-se uma classificação, às vezes a mesma em um grupo de autores ou o acréscimo de uma nova terminologia dos tipos de planejamento. Basicamente, os tipos de planejamentos são: Planejamento Estratégico, Planejamento Tático, Planejamento Operacional (Oliveira, 2003;

Maximiano, 2004), Planejamento em Longo Prazo (Fischmann e Almeida, 1991), entre outros.

Para Oliveira (2003, p. 45), o Planejamento Estratégico está relacionado com um processo que atinge a organização no seu todo, em um período de longo prazo. Já o planejamento tático trabalha com objetivos e ações que atingem partes específicas da empresa, num período de curto prazo. O planejamento operacional é definido como os planos de ação das atividades a serem desenvolvidas. Para melhor entendimento das abrangências e possíveis limites de cada planejamento, apresenta-se a figura 4 a seguir.

Figura 4: Tipos e níveis de planejamento nas organizações.
Fonte: Adaptado de Oliveira (2003, p.46).

Na apresentação da figura acima, observa-se a total abrangência do Planejamento Estratégico em relação aos demais planejamentos, tático e operacional. Compreende-se a existência integrada entre eles de forma a proporcionar à organização uma sinergia em todos os seus objetivos e propósitos,

resultando em um planejamento dinâmico. Como argumenta Oliveira (2003, p.47), o Planejamento Estratégico, percebido de forma separado ou individual, é "insuficiente, uma vez que escalões de uma empresa apresentam os planejamentos de forma integrada". Porém, analisando os impactos que cada um deles exerce nas empresas, são mais perceptíveis à medida que os limites são expandidos. Por exemplo, o planejamento operacional flui de uma forma quase natural na maioria da empresas, pois envolve ações normais de suas atividades fins, produção de produtos, prestação de serviços, vendas, por exemplo.

Partindo desta perspectiva, pode-se considerar que a visualização de um planejamento operacional é mais nítida nas empresas que se iniciam com uma estrutura organizacional ainda bem resumida. Por exemplo, uma empresa que presta serviço na área de implementação e configuração de redes de computadores, não necessariamente, inicia-se com um profissional responsável pela contabilidade ou departamento financeiro, ou ainda, um psicólogo para tratar das contratações de mais funcionários, um profissional de marketing, entre outros. Dependendo do investimento inicial, essa empresa é formada de um profissional que é o administrador de redes, como atividade fim, responsável pela efetuação do serviço prestado, divulgação, recebimento, compras etc. Porém, na medida em que o negócio se expande, outros profissionais são necessários para atender às demandas. Formam-se os departamentos financeiros, recursos humanos, vendas, compras, marketing, almoxarifado, entre outros. A partir desse momento, evidencia-se o planejamento tático que visa ou atende a níveis organizacionais superiores ao operacional. Sendo assim, percebe-se que, dentro da normalidade e progresso das estruturas organizacionais, a demanda por um tipo de planejamento flui automaticamente.

Outro aspecto que deve ser ressaltado, e está diretamente relacionado com o objetivo desse trabalho, é que, dentro dos três tipos de planejamento, percebe-se a existência de um fluxo de informações que, por meio de análise e classificação por relevância, tem-se insumo para iniciar uma proposta para elaborar um Plano de Segurança da Informação.

Conforme Oliveira (2003), as diferenças básicas entre os planejamentos estão no que diz respeito a prazo, amplitude, riscos, atividades e flexibilidade. Esta comparação é realizada, para melhor entendimento, considerando primeiramente as diferenças entre o Planejamento Estratégico e o Planejamento Tático e, por último, em relação ao Planejamento Operacional. Por isso, as informações que apresentam características ou ações a longo prazo e são classificadas no nível estratégico, têm sua amplitude envolvendo toda a organização; os riscos são maiores, suas atividades representam fins e meios e sua flexibilidade é limitada ou menor.

No entanto, como essas informações são gerenciáveis pela própria organização, elas são consideradas sensíveis quanto ao aspecto de segurança, porém, apresentam-se mutáveis nos níveis abordados. Por exemplo, uma informação mercadológica que se encontra no nível estratégico da empresa, implica alta restrição de acessibilidade e confidencialidade; seu estágio é crítico por envolver decisões que impactam toda empresa ou produto/serviço fim a longo prazo. Quando essa informação chega ao nível tático da organização, a restrição de acessibilidade e confidencialidade diminui e sua abrangência é direcionada em planejamento específico, ainda com certo grau de segurança, com prazo menor. No nível operacional, as restrições quanto à acessibilidade, praticamente, desaparecem; a confiabilidade torna-se flexível e valoriza-se a integridade dessa

informação como novo aspecto de segurança. Neste nível, um produto ou serviço que, a longo prazo, era totalmente restrito e confidencial, assume a necessidade de se tornar o mais publico possível para alcançar seu objetivo.

3.3.2 Produtos gerados no desenvolvimento do PE

O processo de elaboração do Planejamento Estratégico demanda e analisa diversos produtos que, interligados, representam o planejamento em sua essência. Segundo Migliato (2004), em resumo às diversas metodologias que, frequentemente, surgem todos os dias nas literaturas sobre Planejamento Estratégico, a sua concepção segue os seguintes passos, conforme representa a figura 5.

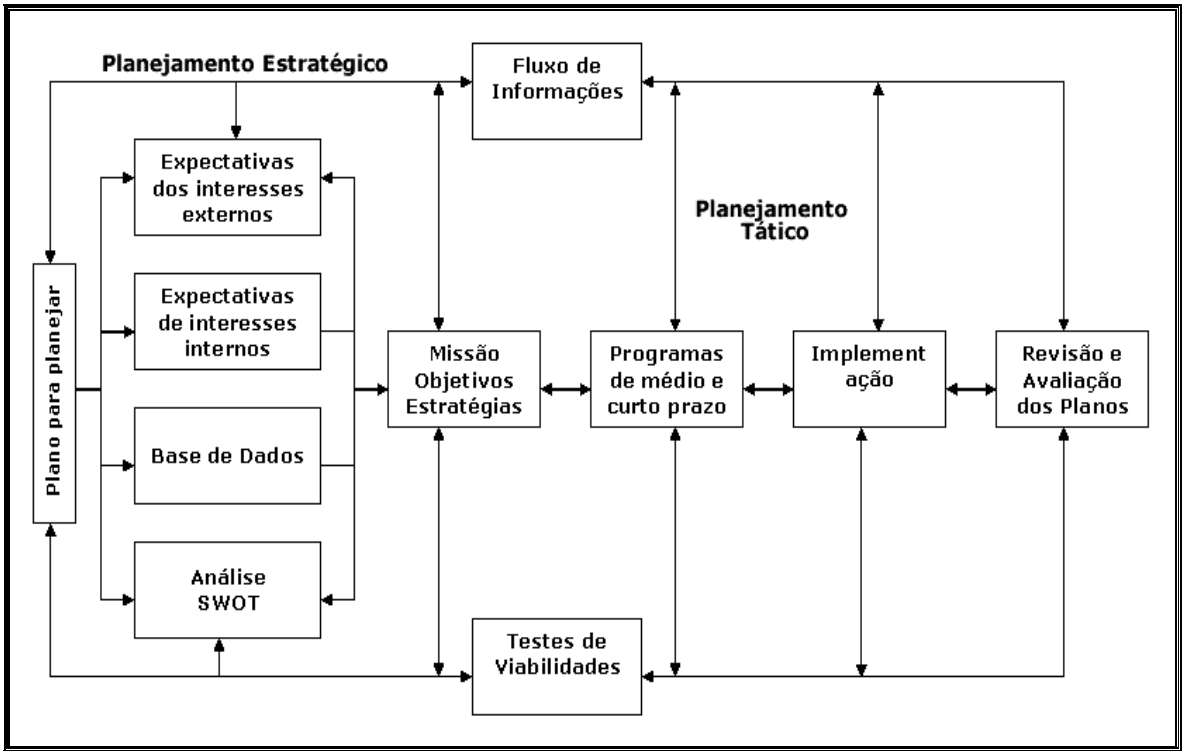

Figura 5: Estrutura e processo de planejamento estratégico.
Fonte: Steiner (1979) apud Migliato (2004).

A figura 5 apresenta uma proposta realizada por Steiner (1979), com o objetivo de ilustrar as etapas ou produtos gerados pelo Planejamento Estratégico.

Conforme Migliato (2004), o primeiro passo na elaboração do PE é constituir um plano daquilo que as pessoas envolvidas no processo esperam do planejamento. É exemplificado como manual ou guia do planejamento. Seria o primeiro rascunho do que se deseja.

O próximo passo é representado e alinha-se com o que Oliveira (2003) chama de diagnóstico estratégico, Maximiano (2004) descreve como análise do ambiente, Moresi (2001) como monitoramento ambiental e Megliato (2004) como o início do PE. No entanto, esta fase apresenta, através de busca de informações sobre o ambiente interno e externo da organização, uma fotografia da organização atual e, através da análise dos ambientes, surgem as possíveis situações desejadas para o futuro, subsidiadas pelos pontos fortes e fracos, como oportunidades e ameaças.

Em seguida, definem-se a missão, os objetivos e as estratégias. Para Maximiano 2004 (p.165), a missão significa “o propósito ou a razão de ser da organização”. Acrescenta que as perguntas que se fazem no momento de elaboração da missão são as seguintes: Quem são nossos clientes? Em que negócio estamos? Que necessidade estamos atendendo? E qual nossa utilidade para os clientes? Já para Oliveira 2003 (p.128), a missão está relacionada a fatos futuros que definem os tipos de atividades em que a empresa deverá concentrar-se futuramente. E suas perguntas são as seguintes: qual a razão de ser da empresa? Qual a natureza do negócio? Quais são os tipos de atividades em que a empresa deve concentrar seus esforços no futuro? (Oliveira, 2003). Acrescenta-se, ainda, a

visão da empresa que são aspectos ligados a valores, ética, desejos e filosofia da empresas, porém a visão serve de bússola na tomada de decisões e ações organizacionais (Migliato, 2004).

