CLAUDETE AURORA DA SILVA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: um olhar a partir da Ciência da Informação

CAMPINAS

2009

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

CLAUDETE AURORA DA SILVA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: um olhar a partir da Ciência da Informação

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Pontifícia Universidade Católica, como parte dos requisitos para obtenção do título de Mestre em Ciência da Informação.

Orientador: Profª Dra. Vera Silva Marão Beraquet

CAMPINAS

2009

Ficha Catalográfica

Elaborada pelo Sistema de Bibliotecas e
Informação – SBI – PUC-Campinas

S750g

Silva, Claudete Aurora

Gestão da segurança da informação: um olhar a partir da Ciência da Informação / Claudete Aurora da Silva – Campinas, São Paulo, 2008. 99 f.

Orientadora: Dr. Profª Vera Silva Marão Beraquet.
Dissertação (Mestrado) – Pontifícia Universidade Católica de Campinas, Centro de Ciências Sociais Aplicadas, Pós-Graduação em Ciência da Informação.
Inclui bibliografia.

1. Segurança da informação. 2. Sistema de informação. 3. Sistema de gestão de segurança da informação.

CDD 22.ed. CDD 171

As minhas filhas Giovanna e Manuella, razão da minha vida.

AGRADECIMENTOS

A CAPES pelo incentivo dado através da concessão de bolsa de estudo.

Aos professores do Programa de Pós-graduação em Ciência da Informação da Pontifícia Universidade Católica de Campinas, sem exceções pelo estímulo e aprendizado.

À professora Dr. Vera Marão Beraquet pela dedicação empreendida na orientação e soube compreender minhas limitações, me incentivando durante o desenvolvimento deste trabalho.

À minha mãe que, sem ela não teria conseguido chegar até o final dessa empreitada. As minhas irmãs Célia, Cleia, Carmen Lúcia e Cleide que me ajudaram sempre na minha educação e por não desistirem de mim.

Aos amigos conquistados ao longo do curso, especialmente ao João Pontes, Gardênia e Cláudia Barbosa pela contribuição dos artigos e ajuda nesse trabalho.

Agradeço ao amigo e companheiro Marcelo Gomes que compreendeu a minha ausência na execução deste projeto.

Agradecimento especial ao meu amigo Francisco Lopes de Aguiar pelo carinho, apoio e amizade ao longo dos anos e por me incentivar a fazer esse curso e pela discussão muito enriquecedora para meu conhecimento.

Agradeço a todos os colegas da Ituran principalmente os estagiários do CEIDOC, os que estão e os que passaram pelo departamento e acompanharam essa jornada, em especial os estagiários de biblioteconomia Eva Nicácio e Williamis Francisco, que responderam pelo departamento na minha ausência e que acompanharam e incentivaram o termino desse projeto. Ao meu Diretor Doron Feller que compreendeu e reconheceu a importância desse curso para minha carreira profissional.

Aos meus colegas da MBA em Gestão de Segurança da informação da FIAP que me ajudaram com esclarecimento da área.

Agradeço a todos que deram apoio, sorrisos, abraços, momentos de compreensão, paciência, ouvidos, livros, artigos, cuidados e alegrias.

A Deus por me dar coragem a não desanimar e conseguir tornar realidade mais esse sonho.

RESUMO

SILVA, Claudete Aurora. **Gestão da segurança da informação:** um olhar a partir da Ciência da Informação. Campinas: [s.n.], 2009. Dissertação (Mestrado) – Pontifícia Universidade Católica de Campinas. Pós-Graduação em Ciência da Informação.

A informação tem sido apontada como a principal fonte de poder nas organizações e, portanto faz necessário ser protegida. Para isso NBR ISO/ IEC 27001 define diretrizes para implementação de um Sistema de Gestão de Segurança da Informação, sujo o objetivo é salvaguardar os ativos da organização, garantir a continuidade dos negócios e propiciar confianças nas partes interessadas. O objetivo deste estudo foi caracterizar os aspectos teórico-metodológicos utilizada no tratamento da informação pode ajudar na implementação de um sistema de gestão de segurança da informação necessária. Os métodos utilizados para essa pesquisa foram qualitativos, partindo-se de um levantamento bibliográfico visando contribuir com a fundamentação teórica sobre o tema e leituras de obras para fundamentação da pesquisa. A partir da discussão dos conceitos, pretendeu-se explicitar como a gestão da informação na perspectiva da ciência da informação pode fornecer elementos para propor o sistema de gestão de segurança da Informação. Como principal resultado é um modelo conceitual de sistema de informação que seja eficaz ao apoiar os gestores no processo de implementação do SGSI.

Palavras-chave: segurança da informação, sistema de informação, sistema de gestão de segurança da informação

ABSTRACT

SILVA, Claudete Aurora. Information security management: a look from the Information Science. Campinas: [s.n.], 2009. Dissertação (Mestrado) - Pontifícia Universidade Católica de Campinas. Graduate Studies in Information Science

The information has been identified as the main source of power in organizations and therefore is necessary to be protected. For that NBR ISO/ IEC 27001 defines guidelines for implementation of a Management System of Information Security, dirty the objective is to safeguard the assets of the organization, ensuring continuity of business and provide confidence in stakeholders. This study aimed to characterize the theoretical and methodological aspects used in the processing of information can help in implementing a safety management system the necessary information. The methods used for this research was qualitative, based on a literature review to contribute to the theoretical foundation on the topic and readings of works for reasons of research. From the discussion of concepts, tried to explain how the management of information in view of information science can provide evidence to suggest the safety management system of information. As the main result is a conceptual model of information system that is effective to support the managers in the implementation process of SGSI.

Keywords: information security, information system, management system of information security

.

LISTA DE ILUSTRAÇÕES

FIGURAS

LISTA DE ABREVIATURAS

ABNT	Associação de Normas técnicas
CI	Ciência da Informação
GI	Gestão da Informação
SI	Segurança da Informação
SGSI	Sistema de Gestão de Segurança da Informação
TI	Tecnologia da Informação

SUMÁRIO

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

Autor (a): SILVA, Claudete Aurora da.

Título: "GESTÃO DE SEGURANÇA DA INFORMAÇÃO: UM OLHAR A PARTIR DA CIÊNCIA DA INFORMAÇÃO ".

Orientador (a): Profa. Dra. Vera Silvia Marão Beraquet

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: 18/02/2009.

BANCA EXAMINADORA

Profa. Dra. Vera Silvia Marão Beraquet

Profa. Dra. Valéria Martin Valls

Prof. Dr. Orandi Mina Falsarella

1 INTRODUÇÃO

À medida que as organizações crescem e se tornam mais complexas, ocorre um aumento da necessidade da importância da informação. A informação passa a ser não somente útil em nível operacional, mas também em nível tático e estratégico. Nesse contexto, não apenas o conteúdo da informação é relevante, mas a forma como a informação é trabalhada ganha importância. A eficácia no tratamento da informação depende de grande parte de como ela é administrada e do bom entendimento de alguns conceitos e relações, sob pena de fornecer ao usuário apenas dados desconexos, comprometendo o processo decisório.

Foram grandes as transformações ocorridas no século XX, principalmente no que se refere aos aspectos tecnológicos: podemos destacar a invenção do computador e conseqüentemente a oferta no mercado desses produtos, tornando clara a importância da informação e do conhecimento na sociedade.

A informação tornou-se algo imprescindível para o sucesso de qualquer organização com a crescente e constante evolução de diferentes tecnologias, tais como: negócios e comércio eletrônicos, telecomunicações e computação, e a própria Internet; ou seja, a quantidade de informações disponíveis tem aumentado.

Lyman (2001) estima que a quantidade de informação disponível duplique de dois em dois anos. Em 2003 foi estimado que a quantidade de informações armazenadas nos computadores, impressa e gravada em suportes óticos e digitais atingiu cerca de oito exabytes, o equivalente a um gigabyte por cada habitante do planeta.

Robredo (2004, p.43) afirma que apesar da tecnologia oferecer soluções para organizar grandes volumes de documentos, a organização da informação neles contida é um problema. Para este autor “é preciso aprofundar e aprimorar os processos de análise da informação e representação da informação para alcançar maior sucesso na recuperação”.

As informações disponíveis nas organizações que são armazenadas são manipuladas entre os mais diversos setores e sistemas de informação. As

decisões e ações são tomadas decorrentes destas informações que devem ser corretas, precisas e estarem disponíveis.

Com todo o avanço tecnológico que se delineou nas últimas décadas, as organizações também vêm sendo forçadas a pensarem não só na aquisição e utilização desses recursos informacionais, mas também em como protegê-los.

No entanto, para que haja o reconhecimento da informação enquanto um ativo social e econômico, faz-se necessária a implementação e gestão de controles nos processos de produção, acesso e uso da informação.

Atualmente a informação pode ser considerada como um dos principais patrimônios de uma empresa, o qual está sob constante risco (DIAS, 2000). Entende-se que uma organização corre risco quando suas vulnerabilidades estão sendo exploradas. Para evitar este risco, uma organização deve ter mecanismos capazes de identificar seus pontos vulneráveis. Não se trata apenas de conhecer algumas ferramentas e técnicas. É necessário ter uma metodologia para orientar as ações a serem tomadas usando recursos, técnicas e ferramentas necessárias.

Desse modo é necessário o controle, normalização e consistência da informação mediada pelo controle dos processos e o tratamento da informação para assegurar os pilares da Segurança da Informação (SI), que são integridade, confidencialidade e disponibilidade.

As práticas de SI baseiam-se no instrumental teórico-metodológico para implementação de um sistema de gestão de segurança da informação. A NBR ISO/ IEC 27001 foi desenvolvida para prover um modelo para estabelecer, implementar, operar, monitorar, analisar, criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

O SGSI é o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que de forma conjunta, definem como são reduzidos os riscos para SI. Uma empresa que implante a NBR ISO/ IEC 27001 acaba por constituir um SGSI.