Já os objetivos representam o alvo ou ponto a que se pretende chegar ou atingir com prazo de realização estabelecido (Oliveira, 2003). Para Maximiano (2004, p.145), “são os fins, propósitos, intenções ou estados futuros” que se pretendem alcançar. Os objetivos, geralmente, são quantitativos. Conquistar 60% dos consumidores de um determinado produto pode ser o objetivo de uma empresa, por exemplo.

As estratégias significam estabelecer os caminhos, os programas de ação que devem ser seguidos para os objetivos ser alcançados. “A arte de utilizar, adequadamente, os recursos físicos, financeiros e humanos, tendo em vista a minimização dos problemas e maximização das oportunidades” (Oliveira, 2003, p.193).

No entanto, observa-se na figura 5 que, durante todo processo ou etapas do PE, há um fluxo de informação que se apresenta em forma de sinais ou mensagens. Segundo Moresi, dentro do contexto de gerenciamento da informação e monitoração, “qualquer mudança ou desenvolvimento no ambiente externo cria sinais e mensagens que uma organização deve estar atenta” (2001, p.41). O autor acrescenta que a percepção desses sinais ou mensagens exige esforço, pois, muitas vezes, apresentam-se de forma sutil, confusa e espúria.

Para Calazans (2006), o fluxo informacional é um fator que influencia de forma direta a informação organizacional. Na concepção da autora, o fluxo informacional é responsável “pela qualidade da informação, distribuição e adequação às necessidades do usuário” (p.68). Conforme Daveport (1998), em uma

organização, existem quatro níveis diferentes de fluxos: a informação não estruturada, informação estruturada em papel, informação estruturada em computadores e o capital intelectual ou conhecimento. Para o autor, informações disponibilizadas em fontes impressas, livros, jornais, revistas e relatórios são classificadas como não estruturadas. Registros, documentos manuscritos, são consideradas como informação estruturada em papel. Já as bases de dados, cadastros, bases de normas técnicas são apresentados como informação estruturada em computadores. De forma mais subjetiva, informações que estão implícitas nas pessoas, são atribuídas ao capital intelectual ou conhecimento. Calazans (2006, p.66) conclui que os fluxos de informação "precisam ser gerenciados e organizados de maneiras diferentes para atender às várias finalidades organizacionais, ter significado e gerar conhecimento".

Partindo dessa perspectiva, resta conhecer os tipos de informação que alimentam este fluxo e suas necessidades na perspectiva do PE. Compreende-se uma maneira de se aprofundar nas descobertas de quais informações circulam e são geradas no Planejamento Estratégico e conhecer algumas técnicas que são recomendadas para análise de ambientes e geração de informações.

3.3.3 Técnicas de buscas e diagnósticos de informações

A técnica SWOT (*Strengths, Weskness, Opportunities, threats),* também conhecida como o diagnóstico dos pontos fortes, pontos fracos, oportunidades e ameaças, é utilizada para avaliar a situação ou posicionamento da organização e seu potencial diante das outras organizações (Silveira, 2001). Esta técnica tem como objetivo analisar os pontos fortes e fracos, que são variáveis internas de uma organização e, por ser interna está sob controle da empresa, como também as variáveis oportunidades e ameaças que estão no ambiente externo à

organização e, consequentemente, estão fora do seu controle. Sendo assim, a organização deve conhecer essas variáveis e classificá-las em ordem de prioridades e relevâncias, conforme a tabela 2.

Tabela 2: Conceitos e exemplos dos fatores de uma análise SWOT.

Fatores	Conceito	Exemplos
Pontos fortes	Fatos, recursos, reputação	Pesquisa e desenvolvimento, tendências tecnológica, recursos financeiros, clima organizacional, liderança, base de clientes, itens de diferenciação de produtos, margem de retorno etc.
Pontos fracos	Deficiências ou limitações que podem restringir o desempenho da organização.	Inabilidades técnicas ou gerenciais, obsolescência de métodos ou equipamentos, endividamento incompatível com o fluxo de caixa, vulnerabilidade à competição.
Oportunidades	Fatos ou situações do ambiente externo que a organização pode vir a explorar com sucesso.	Novas tecnologias, tendências de mercado, novos mercados, novos produtos, alianças estratégicas, entre outras.
Ameaças	Situações do ambiente externo que podem impedir o sucesso da organização.	Legislação restrita, novos competidores, taxas de juros, abertura de mercado, etc.

Fonte: Silveira (2001, p. 214)

Na apresentação da tabela 2, percebe-se que os tipos de informações que exemplificam as variáveis em estudo, são importantes e estratégicas na tomada de decisão das organizações e exigem um cuidado especial quanto à sua integridade, confidencialidade e disponibilidade. Exemplificando, uma informação relacionada à pesquisa e desenvolvimento, pode ser classificada como ponto forte de uma empresa, ser estratégica e agregar valor aos serviços ou produtos. Sendo assim, ressalta-se a necessidade do devido cuidado para não haver acesso a essa informação por pessoas não autorizadas, como também a garantia de que a mesma não foi modificada em algum momento sem autorização ou sem registro. Nesse caso, o controle e proteção estão a cargo da própria organização por ser uma informação que é gerada e gerenciada no ambiente interno. Porém, mesmo no ambiente interno, há a necessidade de políticas de acesso às informações estratégicas, pois a sua divulgação ou acesso por pessoas não-autorizadas ou mal-intencionadas, pode acarretar grandes prejuízos à organização. Afinal, muitos concorrentes gostariam de ter acesso a arquivos de um projeto e especificações de um novo produto.

Por outro lado, as informações tidas e geradas no ambiente externo, como apresentadas na técnica SWOT, geralmente, são informações públicas. Suas formas de disponibilidade variam dependendo das instituições que provêem. Por exemplo, informações sobre tendências de mercado estão disponíveis em sites de informação estatística e indicadores como IBGE, CNI, Ipea, entre outros. No entanto, são informações incontroláveis às organizações por estarem inseridas no ambiente externo e exigem a devida percepção, pois as mesmas podem significar oportunidade de negócio e, conseqüentemente, ganho para empresa ou mesmo ameaça a ser evitada ou minimizada. Entende-se que o

cuidado que se deve a esse tipo de informação quanto ao aspecto de proteção está relacionado à sua integridade e confidencialidade, ou seja, à garantia de que as fontes e as próprias informações são fidedignas.

Sendo assim, a técnica SWOT fornece informações essenciais na elaboração do Planejamento Estratégico, como também as classificam quanto ao grau de relevância e no que diz respeito a políticas de segurança.

Uma outra técnica utilizada no processo de elaboração do PE e, portanto, pode ajudar a verificar as necessidade de informação ou pelo menos demonstrar o modo de buscá-la, é a chamada *benchmarking.* Essa técnica tem como objetivo geral "auxiliar as organizações a identificar, comparar, selecionar e, se for o caso, incorporar o que os concorrentes praticam de melhor no mercado" (Júnior,2001,p.246). Segundo o autor, existem três tipos do *benchmarking*: interno; competitivo; e funcional ou genérico.

O *benchmarking* interno é aquele que é aplicado na própria estrutura organizacional com o objetivo de verificar o compartilhamento de experiências e conhecimentos entre os departamentos. Já o *benchmarking* competitivo é definido como avaliação e comparação dos processos, produtos e serviços internos em relação aos processos, produtos e serviços de empresas concorrentes. Significa aprender com competidores do mesmo mercado ou outros que utilizam estratégicas diferenciadas. E o *benchmarking* funcional ou genérico é um tipo que pode ser aplicado em qualquer empresa.

O *benchmarking* é utilizado como técnica de apoio ao planejamento estratégico organizacional, sendo assim, corresponde a um processo dinâmico e contínuo por lidar com informações que mudam freqüentemente. O autor ainda apresenta seis características básicas do benchmarking:

- Envolve um processo “contínuo e sistemático” que avalia as empresas líderes de mercado;
- Tem em si uma “interatividade”, que envolve os sistemas de comunicação das organizações para divulgar os objetivos;
- É um processo “investigativo”, pois seu objetivo é diagnosticar a concorrência, dando uma visão geral sobre o mercado;
- Processo “voltado para a aprendizagem”, pois gera conhecimento através da monitoração do melhores concorrentes líderes;
- Representa um processo “pró-ativo”, assim que o conhecimento adquirido fornece subsídios básicos para decisões futuras (Júnior,2001);

Apresenta ainda, os princípios do código de conduta para a técnica *benchmarking*: “principio da troca, da confidencialidade, do uso, do contato, da preparação, da conclusão e da compreensão e ação” (Júnior,2001,p.260).

Tendo em vista o contexto deste trabalho, observa-se que as formas como as informações são capturadas, analisadas e utilizadas, via essas técnicas, conseguem detectar a necessidade de informações adequadas, que subsidiam o processo decisório de qualquer organização, e as priorizam dentro do contexto da segurança de informação. A técnica de benchmarking trata de informações que geram aos parceiros[2] reciprocidade, aproximação e contato.

---

[2] Parceiros de *benchmarking* significam uma determinada empresa, operação ou função, que exerce no mercado desempenhos relevantes, e são referenciais para comparação (Júnior, 2001).