A Gestão da Informação vem se concentrando em uma metodologia nas questões de coerência, redundância e qualidade de informação por via de meios automáticos. Estas facilidades têm de garantir um equilíbrio entre os meios colocados ao dispor para assegurar a rastreabilidade (quem fez o quê, e quando) e

auditabilidade (o que foi feito) tendo em atenção às questões de privacidade (quem acede ao quê) e confidencialidade (o que é obtido de quem). Este equilíbrio, regulado por políticas internas, por questões de ética e cada vez mais é sujeito a normas e regulamentações diversas impostas por meios legais.

Diante do enunciado acima, acredita-se ser vital o desenvolvimento de pesquisas que busquem compreender e aproximar o corpus teórico e metodológico que norteiam a GI e a importância da aplicação através das principais medidas utilizando o campo da CI para auxiliar os processos de controle do SGSI.

1.1 Justificativas do estudo

O presente trabalho tornou-se justificável pelos seguintes motivos:

- ✓ Ordem pessoal

Graduada em Biblioteconomia e atuando com gestão de informação e arquivos em empresas há mais de seis anos, recebi um convite, em 2007, para assumir a função *Chief Security Office* (CSO), em uma empresa multinacional israelense. No início fiquei um tanto perplexa, mas aceitei o desafio. Atuando nessa função, tive a necessidade de buscar conhecimento e aprimorar minhas habilidades no tratamento da informação para implementar políticas e dispositivos de segurança. Com isso pude perceber a utilização da SI como uma poderosa ferramenta de competitividade e como diferencial estratégico para as organizações.

Esta pesquisa foi de grande enriquecimento pessoal e profissional, uma vez que tive a oportunidade de aliar meus conhecimentos técnicos a uma abordagem aos princípios do SGSI.

- ✓ Ordem Institucional

Esta pesquisa contribuirá para a melhor concepção de alunos e professores da área de CI sobre o tema de SI e apresentá-la como controle e processo e não somente como software e hardware na proteção da informação.

Destaca-se também que a literatura existente sobre segurança da informação refere-se em grande parte a uma concentração de pesquisadores oriundos da ciência da computação, sistemas da informação e engenharia de

produção. Diante desse quadro, entendeu-se como bastante relevante a investigação desse tema sob a ótica da Ciência da Informação.

- ✓ Ordem teórica

No processo de sistematização desse estudo foi enfatizada a área da CI sob a linha de pesquisa “Gestão da Informação” no âmbito da “Organização e Tratamento da Informação” como recurso para melhor compreensão dos processos de implementação de um SGSI.

Para compreensão da importância da informação no contexto da SI e a necessidade de mecanismos de SI, nos pautamos nas orientações teórico-conceituais e metodológicas da CI, visto que esta investiga as propriedades e o comportamento da informação, seu fluxo e os meios de processá-la para otimizar a sua acessibilidade.

É importante ressaltar que a produção de conhecimentos sobre o desenvolvimento, aplicação e uso do SGSI no campo da CI ainda é pouco expressivo, em termos acadêmicos. No Brasil a questão é legitimada com pioneirismo nas discussões empreendidas pelas áreas da Tecnologia da Informação (TI).

- ✓ Ordem prática

Trabalhos produzidos na linha desta dissertação podem ser de grande relevância no sentido de apresentar argumentos que venham a ajudar gestores a trabalharem com sistema de informação voltado para as melhores práticas de SI, ajudando seu posicionamento estratégico devido ao conhecimento das normas e padrões que garantam os serviços corporativos, bem como para continuidade dos negócios da empresa.

1.2 Hipótese

A revisão da literatura e a observação empírica da autora mostraram que o SGSI é muitas vezes implementado e estruturado somente no ambiente lógico, isto é, as práticas usuais privilegiam os seus aspectos técnicos e tecnológicos, tais como implementação de ferramentas de monitoração de diversas atividades dos usuários e *firewall*.

Considerando o fato de que, cada vez mais as organizações manipulam grandes volumes de informações, dados e conhecimentos no âmbito formal e informal, há necessidade de dotar mecanismos e recursos tecnológicos baseados nas premissas da organização, tratamento e representação, recuperação da informação para garantir uma abordagem sistêmica de um SGSI.

Nesse sentido Davenport (2000, p.12) alerta que não basta somente investimentos em recursos tecnológicos para se fazer a gestão da informação, é necessário implementar uma abordagem sistêmica dos processos de produção, comunicação e uso da informação, enfatizando principalmente as questões em torno da organização e tratamento da informação.

Davenport (2000, p.14), propõe uma abordagem denominada de "ecologia da informação" para o gerenciamento da informação. Enfatiza "a maneira como as pessoas criam, distribuem, compreendem e usam a informação". O autor complementa esta orientação ao afirmar que:

- a informação não é facilmente arquivada em computadores – e não é constituída apenas de dados;
- quanto mais complexo o modelo de informação, menor será sua utilidade;
- a informação pode ter muitos significados em uma organização;
- a tecnologia é apenas um dos componentes do ambiente de informação e freqüentemente não se apresenta como meio adequado para operar mudanças.

Considera-se inicialmente como hipótese que os princípios da GI na perspectiva da CI podem contribuir significativamente ao indicar uma abordagem sistêmica dos processos; enfatizando as especificidades de controle (organização e tratamento), acesso e uso (representação e recuperação) na concepção de um SGSI.

1.3 Delimitação do estudo

Salienta-se que a área desta pesquisa consistiu na Gestão da Informação, dentro da perspectiva da Ciência da Informação, incluindo sua interface com a área de Segurança da Informação.

Dessa forma não se abrangeu aspectos específicos de tecnologia como *Software* e *Hardware* de sistemas de informação, assim como considerações relativas à sua implementação.

Sobre a SI, foi utilizada uma abordagem que permite conhecer seus conceitos básicos e as definições amplamente utilizadas, bem como utilizando as normas NBR ISO/ IEC 27001 SGSI requisitos e a NBR ISO/ IEC 27002 código de práticas como referência principal.

1.4 Objetivos

Esta pesquisa buscou examinar a concepção de um SGSI através de dispositivos metodológicos no contexto da Gestão da Informação (GI) na perspectiva da Ciência da Informação (CI), utilizando o tratamento da informação no seu ciclo de vida, ou seja, no contexto de coleta, organização, armazenamento, recuperação e disseminação. Parte dos esforços realizados pelos sistemas de informação é assegurar o fluxo de informação de modo a servir os profissionais e parceiros de uma organização e a sustentar a operacionalização do seu negócio.

Caracterizar os princípios básicos dos controles de segurança do tratamento da informação, da classificação e controles dos ativos de informação enquanto componentes de um SGSI, proposto pela NBR ISO/ IEC 27001;

1.5 Procedimentos metodológicos

Toda pesquisa científica é caracterizada pelo uso de um método. Na opinião de Marconi e Lakatos (2000), o método constitui-se como um conjunto de atividades sistemáticas e racionais, que dá maior segurança e economia para alcançar os objetivos, delineando o caminho a ser seguido, detectando erros e auxiliando as decisões do pesquisador.

O método que norteia esta pesquisa é o indutivo. “Indução é um processo mental por intermédio do qual, partindo de dados particulares, suficientemente constatados, infere-se uma verdade geral ou universal, não contida nas partes examinadas” (MARCONI; LAKATOS, 2000, p.53). Dessa forma, serão buscados na literatura, dados que tragam respostas à hipótese estabelecida.

De acordo com Richardson et al. (1999), o presente trabalho possui também uma característica qualitativa, que é uma forma adequada para entender a natureza de um fenômeno social. Para o autor, os estudos que empregam esta metodologia qualitativa podem descrever a complexidade do problema em questão, analisando a interação de certas variáveis. Para Serapioni (2000, p.27), o método qualitativo “se aplica às áreas com pouco conhecimento teórico ou conceitual ou às pesquisas que não possuem hipóteses formuladas ou precisas”. Nesses casos, este método ajuda a compreender não apenas ao objeto de estudo, mas também a construí-lo a partir de novos aspectos e sob novas perspectivas.

Além disso, de acordo com Gil (1991), esta pesquisa é exploratória, pois tem o objetivo principal de aprimorar idéias, considerando os mais variados aspectos relativos ao fato a ser estudado, e que envolve levantamento bibliográfico e análise de cenários relacionados a fim de estimular a sua compreensão.

A abordagem metodológica escolhida para esse estudo foi exploratória, partindo-se de um levantamento bibliográfico na qual efetua um levantamento de teses, dissertações e trabalhos existentes nas universidades brasileiras, particularmente os desenvolvidos nas áreas da CI, computação e administração.

Procede-se, também, às pesquisas em livros, revistas especializadas e na rede mundial de computadores internet para afirmar os conceitos sobre SI na CI.

Além da pesquisa bibliográfica, considera também a experiência profissional do autor deste trabalho na área de SI, o que proporcionou oportunidade única de perceber, dentre outros fatores a importância de se fazer GI levando em consideração os princípios da SI e a importância da terminologia e linguagens dessa especialidade.

1.7 Estrutura do trabalho

Esta pesquisa está estruturada da seguinte forma: o primeiro capítulo compreende a introdução do trabalho, contextualizando-o e apresentando a justificativa, hipótese, problema, delimitação do estudo, objetivos e os procedimentos metodológicos adotados.

No segundo, terceiro e quarto capítulo foi feita uma revisão de literatura acerca dos conceitos de Segurança da Informação, Sistema de Gestão da Segurança da Informação e Gestão da Informação, que são a base deste trabalho.