Considerando as diferenças entre as duas técnicas, a SWOT preocupa-se em conhecer, através de processos de buscas, as informações dos ambientes interno e externo, para assim ter-se conhecimento não só dos pontos fortes e fracos, mas também das oportunidades e ameaças. Por sua vez, a técnica benchmarking tem, como seu principal objetivo, conhecer as informações, em primeiro lugar, que estão no ambiente externo ou de empresas em destaque, para então compará-las e, se possível, executá-las em seu próprio ambiente.

As duas técnicas analisam os dois ambientes de uma organização, interno e externo. Elas trabalham com informações essenciais para elaboração do planejamento estratégico.

Fatores do ambiente externo organizacional como clientes, fornecedores, concorrentes, econômico, político e tecnológico, entre outros, representam para as organizações oportunidades ou ameaças. As facilidades de financiamento de fundos estatais ou privados podem custear projetos que atendem a área de atuação da organização, ou mesmo programas governamentais destinados à maximização do setor participante, são exemplos de **oportunidades** a que as organizações devem estar atentas.

Já as **ameaças** são forças que podem afetar a empresa de forma negativa, como a extinção ou o não investimento (em um determinado setor que a organização atua como prestadora de serviços ou geração de novos serviços), privatizações, fusão, demissões, entre outros. Estes são exemplos de ameaças que surgem freqüentemente e representam fatores do ambiente externo (Almeida, et al 1999).

A análise do ambiente interno resulta em conhecer e estabelecer diretrizes para implementação de novos objetivos e quais estratégias seguirem. É o

conhecimento das qualidades e das deficiências da organização. Consiste em diagnosticar os pontos fortes e fracos. Alta qualificação do pessoal técnico e administrativo, elevada credibilidade junto à sociedade, situação financeira sólida são exemplos de pontos fortes. Porém, sistema de planejamento ultrapassado, elevado grau de centralização nas decisões e desatualização do pessoal são pontos fracos de uma organização (Almeida, et al 1999).

Nesse sentido, como pode ser percebido nas descrições anteriores é necessário em qualquer uma das técnicas conhecer as informações do ambiente interno e externo, permitindo, desse modo, refletir que um Planejamento Estratégico gera informações durante o seu desenvolvimento e execução.

Os instrumentos utilizados para tratar e organizar as informações oriundas do PE são os sistemas de informação, que facilitam as instituições na gestão das informações nos seus vários níveis (operacional, tácito e estratégico).

Assim, com as informações provenientes do PE tratadas e organizadas é possível caracteriza-las, verificando o nível de relevância e definindo os níveis de proteção, conforme proposta apresentada no Quadro 2.

4. PROPOSTA DE CONTRIBUIÇÃO DA CIÊNCIA DA INFORMAÇÃO PARA CRIAÇÃO DO PSI

O objetivo deste trabalho é apresentar uma proposta como a Ciência da Informação pode contribuir para a criação de um Plano de Segurança da Informação (PSI). Para tanto, analisou-se a dinâmica da informação no ambiente organizacional, o fluxo de informações que o Planejamento Estratégico proporciona ou gera, como também os tipos, características e relevância, entre outros, que subsidiam a tomada de decisão nas organizações.

Os conceitos abordados no capítulo 3 (definição do PE, tipos de PE, produtos gerados pelo PE e técnicas de monitoração dos ambientes), permitiram compor um referencial que discute a contribuição da Ciência da Informação, mediante a necessidade de informação que esses processos evidenciam, e paralelamente, demonstraram a importância do alinhamento com os planos de segurança da informação.

Diante disso, partindo da premissa de que existe um fluxo de informações no PE e que dele podem-se extrair as necessidades de informação organizacional, é possível representar na figura 6 este processo e sua contribuição para desenvolvimento do PSI.

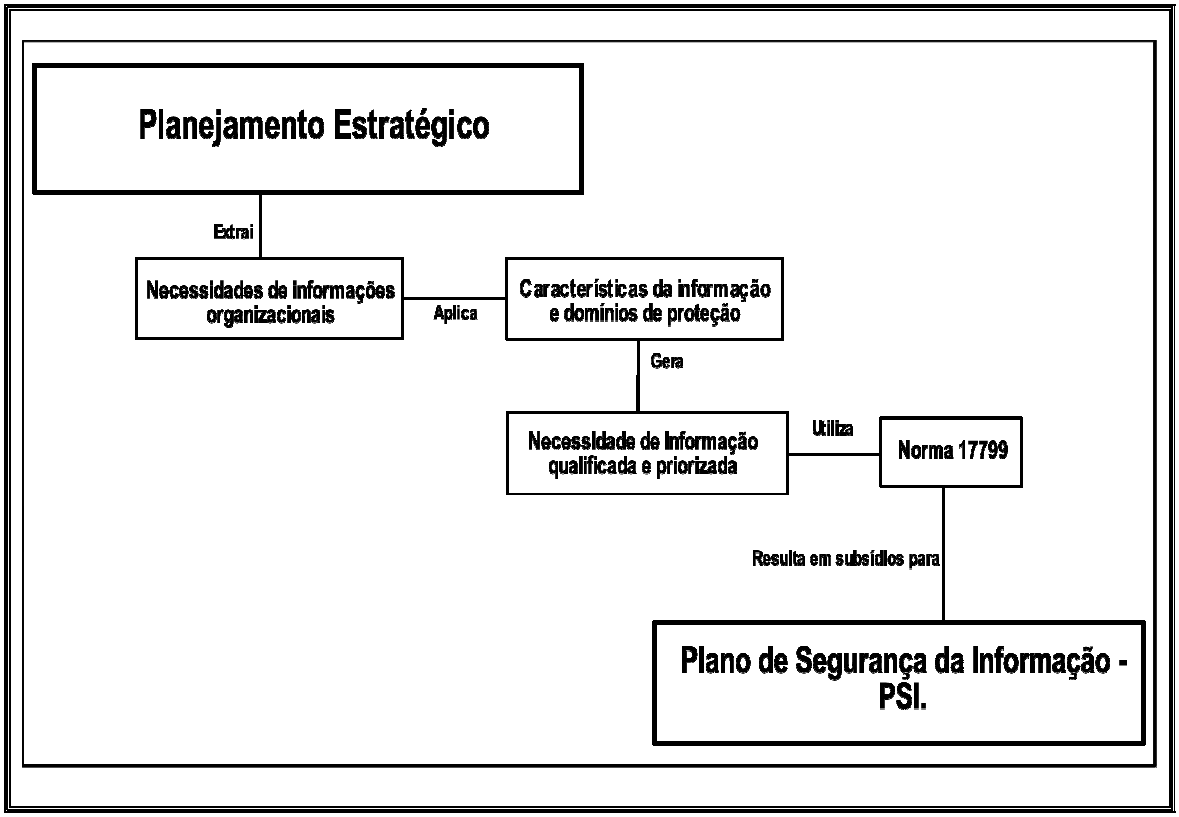

Figura 6: Contribuição para criação do PSI

Analisando e descrevendo a figura 6 percebe-se que ela é estruturada em quatro etapas. São elas:

- Extração das necessidades de informações organizacionais;
- Aplicação das características da informação e domínios de proteção;
- Geração das necessidades de informação qualificada e priorizada em termos de necessidades de proteção;
- Utilização da norma ISO NBR 17799:1.

A seguir, serão descritas, em detalhes, essas etapas.

4.1 Extração das necessidades de informações organizacionais

O Planejamento Estratégico como um instrumento de gestão para as organizações e tendo como objetivo o fornecimento de diretrizes que proporcionam uma visão do ambiente presente como também dos possíveis ambientes futuros e suas implicações na tomada de decisão, gera e organiza diversos tipos de informações. Dentro desse processo dinâmico, sistêmico e formal, é possível extrair as necessidades de informação que estão presentes em suas etapas de desenvolvimento, execução e controle.

Extrair significa, especificamente neste contexto, observar os aspectos de geração e organização das informações no processo de Planejamento Estratégico. A geração, partindo desta premissa, relaciona-se com o próprio processo de busca que o PE empreende. Uma quantidade enorme de informações são analisadas quando se procura conhecer os ambientes em que a organização está inserida, o estabelecimento da sua visão, da missão, dos objetivos e de suas estratégias. A geração se dá, também, pelo fato de muitas informações estarem em um determinado momento em sua forma bruta, ou seja, sem um significado evidente, porém com a extração, utilizando-se técnicas de diagnósticos (análise ambiental, SWOT, Benchmarking, entre outras), esses dados são organizados e estruturados no contexto geral da empresa, podendo, assim, transformar-se em uma informação importante.

Com relação à organização das informações, ela ocorre por meio da classificação e priorização conforme sua relevância. A partir do momento em que as informações são conhecidas nas várias etapas do PE, é necessário classificá-las de forma que seu acesso ou mesmo sua recuperação ocorra de maneira rápida e eficiente. Já a priorização se enquadra no devido cuidado de não se consumir

recursos em informações sem utilidade, ou seja, deve ser estabelecido o nível de relevância para assim organizá-las adequadamente.

Sendo assim, a extração das necessidades de informação organizacional é um processo de analise e acompanhamento do fluxo de informações no Planejamento Estratégico, por meio de técnicas de monitoramento, que fornecem as diretrizes de geração e organização das informações classificadas e priorizadas conforme sua utilidade ou relevância (vide a figura 7).