O quinto capítulo apresenta a análise das informações obtidas na revisão de literatura. Por último, o sexto capítulo traça as considerações finais, seguido das Referências utilizadas.

2 SEGURANÇA DA INFORMAÇÃO

A preocupação com a SI sempre existiu na humanidade. Estudos mostraram que alguns monumentos construídos por Khnumhote, arquiteto do faraó Amenemhet II, foram documentados e tiveram trechos dessas documentações “codificados” através da substituição de palavras ou trechos do texto escrito em tabletes de argila. Caso esse tablete fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro – morreria de fome, perdido nas catacumbas da pirâmide. (KAHN, 1967).

Diversos algoritmos de compactação foram desenvolvidos desde a Segunda guerra mundial devido à necessidade de comunicação entre as tropas. Durante a guerra, a utilidade da compactação não era apenas a de diminuir a quantidade de informação que era passada através dos rádios, mas também a de “esconder” de alguma forma, o conteúdo da informação para que esta não pudesse ser lida pelo inimigo. Isto é possível, pois um algoritmo de compactação nada mais é do que um codificador e um decodificador que é aplicado a um conjunto de dados.

Já nos tempos dos mainframes, as empresas não tinham somente uma preocupação com o sigilo das informações, mas também com o próprio equipamento devido ao seu grande custo. Estes equipamentos ficavam em salas isoladas com baixa temperatura e acesso restrito à poucas pessoas. Além da preocupação com o ambiente físico, as empresas também buscavam se assegurar que, em caso de danos das informações por acidentes ou defeitos nos equipamentos, também pudessem recuperar as informações perdidas. Realizavam então, cópias das informações (b*ackup*) como medida de segurança, para recuperação de dados em caso de perdas acidentais ou intencionais.

Para enfatizar a segurança de informação e os mecanismos, foi aplicada uma pesquisa nacional de SI realizada em outubro de 2003 pela empresa Módulo Security Solutions S.A, conforme os resultados abaixo .

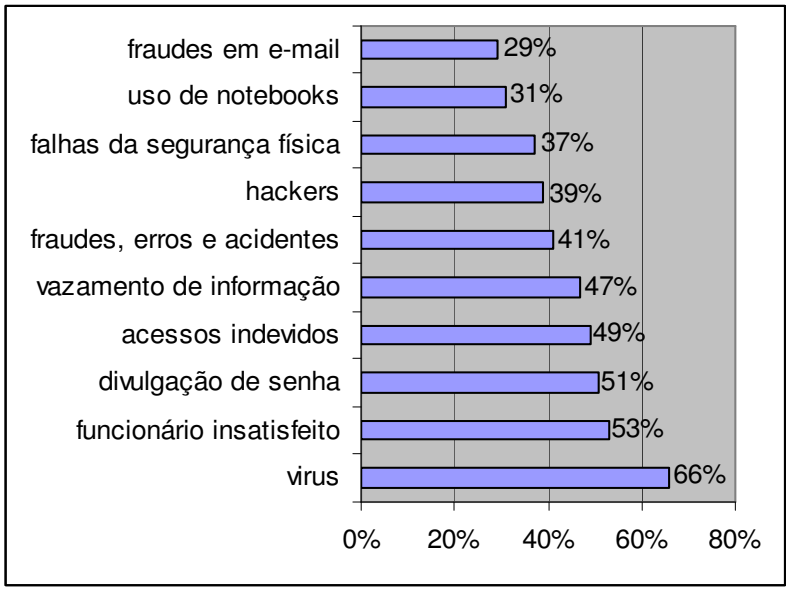


Figura 1 – Gráfico de pesquisa realizada pela empresa Módulo Security Solutios S.A.[1]
Fonte: Menezes (2006, p.26)

Conforme CARUSO, STEFFEN (1999), a necessidade de segurança é um fato que vem transcendendo o limite da produtividade e da funcionalidade. Enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios.

O conceito segurança significa no dicionário Houaiss, “um conjunto de processos, de dispositivos, de medidas de preocupação que asseguram o sucesso de um empreendimento, do funcionamento preciso de um objeto, do cumprimento de algum plano etc.”.

No mundo informatizado, segurança significa, segundo a norma NBR ISO/ IEC 27002, “proteção” da informação contra vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades para a organização.

A partir do conceito da norma verificamos que outros autores conceituam SI, uns com mais especificidades e outros mais generalistas, conforme apresentamos a seguir:

[1] As questões aceitavam respostas múltiplas.

- Segundo Sêmola (2003, p.43), SI é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou a sua indisponibilidade.
- Fontes (2006), SI 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.
- Beal (2005) define SI como processo de proteger as informações das ameaças, usando a preservação dos ativos, levando em conta os três objetivos fundamentais da SI.

Portanto, pondera nessa dissertação o conceito elucidado por Dias (2000), que ao pensar em SI devemos ter em mente que a informação precisa ser protegida independente do suporte onde esteja armazenada ou do canal na qual será transmitida ou transportada, não importando onde ela esteja (no papel, na memória do computador, em mídia ou trafegando pela linha telefônica). Um sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como esperado, porém, segurança é um conceito que vai além; é expectativa de todos que a informação armazenada em um sistema computacional permaneça lá, sem que pessoas não autorizadas tenham acesso a seu conteúdo.

Podemos afirmar que a expectativa de qualquer usuário é que as informações estejam em local adequado, disponíveis no momento desejado, que sejam confiáveis, corretas e permaneçam protegidas contra acessos indesejados.

A SI é dividida em segurança física e lógica. Ainda que a estrutura da administração de segurança se volte mais para a segurança de acesso lógico a segurança física é tão importante quanto.

Segundo a (NBR ISO/ IEC 27001, p13) objetivo da segurança física é “prevenir o acesso não autorizados, dano e interferência às informações e instalações físicas da organização”.

A segurança lógica compreende a integridade dos arquivos de dados e os programas da empresa. A segurança física compreende equipamentos

(processadores, monitores, laptops) equipamentos de comunicação (roteadores, PABXs, fax, secretárias eletrônicas), mídia magnética (fitas e discos).

Podemos afirmar que para obter um ambiente lógico inteiramente seguro, faz-se necessária a aplicação dos mesmos cuidados com a segurança física no que diz respeito aos equipamentos que armazenam essas informações, pois a segurança física complementa a segurança lógica.

Para Foina (2001, p. 138) o objetivo da segurança física é preservar o patrimônio da empresa, inclusive seus arquivos, contra roubos e sabotagem para prevenção. Garantir os controle físicos para a preservação dos equipamentos e instalações para que usuários mau intencionados não danifiquem ou destruam equipamentos e instalações poderia provocar a paralisação da organização, que prejudicaria a imagem junto ao mercado. Os problemas mais comuns relacionados com a segurança física são:

- Roubo de insumos (fitas, disquetes, etc.) e partes de microcomputadores (memórias, discos etc);
- Acesso de pessoas não autorizadas aos relatórios com dados estratégicos da empresa, ainda dentro do setor de tecnologia de informação;
- Cópias não autorizadas dos cadastro de clientes e fornecedores com o objetivo de vender mala direta para outras empresas;
- Sabotagem em equipamentos e arquivos de dados.

Os recursos e instalações de processamento de informações críticas ou sensíveis do negócio devem ser mantidos em áreas seguras e protegidos. Para diminuir os problemas causados pelo acesso físico é necessário a adoção de alguns controles, tais como: cartões magnéticos e bloqueios de portas; considerando que certas áreas devem ter acessos limitados como a fitoteca[2] de segurança e o próprio centro de processamento.

[2] Segundo LAROUSSE Cultural. São Paulo: Nova Cultural, 1999. p. 435. Conjunto de fitas magnéticas estocadas e organizadas para serem conservadas ou utilizadas em um centro de processamento de dados.

Um sistema confiável de controle de acesso permite identificar tentativas de quebras de segurança antes que ela se efetive. Consideram-se ameaças físicas: incêndios, desabamentos, relâmpagos, alagamento, acesso indevido de pessoas, forma inadequada de tratamento e manuseio do material.

O reconhecimento da SI como processo que garante a proteção da informação no ambiente físico e lógico, só é possível com o envolvimento simultâneo dos três principais recursos da organização que são pessoas, tecnologias e processos,

Na gestão da SI, a qualidade do processo deverá contemplar os três principais recursos da organização, conforme a figura abaixo:

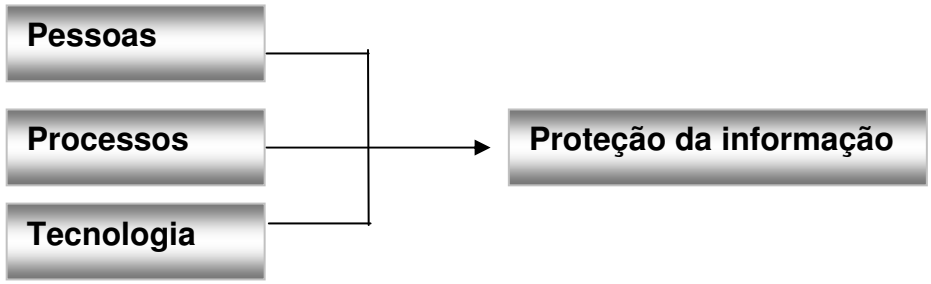


Figura 2 – Diagrama da SI.
Fonte: A autora.

Garantir a segurança da informação exige a proteção dos ativos da informação contra a perda, furto, alteração, divulgação ou destruição indevida. Toda organização precisa adquirir uma visão sistêmica da suas necessidades de segurança dos recursos a serem protegidos e das ameaças a que estão sujeitas. Enfim, utilizando um conjunto de controles que permite conhecer e gerir riscos, orientar as ações de continuidade do negócio, níveis de responsabilidade e conformidade com diretrizes, legislação e acordos contratuais como recomenda a norma ISO para segurança da informação.