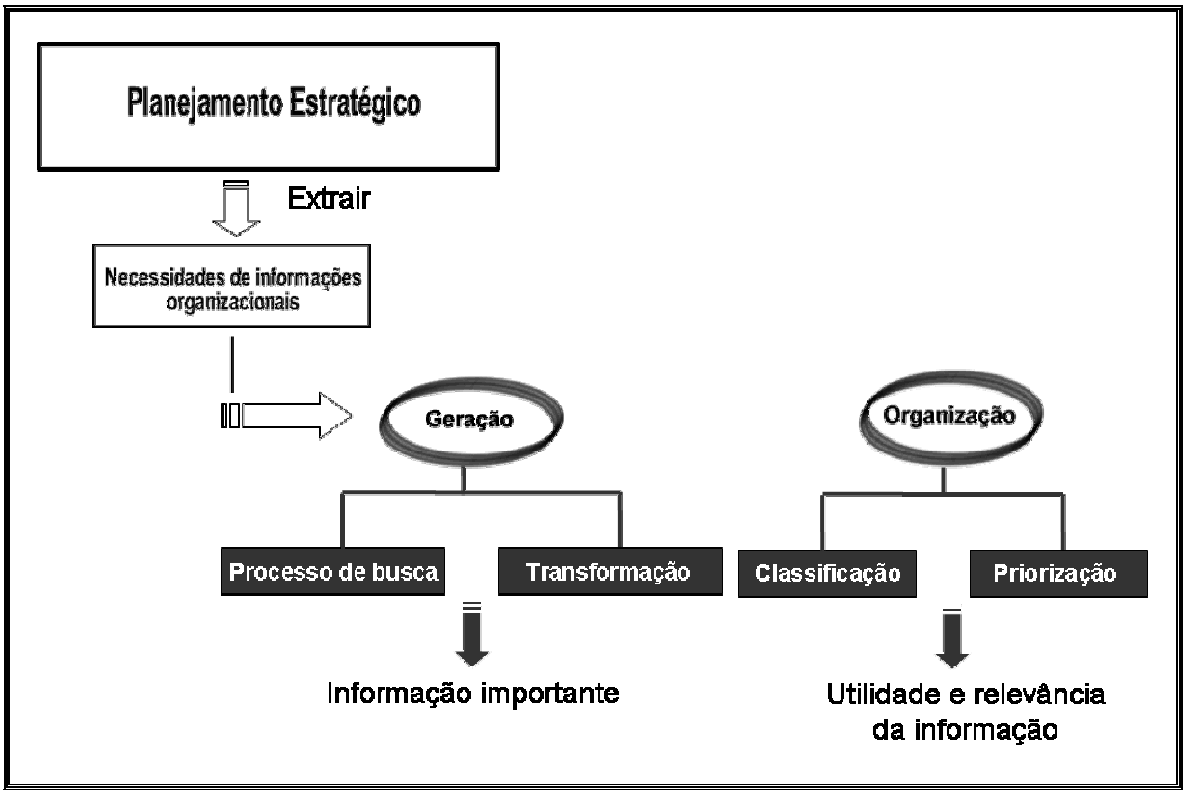

Figura 7: Extração das necessidades de informações organizacionais

Por conseguinte, as informações que se apresentam como relevantes, devem conter cuidados que garantam sua integridade, confidencialidade e disponibilidade.

4.2 Aplicação das características da informação e domínios de proteção

A aplicação das características da informação e domínios de proteção pode ser melhor compreendida analisando o quadro 2, apresentado no final do capítulo 2.

Observando as informações contidas no referido quadro, pode-se caracterizar a informação e refinar sua prioridade conforme o nível de proteção que ela necessita, conforme sua importância no contexto organizacional. Nesse sentido deve ser vista a informação quanto a:

- Seus diversos tipos (informações de clientes, econômicas, invenções e inovações, entre outras);
- Sua classificação (informação estratégica, cientifica, tecnológica e informação para negócio);
- Sua forma de armazenamento (bases de dados, relatórios impressos, teses e pesquisas, entre outros);
- Sua relevância (informação crítica, potencial, mínima) e;
- Seus domínios de proteção (política de segurança, segurança organizacional, classificação e controle, segurança em pessoas, entre outros).

Caracterizar as informações significa, basicamente, conhecê-las em seus diversos atributos e perceber seus impactos na tomada de decisão, ou seja, ter conhecimento minucioso das diversas formas que estas informações assumem em determinado momento organizacional e, conseqüentemente, estabelecer critérios para que essas informações estejam disponíveis, acessíveis e confiáveis.

Esses critérios se referem ao agrupamento ou conjunto de informações importantes e estratégicas que servirão de apoio a um dado momento decisório.

O atributo **tipos de informação** é caracterizado por informações que estão disponíveis tanto no ambiente interno como no externo da organização. Sendo assim, tipificar as informações, segundo sua qualidade ou representação, significa conhecer a informação quanto à sua forma de explicitação, tanto dentro da organização como fora dela. É visualizar a informação na sua real representação. Uma instituição de ensino, por exemplo, trabalha com informações internas referentes a ensino e pesquisa como: invenção, inovação, conhecimento, entre outras. A instituição também se relaciona com informações externas como, alunos, fornecedores, governo, concorrentes. Elas representam os tipos de informações com que cada organização lida no seu dia-a-dia.

Portanto, a caracterização se dá, neste caso, em conhecer a informação e sua importância para o negócio. Sendo assim, uma Instituição de ensino pode trabalhar com informações referentes à pesquisa, objetivando, por exemplo, ser reconhecida como uma organização que fomenta conhecimento para a sociedade e forma profissionais adequados às necessidades do mercado.

O atributo **classificação** é determinado pelo impacto que a informação possui para a organização em termos de valor. Este atributo é testado e analisado inicialmente em seu contexto interno e posteriormente pode se tornar uma informação com influências no ambiente externo ou público. Complementando o exemplo anterior da instituição de ensino, a classificação de uma informação como invenção, está totalmente restrita, pelo menos na fase inicial, ao ambiente interno da instituição, mais ainda, mesmo no ambiente interno pode ainda se limitar a um determinado departamento ou grupo de pessoas. Todavia, a partir do

momento em que essa informação se transforma em um produto, serviço ou conhecimento, sua classificação pode persistir e a sua restrição se expande para o público interno e externo, deixando assim de ser uma informação crítica quanto à sua acessibilidade.

Exemplificando este conceito, um artigo cientifico empreendido por um determinado pesquisador ou grupo de pesquisadores, inicialmente e durante seu desenvolvimento, se torna restrito a esse pesquisador ou grupo. Porém, com sua conclusão e aceitação em um periódico ou evento científico o mesmo se torna público. E diga-se mais, o que torna um pesquisador contente é saber que seu artigo está sendo referenciado e acessado por todos sem qualquer restrição. Na verdade, a restrição se dá no cuidado de manter a confidencialidade do documento, sendo a preocupação quanto à veracidade e integridade da informação, que é a garantia de que não houve nenhuma alteração durante sua reprodução ou divulgação.

Contundo, podem ser aplicados os conceitos acima não apenas para documentos científicos, mas também para produtos e serviços gerados por empresas que não estão, necessariamente, incluídas em ambientes acadêmicos, mas que investem grande quantidade de seu capital em inovações e descobertas, e possuem um controle rigoroso quanto à proteção destes produtos ou serviços, como novos modelos de carros, novos serviços de telecomunicação ou novos produtos eletrônicos.

Portanto, classificar as informações se resume em analisar não só sua significância como também sua influência tanto no ambiente interno como no externo da organização. Quanto mais estratégica for para a organização a informação, maior nível de proteção requererá.

Já o atributo **fonte** significa a estrutura física e/ou lógica, em que as informações são armazenadas. São os suportes que auxiliam a organização, classificação, recuperação e distribuição das informações de forma eficaz, seja elas em meios tradicionais ou digitais. Uma informação bem representada pode ser recuperada de um banco de dados, instalado, por exemplo, em um *HD* (*hard disk)* de um computador. Porém, devido às inúmeras fontes de armazenamento existentes, a caracterização e domínio de proteção desse atributo devem ser complementados ainda pelo reconhecimento da sua relevância e utilidade.

O atributo **relevância** diz respeito ao interesse que ele desperta em seus proprietários ou mesmo nos concorrentes. A relevância da informação se dá também pela importância que tem para a organização, de maneira que pode ser vista como informação crítica, ou como informação sem interesse.

Entende-se também por relevância quando uma informação passa pelas etapas de caracterização quanto ao tipo, classificação, fonte e se torna importante na tomada de decisão. Nesse caso, pode-se dizer que a informação é relevante. Por exemplo, se uma empresa precisa decidir qual investimento realizar (bolsa de valores, fundo de capitalização, compra de um novo produto, serviço ou empresa) e as informações adquiridas fornecerem indicadores que a ajudam a decidir, com segurança, o retorno desse investimento, considera-se essa informação como relevante, pois proporciona uma decisão correta.

Por outro lado, existem informações que não foram devidamente classificadas, valorizadas e sua forma de representação atendida. Nesse caso, tal informação não forneceu subsídios para uma tomada de decisão correta, portanto a informação não é relevante.

O atributo **domínios de proteção** diferencia-se dos demais atributos por estar mais diretamente relacionado ao aspecto de zelar as informações de utilizações inadequadas. É um atributo que inspeciona todos os demais atributos no que se refere ao privilégio de acessibilidade, confidencialidade e integridade das informações.

Estabelecer proteção sobre os tipos de informações que circulam nas organizações, sobre os devidos valores que cada informação expressa, a maneira como elas estão armazenadas e em seu uso efetivo, resulta em um gerenciamento do fluxo de informações que pode ter acesso mediante o desenvolvimento de um Planejamento Estratégico eficiente.

A figura 8 representa como pode ser feita a aplicação das características da informação e os domínios de proteção.