2.1 Norma ISO para segurança da informação

Conforme a ABNT a palavra ISO não é uma sigla e sim um nome, que pode ser abreviada de diversas formas, em diversos idiomas (OIN em português, IOS em inglês, OIN em francês ,etc). O nome ISO è derivado da palavra grega isos que significa igual. A NBR ISO/ IEC 27001 é no Brasil é representado pela Associação Brasileira de Normas Técnicas ABNT.

A norma é um conjunto de requisitos necessários para a execução de um SGSI, permitindo às organizações obterem uma certificação de segurança, sendo um padrão de excelência que orienta a organização de um SGSI.

Motivados pela busca de soluções para o desafio de criar ambientes seguros para a informação, diversos profissionais de várias áreas e organizações vêem se esforçando para criar normas que sistematizem o trabalho de criar ambientes seguros, principalmente de TI. Um desses resultados foi consolidado com a norma NBR ISO/ IEC 27002. Utilizando-se essa norma, que é um guia de melhores práticas, simplifica-se o trabalho de adoção e cumprimento de políticas e padrões definidos, bem como da posterior verificação da conformidade dos resultados alcançados.

Um modelo de SGSI visa assegurar o implemento de processos que garantam as operações para proteger as informações estratégicas aos negócios e evitar incidentes de segurança. A medida de proteção deve ser proporcional à necessidade do negócio

Uma norma de SI apresenta mais do que vários controles de segurança. Ela permite a criação de um mecanismo de certificação das organizações semelhantes às certificações ISO já existentes., Contudo, esta nova certificação afirma que a organização certificada manipula seus dados e os dos clientes de forma segura, independente da forma como os registros estão armazenados.

A preparação para a certificação representa a preocupação da empresa em demonstrar sua capacidade em atender os controles necessários para garantir os requisitos de segurança sobre os ativos da informação.

Afirmar que uma organização é normatizada significa dizer que a mesma utiliza os recursos adequados para garantir a disponibilidade, confidencialidade e a integridade de suas informações.

Com a alta direção compromissada e o treinamento eficaz dos colaboradores, é possível reduzir o número de ameaças que exploram eventuais vulnerabilidades.

A seguir, apresentamos os principais conceitos estabelecidos e as práticas adotadas na implementação do SGSI que foram utilizadas na condução dessa pesquisa.

Principais elementos da norma:

1. escopo: abrangência da norma ;
2. referências normativas: determina que os requisitos apresentados sejam genéricos para implantação em qualquer organização;
3. termos e definições: apresentação dos principais conceitos relacionados a segurança da informação;
4. sistema de gestão de segurança da informação: determina que a organização deva desenvolver , implementar, manter e melhor continuamente o SGSI;
5. responsabilidade da alta direção: comprometimento da alta administração com SGSI;
6. análise crítica da SGSI: a alta administração deve revisar o SGSI em intervalos planejados;
7. melhoria do SGSI: a organização deve melhorar continuamente a efetividade na SGSI.

A NBR ISO/ IEC 27001 propõe o SGSI, que utiliza o modelo de PDCA visando prover um modelo de gestão dentro de uma perspectiva da estratégica da organização. Por sua vez, a NBR ISO/ IEC 27002 é um conjunto de boas práticas que podem ser aplicadas por um SGSI.

Ao Implementar um modelo de SGSI em uma organização significa construir uma sistemática abrangente, integrada e contínua, para minimizar ricos associados a informação.

A NBR ISO/ IEC 27001 incorpora um processo de escalonamento de risco e valorização de ativos orientando quanto sua à sua análise e identificação de riscos e a implantação de controles para minimizá-lo.

A organização pode adotar os padrões da ISO sem necessariamente solicitar a certificação além disso podemos verificar que a norma não traz as ferramentas a serem adotadas e sim orienta para desenvolver mecanismos de acordo com as suas necessidades do negócio em relação a seus riscos considerando os critérios básicos da SI.

2.2 Vulnerabilidade e ameaças

Um incidente de segurança poderá assim ser causado pelo ponto de uma vulnerabilidade onde poderá acontecer um ataque, ou seja, o ponto onde uma fraqueza ou deficiência de segurança poderá ser explorada.

Para Moreira (2001, p.22) a vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc. Condição causada muitas vezes pela ausência ou ineficiência das medidas de proteção utilizadas de salvaguardar o bem da empresa.

O autor ilustra a questão das vulnerabilidades que possibilitam os incidentes de segurança, sendo que estes afetam o negócio da empresa causando impactos negativos para clientes e demais envolvidos.