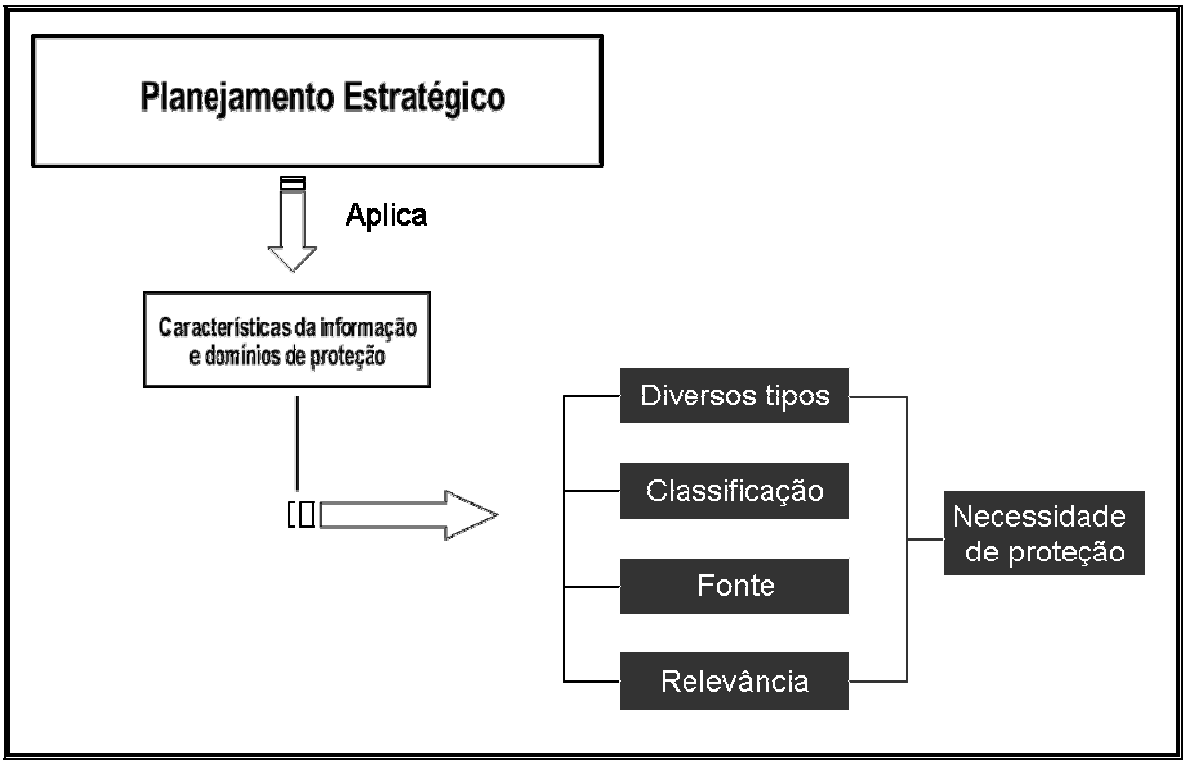

Figura 8: Aplicação das características da informação e domínios de proteção

Sendo assim, conclui-se que a aplicação das características de informação e domínio de proteção sintetiza-se em conhecer, de forma criteriosa, as informações disponíveis para então poder gerar uma necessidade de informação qualificada e priorizada em termos de necessidade de proteção.

4.3 Geração de necessidade de informação qualificada e priorizada

Com a aplicação das características da informação foi possível visualizar as informações quanto à sua peculiaridade no ambiente organizacional, ou seja, analisou fatores que estão implícitos na informação e que demonstram seu significado de maneira bem específica. Agora nessa etapa, tem-se como objetivo visualizar as informações no contexto geral da organização, qualificando-as quanto ao seu valor estratégico e priorizá-las, fundamentalmente, sobre uma base de necessidade de proteção.

A geração de necessidade de informação qualificada, no contexto deste trabalho, denota as ações de selecionar, formalizar e estabelecer regras e práticas de segurança como premissas fundamentais para manter as informações estratégicas protegidas contra acessos indevidos, modificações e perda de credibilidade.

A premissa **selecionar** envolve uma ação do gestor ou pessoa responsável por tratar as informações, em observar e determinar os critérios que as organizações utilizam quanto às suas necessidades de informação. Devido às diversas fontes, meios e forma como as informações são apresentadas, percebe-se uma enorme quantidade de informações disponíveis aos tomadores de decisão, porém, necessitam ser selecionadas.

A observação envolve, desta forma, ter conhecimento em uma dimensão ampla que seja possível identificar em qual momento a informação se torna relevante ou sem interesse do ponto de vista estratégico. As informações são passadas por um crivo que observa o seu impacto no negócio da organização. Com essa observação, é possível qualificar a informação e estabelecer sua necessidade de proteção. Já a determinação dos critérios diz respeito aos meios que são utilizados para observar ou selecionar as informações.

Um dos critérios pode ser o de classificar as informações segundo sua prioridade considerando que as mesmas já foram selecionadas como importantes. Uma outra forma, em meio a tantas informações, é utilizar-se de técnicas de diagnóstico ou de sistemas de informação na busca de informações que, comumente, são utilizadas, acessadas e classificadas como importantes para tomada de decisão.

Sendo assim, selecionar enquadra-se em ter uma visão sistêmica do ambiente organizacional como também apurar e refinar, por meio de técnicas de observação, os critérios que são utilizados para qualificar as informações, tendo ciência de que a informação considerada de qualidade é aquela que, diante de um montante de informações, é selecionada e formalizada para atender a tomada de decisão.

Já a premissa **formalizar**, significa estabelecer alguns parâmetros recomendados pela gestão de informação que envolve os processos de planejar e direcionar as informações de maneira a atender os requisitos de qualidade.

Planejar, partindo desta perspectiva, aparece no sentido de identificar as necessidades de informação como também sua real valorização

considerando o todo da organização. Caracteriza-se em não simplesmente atender as necessidades imediatas, mas ter informações para as possíveis ações futuras.

Direcionar, dentro do aspecto de formalizar as informações, abrange encaminhar as informações qualificadas aos seus devidos lugares e pontos estratégicos da organização, de forma que sejam estabelecidos os tipos de controles e regras de segurança da informação. Nesse aspecto, os meios que envolvem os fluxos de informação, sistemas de informação, comunicação de dados e inter-pessoais devem ser conduzidos por um órgão de controle ou por pessoas responsáveis pelos planos de segurança.

Portanto, formalizar as informações é enquadrá-las em um processo de gestão que envolve o ato de planejar as informações e direcioná-las considerando seu verdadeiro objetivo.

Apresenta-se a última premissa desta etapa, que **estabelece regras e práticas de segurança.** Esta análise prioriza as informações quanto à necessidade de proteção, pois como as informações já foram qualificadas nas premissas de seleção e formalização, resta estabelecer alguns princípios que garantam a sua integridade, confidencialidade e disponibilidade. Essa premissa tem como objetivo evidenciar a necessidade de se aplicar a norma NBR/ISO 17799:1, descrita na etapa seguinte.

A figura 9, resume os conceitos da geração da necessidade de informação qualificada e priorizada.

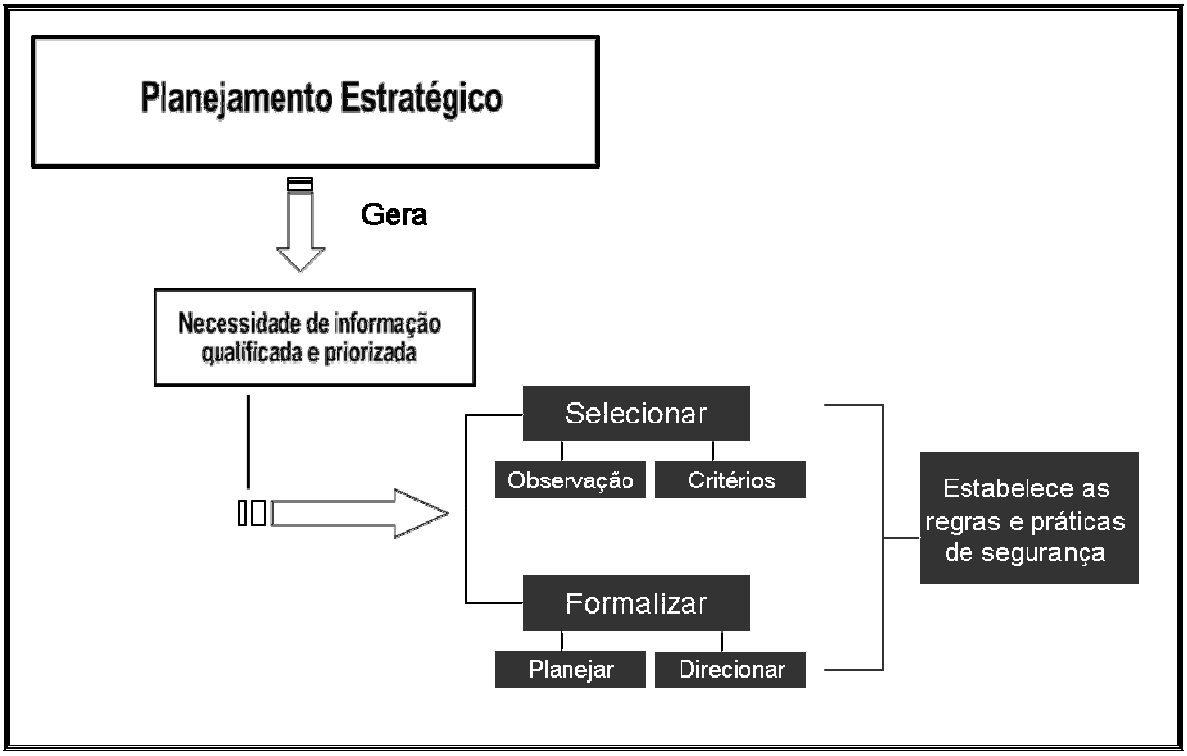

Figura 9: Geração da necessidade de informação qualificada e priorizada

Finalizando esta etapa, uma informação explicita valor para organização proprietária, como também para a concorrência e mercado de atuação. Sendo assim, conforme seu valor se estabelece a priorização. Por exemplo, as informações dos clientes de uma empresa são, geralmente, tratadas como uma informação crítica por se tratar dos dados pessoais, contatos, preferências ou seus perfis, números de cartões de créditos, entre outras. Trata-se, neste caso, de uma informação importante para a empresa porque, através delas, podem-se montar estratégias de marketing e de vendas. Essas informações devem ser priorizadas no que diz respeito à segurança para não ocorrer o risco de supostos incidentes como o noticiado pelo o jornal O Estado de S. Paulo no dia 03/02/2004 sobre a disputa entre duas academias na cidade de S. Paulo:

> "A concorrência acirrada entre as academias de ginástica de São Paulo chegou à justiça. A companhia *Athletica* está

> processando a academia *Reebok* por suposto roubo de mala direta, o que caracteriza crime de concorrência desleal. Como parte do inquérito policial aberto pela Polícia Civil de São Paulo, o Instituto de Criminalística da Secretaria de Segurança Pública do Estado elaborou um laudo comprovando que a maioria dos nomes de clientes da Cia. *Athletica* consta de forma idêntica no arquivo da *Reebok* apreendido pela polícia. A briga começou quando a *Rebook* inaugurou uma unidade a cerca de 500 metros da Cia. *Athletica*. Vários clientes da Cia *Athletica* reclamaram de terem recebido correspondência da concorrente" (apud Fontes, 2004, p.16)

Os métodos para adquirir informações estratégicas variam desde os eticamente aceitáveis, SWOT e Benchmarking, até a técnica ilegal de espionagem empresarial. Dentro dessa perspectiva, adotar políticas de priorização da informação é ter o cuidado de conscientizar todos os envolvidos deixando claro sua responsabilidade quanto à preservação ou proteção da informação.

4.4 Aplicação da Norma NBR/ISO 17799

Diante da necessidade de proteger as informações estratégicas nas organizações, torna-se fundamental aplicar o código de práticas para gestão da segurança da informação estabelecido pela norma NBR/ISO 17799:1 que possui uma série de recomendações básicas, que atendem as necessidades de proteção de qualquer organização que lida com informação no seu dia-a-dia.

Ela se divide em dez domínios. São eles:

- Política de segurança;

- Segurança organizacional;
- Classificação e controle dos ativos de informação;
- Segurança em pessoas;
- Segurança física e do ambiente;
- Gestão das operações e comunicações;
- Controle de acesso;
- Manutenção e desenvolvimento de sistemas;
- Gestão da continuidade do negócio;
- Conformidade.

Analisando as características da informação estudadas nas etapas anteriores com a aplicação nesta etapa dos domínios de proteção, percebe-se que, quanto maior for o valor agregado das informações, maior será o número de domínios de proteção necessários. Sendo assim, entende-se que estes domínios atendem os tipos, a classificação, a fonte e relevância das informações abordadas neste trabalho.

Os **tipos de informação,** (clientes, concorrentes, econômicas, tecnológicas, entre outras) presentes no dia-a-dia das organizações, devem ser assistidos por uma **política de segurança** que determina as regras e diretrizes de proteção. Essa política representa um documento formal esclarecendo todos os passos do que proteger, como proteger, quando e onde proteger. Em seguida, assinala-se o necessário trabalho de conscientização e estabelecimento da norma para todos os níveis hierárquicos organizacionais, através do estabelecimento da **segurança organizacional**. É estratégico que a aprovação e apoio à adoção da

segurança organizacional iniciem-se do topo da pirâmide (dos principais executivos da empresa) até a parte operacional envolvendo assim todos os funcionários, parceiros, fornecedores e prestadores de serviço. Um outro fator diz respeito às informações que devem também ser classificadas e controladas, conforme sua valorização e prioridades.

Registra-se também a necessidade de informar às pessoas que trabalham diretamente ou aos prestadores de serviços, os seus devidos papéis de proteger as informações disponíveis, de forma que se sintam responsáveis por elas. Normalmente, funcionários de um departamento estratégico de uma empresa têm acesso a informações que são confidenciais e restritas ao próprio departamento. Para tanto, a **segurança em pessoas** preocupa-se com a segurança tanto das informações do próprio funcionário, dando as devidas recomendações e procedimentos, como do sigilo dos dados estabelecidos pela empresa.

Dentro dos tipos de informação, pode ser citada também a necessidade de gerenciar as **operações e comunicações e o domínio de controle de acesso**. As operações e comunicações envolvem a atualização de softwares e os sistemas de monitoramento dos meios de propagação que estas informações utilizam como as redes de computadores. Já o controle de acesso estabelece os tipos de privilégios e as políticas que controlam o acesso a cada informação.

A norma enfatiza, nesses pontos, os riscos que as organizações sofrem por haverem diversas vulnerabilidades nos ambientes de sistemas e nos de redes de computadores. Uma empresa pode, por exemplo, investir em softwares como *firewall*, antivírus, entre outros métodos de proteção. No caso do *firewall, este* serve para controlar (como uma barreira) os acessos do ambiente interno e

ambiente externo estabelecendo bloqueios quando as informações não atendem a critérios predefinidos de segurança e liberando quando está em conformidade com as regras estabelecidas ou configuradas. Já o antivírus ajuda a impedir ataques de códigos maliciosos que chegam aos computadores via arquivos anexos em e-mail, *downloads* ou dispositivos remotos.

Sendo assim, aplicar os domínios de proteção a alguns tipos de informações em específico, é preocupar-se com as necessidades de segurança que cada informação requer.

Já na **classificação**, envolve uma cobertura dos domínios de **política de segurança**, **segurança organizacional**, **classificação e controle das informações e de acesso**. No entanto, apresenta um diferencial, pois requer também uma **gestão da continuidade do negócio e um grau de conformidade** com os interesses da organização. Estes dois domínios se completam por estarem relacionados com a garantia de que não haverá interrupções ou barreiras que dificultam o fluir dos processos na organização, por meio da gestão da continuidade. Já a conformidade relaciona-se com a concordância entre a missão da organização com as leis vigentes do país, estado ou cidade.

As informações classificadas como informação para negócio (as que geralmente subsidiam a decisão), por exemplo, fornecem conhecimento do ambiente onde as empresas atuam ou gostariam de atuar. Para tanto, para uma tomada de decisão que resulte benefícios, é importante que se conheça bem esse ambiente para não causar conflitos com os processos já estabelecidos na organização. E ainda, garantir a conformidade com seu planejamento constituído atendendo os parâmetros da visão de futuro, missão e objetivos. Geralmente a empresa que reconhece o dinamismo do mercado atual, utiliza-se de informações

para negócio (estatísticas de mercado, mercadológicas, financeiras, econômicas), para se preparar e planejar suas ações futuras. Proteger essas informações quanto ao impacto na continuidade e conformidade do negócio da organização, são orientações presentes na norma.

Com relação à **fonte**, que é o local físico ou lógico onde as informações são armazenadas, os domínios de **política de segurança**, **segurança organizacional**, **de pessoas e o de manutenção e desenvolvimento de sistemas** são necessários, porém, priorizam-se também os domínios da segurança física e do ambiente.

A segurança física e do ambiente, na forma de armazenamento, relaciona-se com a análise e conhecimento do perímetro de proteção, ou seja, as atenções necessárias quanto às barreiras impostas que dificultem ou registrem o acesso a estas informações. O ambiente onde esteja localizado um computador com banco de dados, por exemplo, requer a segurança física para evitar que pessoas não autorizadas tenham acesso, roubem ou causem algum tipo de desastre proposital. Exemplos dessas barreiras são a utilização de guardas nas portarias, câmeras, catracas eletrônicas ou outros tipos de identificações, como também o planejamento do local físico evitando danificações naturais como falta de refrigeração requerida, ambientes impróprios, entre outras.

Um domínio também importante, no contexto das fontes, é o da **manutenção e desenvolvimento de sistemas**, pois se entende que os sistemas responsáveis por proverem autenticação, validação de usuários, criptografia dos dados e outras funções de verificação, passam sempre por uma atualização, visto que as técnicas de ataques são renovadas freqüentemente ou diariamente.

Por fim, a **relevância** das informações é um fator que justifica a adoção dos domínios de proteção, pois considera, primordialmente, o valor e a utilidade que essas representam para a organização. Inicialmente é necessário considerar as duas dimensões de relevância da informação: a informação crítica de um lado e a informação sem interesse do outro, conforme colocação de Moresi (2000).

Informações críticas são aquelas que significam para a organização a sua própria sobrevivência, ou seja, informações que se não forem gerenciadas ou tratadas adequadamente, podem resultar em até dissolução da organização. Dentro da extração da necessidade de informações empreendida no PE, da aplicação das características da informação, da geração de necessidade de informação qualificada, percebe-se a possibilidade de reconhecimento desse tipo de informação.

Portanto, essas informações críticas se tornam alvos de interesses tanto dentro das organizações, como fora delas (concorrentes, hackers, etc.). No ambiente interno, diante de muitas informações relevantes, procura-se, mediante uma priorização, focalizar recursos de proteção nas informações críticas. Estes recursos significam a explicitação de diretrizes e normas de segurança, técnicas de controle, trabalhos de conscientização das pessoas envolvidas, segurança física e lógica e desenvolvimento de sistemas de validação.

Exemplo de informações críticas são as informações dos correntistas de um banco, em que constam dados pessoais do cliente, senhas do seu cartão eletrônico, cartão de crédito, investimentos realizados e todos os tipos de transações financeiras realizadas. O acesso ou tornar essas informações públicas, praticamente resulta em grande prejuízo para o banco. Prejuízos financeiros e de

confiança, podendo levá-lo a falência. Percebe-se neste exemplo que o nível de proteção desse tipo de informação é alto e geralmente, necessita da cobertura de todos os domínios de proteção.

Por outro lado, as informações sem interesse são aquelas que não possuem de imediato nenhum valor para a organização no que tange a preocupação com proteção e tomada de decisão. No entanto, por acreditar que as informações mudam com o passar do tempo, hoje ela pode não ter valor, porém, na sua geração ou organização, pode ter sido representada como uma informação estratégica. Sendo assim, as informações sem interesse devem ser reconhecidas para evitar a locação de recursos (principalmente financeiro e tecnológico) a essas informações. Ressalte-se que essa avaliação de informações sem interesse considera o contexto e a área de atuação da organização, pois uma informação pode ser sem interesse para uma determinada organização e estratégica para outra, dependendo de sua área de atuação.

Informações como leis, por exemplo, por serem externas e estar disponibilizadas publicamente, representam para uma instituição de ensino, no aspecto de locação de recursos de segurança e proteção, uma informação sem interesse. Não se questiona o valor dessa informação, mas a necessidade de proteção por parte da instituição. Para a instituição, sua preocupação está voltada para informações que lhe apresentam um diferencial competitivo em sua área de atuação. Agora, se colocando no lugar dos órgãos governamentais, eles sim, preocupam-se com a integridade e disponibilidade dessas informações.

Sendo assim, verifica-se que as organizações lidam com uma multiplicidade de informações tanto no seu ambiente interno como no externo, freqüentemente. O primeiro passo, como analisado nas etapas anteriores, é

evidenciá-las por meio da extração, aplicação da suas características e geração de um modelo de qualificação, para se ter uma visão geral dos seus atributo e impacto nos negócios. O segundo, envolve a priorização dessas informações e, consequentemente, a aplicação da norma para garantir as suas devidas proteções, conforme ilustra a figura 10.

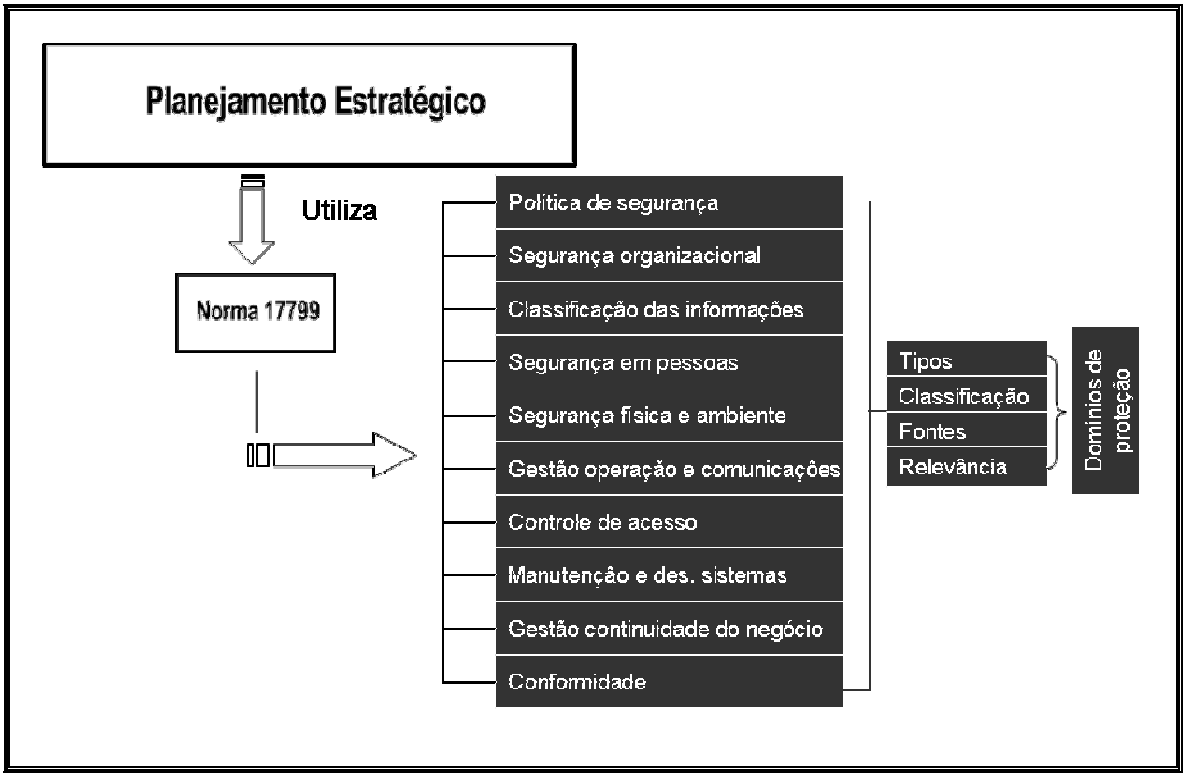

Figura 10: Utilização da norma NBR/ISO 17799:1

Portanto, é neste contexto de todas as etapas apresentadas, que se insere a contribuição da Ciência da Informação, tratando os fluxos de informação gerados a partir da elaboração do Planejamento Estratégico. Vê-se não simplesmente o uso de uma técnica que gera, trata, organiza, armazena e dissemina a informação em um contexto isolado dentro da organização, mas também um trabalho de gerenciamento da informação que atende os interesses sistêmicos na tomada de decisão e cria subsídios para criação efetiva de um Plano de Segurança da Informação.

5. CONCLUSÕES E SUGESTÕES PARA NOVOS TRABALHOS

Em decorrência das análises realizadas neste trabalho, desde a revisão dos conceitos de informação, Ciência da Informação, planejamento, estratégia, Planejamento Estratégico e segurança da informação, até a devida contribuição argumentada, chega-se às seguintes conclusões:

- É possível no processo de Planejamento Estratégico organizacional extrair as necessidades de informações que são geradas e organizadas em suas etapas de desenvolvimento, execução e controle;
- As informações podem ser caracterizadas conforme seus atributos como tipo, fonte, classificação, relevância e preparadas para aplicação dos domínios de proteção;
- A qualificação e priorização das informações são realizadas para classificá-las de acordo com seu nível de segurança e no contexto geral das organizações;
- A aplicação da Norma NBR/ISO 17799:1 é resultado das necessidades analisadas nesse trabalho, uma vez que, para sua aplicação, as informações foram caracterizadas;
- Diante das conclusões acima, é possível, de fato, realizar um Plano de Segurança da Informação, pois a informação foi

trabalhada desde sua origem no PE até a sua real necessidade de proteção.

Essas conclusões foram obtidas mediante análise dos fluxos de informações que o PE gera nas suas etapas de desenvolvimento, execução e controle.

Percebem-se diversos tipos de informações no momento de desenvolvimento do PE quando se utiliza técnicas de diagnóstico do ambiente, por exemplo, que é possível conhecer quais são os pontos fortes e fracos das organizações, como também suas oportunidade e ameaças.

Na execução, vê-se a necessidade de organizar as informações de forma que atendam os objetivos propostos no planejamento, atendendo os requisitos de valorização, utilidade e prioridades.

Já o controle enfatiza a revisão do processo de Planejamento, por considerar o dinamismo do ambiente organizacional. Portanto, são geradas novas informações a cada análise e realização de controle, podendo rever as necessidades de segurança.

Entende-se que a preocupação com a proteção das informações estratégicas nas organizações, se eleva na mesma proporção da sua valorização e utilidade para os departamentos estratégicos. Pois são nesses que são requisitadas as informações pelas quais subsidiam as tomadas de decisões.

Faz-se necessário também, apresentar as seguintes sugestões para novos trabalhos:

- Criar um modelo de Plano de Segurança da Informação – PSI, de forma abrangente e que se alinhe com a proposta apresentada neste trabalho.
- Aplicar em uma instituição a contribuição apresentada, realizando assim os processos de caracterização e seus respectivos domínios de proteção.

REFERÊNCIAS

17799:1, N. I. **Tecnologia da Informação –** código de prática para segurança da informação. Rio de Janeiro, 2000.

AGUIAR, Afrânio C. **Informação e atividades de desenvolvimento científico, tecnológico e industrial:** tipologia proposta com base em análise funcional. Ci. Inf., jan./jun. 1991, v.20, n.1, p.7-15.

ALDAY, H. E. C. **O planejamento estratégico dentro do conceito de administração estratégica.** Revista da FAE. Curitiba-PR; v.3, n.2, p. 9-16.

ALMEIDA, Amauri;SCHERER, Ivanói B.;VENTURA,Juarez L.;JÚNIOR,Roberto L.;ZANIN,Rogério F. **PLANEJAMENTO ESTRATÉGICO – UFSM REFERENCIAL TEÓRICO.** Santa Maria: UFSM, 1999.

ALMEIDA, Martinho Isnard Ribeiro de. **Manual de planejamento estratégico: desenvolvimento de um plano estratégico com a utilização de planilhas Excel.** São Paulo: Atlas, 2001.

ALVES, Gustavo A. **Segurança da informação:** Uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna Ltda, 2006.

AMARAL, Luis A M. **PRAXIS:** um referencial para planejamento de Sistemas de Informação. Tese de Doutorado apresentada na Universidade do Minho, Portugal, 1994.

ANSOFF, H. I. **Estratégia empresarial.** São Paulo: McGraw-Hill do Brasil, 1977. **Administração Estratégica**. São Paulo: Atlas, 1997.

ARAÚJO, Vânia M. R. Hermes de. **Sistemas de informação:** nova abordagem teórico-conceitual. Ci. Inf., Brasília, v.24, n.1, 1995.

AURÉLIO Buarque de Holanda Ferreira, **Novo dicionário Aurélio - O dicionário da língua portuguesa***, século XXI- 1ª ed.* Rio de Janeiro: Editora Nova Fronteira, 1975.

BARBOSA, R. R. **Inteligência Empresarial: uma avaliação de fontes de informação sobre o ambiente organizacional externo.** DataGramaZero – Revista de Ciência da Informação, v.3, n.6, dez/02.

BATTAGLIA, Maria da Glória Botelho. **A Inteligência Competitiva modelando o Sistema de Informação de Clientes – Finep.** Ci. Inf., Brasília, v.29, n.2, p.200-214, 1999.

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

BORGES, M. E. N; CAMPELLO, B. S. **A organização para negócio no Brasil.** Perspect. Ci. Inf., jul./dez. 1997, vol.2, nº2, p. 149-161.

BUCKLAND, Michal K. ***Information as thing.*** *Journal of the American Society for information Science (JASIS),* v.45, n.5, p.351-360, 1991.

BUSH, Vannevar. ***As we may think.*** *The Atlantic Monthly, Jul. 1945.* Disponível em: http://www.theatlantic.com/unbound/flashbks/computer/bushf.htm acesso no dia 02/01/07.

CALAZANS, A, T, S. **Conceitos e uso da informação organizacional e informação estratégica.** Transinformação, jan./abr., 2006, p. 63-70.

CAPURRO, R. ***Foundations of information science: review and perspectives.*** Tampere: University of Tampere, 1991. Disponível em: http://www.capurro.de/tampere91.htm acesso dia 02/01/07.

CAPURRO, R; HJORLAND, B. ***The Concept of Information***. Disponível em: http://www.capurro.de/infoconcept.html acesso dia 02/01/07.

CASTELLS, Manuel, ***A Era da Informação****, Vol.1 - A Sociedade em Rede*, São Paulo, Paz e Terra, 1999 (7ª edição).

CENDÓN, B. V. **Bases de dados de informação para negócio no Brasil.** Ci. Inf., maio/agosto 2003, vol. 32, nº 2, p. 17-36.

CERTO, Samuel; PETER, J. Paul. **Administração estratégica.** São Paulo: Makron Books, 1993.

CHIAVENATO, Idalberto. **Introdução à Teoria Geral da Administração.** 6.ed Rio de Janeiro: Campus,2000.

DAMASIO, Edílson. **O profissional da informação na indústria:** habilidades e competências. Dissertação (Mestrado) – Programa de Pós-Graduação em Biblioteconomia e Ciência da Informação da Pontifícia Universidade Católica de Campinas. Campinas, 2001.

DAVENPORT, Thomas H. **Ecologia da informação:** por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

DAWEL, George. **A segurança da informação nas empresas.** Rio de Janeiro: Ciência Moderna Ltda, 2005.

DEMO, Pedro. **Ambivalências da sociedade da informação**. Ci. Inf., Brasília, v. 29, n. 2, 2000.

EDWARDS, E. **Introdução à teoria da informação**. 2.ed. São Paulo: Cultrix, 1964. 147p.

FALSARELLA, Orandi M; JANNUZZI, Celeste A S C; BERAQUET, Vera S M. **Informação empresarial:** dos sistemas transacionais à latência zero. Transinformação, Set./Dez. 2003, p. 141-156.

FERREIRA, Fernando N. F. **Segurança da informação.** Rio de Janeiro: Ciência Moderna, 2003. 162p.

FISHMANN, A. A.; Almeida, M. I. R. *Planejamento estratégico na prática*. 2. ed. SãoPaulo: Atlas, 1991.

FONTES, Edison. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

GEUS, P. L.; NAKAMURA, E. T. **Segurança de redes em ambientes cooperativos.** 2.ed São Paulo: Futura, 2003.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** São Paulo:Atlas, 2002. 175p.

GRAY, Patrick. **O James Bond da Internet.** IstoÉ, São Paulo,jun. 2004. Entrevista concedida a Mariana Barros. Disponível em: http://www.terra.com.br/istoe/1812/1812_vermelhas_01.htm Acesso 30 de agosto 2006.

HAMPTON, David R. **Administração contemporânea:** teoria, prática e casos. 3ed. São Paulo: McGraw-Hill, 1981. 370p.

HOLANDA, Roosevelt de. **O estado da arte em sistemas de gestão da segurança da informação:** norma ISO/IEC 27001:2005. Módulo Security Magazine, disponível em: http://www.modulo.com.br/index.jsp?page=3&catid=18&objid=22&pagecounter=0&idiom=0 . Acesso em 30 de agosto 2006.

JANNUZZI, Celeste Aída Sirotheau Corrêa; MONTALLI, Katia Maria Lemos. Informação tecnológica e para negócios no Brasil: introdução a uma discussão conceitual. **Ci. Inf.**, Brasília, v. 28, n. 1, 1999.

JÚNIOR, Rogério H. A. **Benchmarking.** In: TARAPANOFF, K. (Org.). Inteligência organizacional e competitiva. Brasília: UnB, 2001. p. 241-263.

KOBASHI, Nair Y; TÁLAMO, Maria de Fátima G. M. **Informação:** fenômeno e objeto de estudo da sociedade contemporânea. Revista Transformação, Campinas, v. 15, p. 7-21, set./dez. 2003.

MAXIMIANO, Antonio C. A. **Introdução à administração.** 6ed. São Paulo: Atlas, 2004.

MCGARRY, Kevin J. **Da documentação à informação:** um conceito em evolução. Lisboa: Presença, 1984.

MESSIAS, Lucilene C S. **Informação:** matéria prima da Ciência da Informação. 2002. 113f. Trabalho de conclusão de curso – Departamento de Ciência da Informação da faculdade de Filosofia e Ciências, UNESP, Marília.

MIGLIATO, A. L. T. **Planejamento estratégico situacional aplicado à pequena empresa:** estudo comparativo de casos em empresas do setor de serviços (hoteleiro) da Região de Brotas – SP**.** 223f. Dissertação (Mestrado) – Escola de Engenharia de São Carlos. Universidade de São Paulo. São Carlos, 2004.

MIRANDA, Roberto C. R. **O uso da informação na formulação de ações estratégicas pelas empresas.** Ci. Inf., Set. 1999, v.28, n. 3.

MODULO E C. **2ª Pesquisa Nacional sobre o perfil do profissional em segurança da informação.** Rio de Janeiro, 2004. Disponível em: <http://www.modulo.com.br/pdf/pesquisa_perfil_2004.pdf>. Acesso em 30 de agosto de 2006.

MONTALLI, Katia Maria Lemos; CAMPELLO, Bernardete dos Santos. **Fontes de informação sobre companhias e produtos industriais**: uma revisão de literatura. Ci. Inf., Brasília, v. 26, n. 3, 1997.

MORESI, Eduardo A D. **Delineando o valor do sistema de informação de uma organização.** Ci. Inf., jan./abr. 2000, v.29, n.1, p.14-24.

OLIVEIRA, D. P. R. **Planejamento Estratégico:** conceitos, metodologia, práticas. São Paulo: Atlas, 2003.

PEREIRA, Maurício Fernandes. **O Processo de Construção do Planejamento Estratégico através da Percepção da Coalizão Dominante.** Florianópolis, 2002. 294 f. Tese (Doutorado em Engenharia de Produção) - Graduação em Engenharia de Produção, UFSC, 2002.

PINHEIRO, L. V. R. **Informação esse obscuro objeto da Ciência da Informação**. Morpheus, Rio de Janeiro, v. 02, n. 4, 2004

PORTER, Michael E. **Competição=on competiotion: estratégias competitivas essenciais.** Tradução de Afonso Celso da Cunha Serra. Rio de Janeiro: Campus,

1999.

ROBREDO, Jaime. **Da Ciência da Informação revisitada aos sistemas humanos de informação**. Brasília: Thesaurus; SSRR, 2003.

SARACEVIC, T. **Ciência da Informação:** origem, evolução e relações. Perspectivas em Ciência da Informação, Belo Horizonte, v.1, n.1, p. 41-62, jan./jun. 1996

SÊMORA, Marcos. **Gestão da Segurança da Informação.** Rio de Janeiro: Elsevier, 2003.

SHANNON, C. E.; WEAVER, W. **Teoria Matemática da Comunicação.** Urbana: The University of Illionois Press, 1963.

SILVA, Antônio G. **A escola dominical.** Rio de Janeiro: CPAD, 1998.

SILVEIRA, Henrique. **SWOT.** In: TARAPANOFF, K. (Org.). Inteligência organizacional e competitiva. Brasília: UnB, 2001. p. 209-226.

STEINER, G. A. ***Strategic planning:*** *what every manager must know. New York, the Free Press, 1979.*

VALENTIM, M L P. **O moderno profissional da informação: formação e perspectiva profissional**. Revista eletrônica de Biblioteconomia e Ciência da Informação, Florianópolis, nº 9, jun. 2000. Disponível em: <http://www.encontros-bibli.ufsc.br/Edicao_9/marta.html>. Acesso em 08 de maio 2006.

WILDEN, Anthony. **Informação.** In Enciclopédia Eunaudi, Vol 34. Lisboa: Imprensa Nacional, 2000, p. 11- 77.