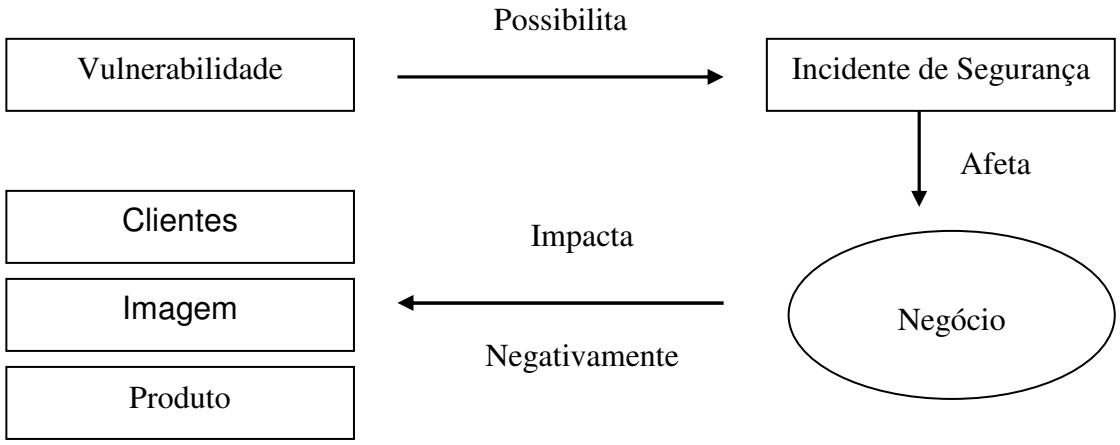


Figura 3 – Impactos dos incidentes de segurança nos negócios
Fonte: Moreira (2001)

Devido inúmeras vulnerabilidades em redes conectadas à internet, muitos incidentes têm marcado presença no dia-a-dia das empresas. Uma invasão que explora uma vulnerabilidade pode ocasionar as seguintes ocorrências:

- documentos confidenciais divulgados na internet;
- funcionários divulgando material pornográfico;
- contas e senhas roubadas para posterior utilização;
- linha de comunicação grampeada e informações sigilosas da empresa ficam comprometidas;
- servidores podem entrar em pane através do recebimento de vírus.

Há incidentes e ameaças que comprometem as informações e seus ativos os que certamente acarretam graves problemas para a organização.

Sêmola (2003, p.47) conceitua ameaça como sendo agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio de exploração de vulnerabilidades, provocando perdas, causando impactos aos negócios de uma organização e classifica ameaça como:

- naturais: ameaças decorrentes da natureza, como incêndios, enchentes, terremotos, entre outros;

- involuntárias: ameaças inconscientes, quase sempre causadas pelo desconhecimento. Exemplos: acidente, erros, falta de energia, entre outros;
- voluntárias: ameaças propositais causadas por agentes humanas como hacker, invasores, disseminadores de vírus, entre outros.

A ameaça é qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade, gerando um determinado impacto e para as ameaças existir precisa das vulnerabilidades para causar os impactos.

A segurança desenvolvida a partir de um evento negativo esperado se baseia no tempo em que se vive tal evento, ou seja, antes, durante e depois do acontecimento. As respostas são distintas para cada momento dependendo da segurança contemplada. A aproximação negativa implica na fase antes do evento onde gastos são feitos para manter um estado de alerta mesmo que este evento nunca ocorra. Esta fase é pró-ativa, identificando futuras vulnerabilidades e possíveis oportunidades. Os custos são diferenciados e dependentes de cada momento do ocorrido.

Nas ações reativas durante o evento, os gastos são feitos para conter as perdas cujo objetivo é restabelecer as condições necessárias para continuidade dos negócios. Na aproximação de um evento negativo, o benefício oferecido à organização pela gestão da segurança é medido com a redução das perdas. No ato do evento, a função da gestão da segurança se fará eficaz se permitir a organização melhorar seu ambiente de trabalho, a direção estratégica inclusive as funções táticas que darão suporte as ações garantindo a capacidade do negócio.

Finalizando, uma fase mais reflexiva em que ações são planejadas e implementadas para normalização do ambiente no intuito de restabelecer o estado de alerta. As estratégias em segurança serão traçadas para visualizar um ambiente em que tais perdas sejam minimizadas otimizando a utilização dos recursos.

2.3 Confidencialidade, Integridade e Disponibilidade

O princípio da confidencialidade da informação tem como objetivo garantir apenas que a pessoa correta tenha acesso a informação.

As informações trocadas entre os indivíduos e empresas nem sempre deverão se conhecidas por todos. Muitas informações geradas pelas pessoas se destinam a um grupo específico de indivíduos e, muitas vezes, a uma única pessoa. Isso significa que esses dados deverão ser conhecidos apenas por um grupo controlado de pessoas, definido pelo responsável da informação.

Ter confidencialidade na comunicação é ter a segurança de que o que foi dito a alguém ou escrito em algum lugar será escutado ou lido por quem tiver autorização para tal.

Perda de confidencialidade significa perda de segredo. Se uma informação for confidencial, ela será secreta e deverá ser guardada com segurança, e não divulgada para pessoas não-autorizadas.

Proteger a confidencialidade é um dos fatores determinantes para a segurança e uma das tarefas mais difíceis de implementar, pois envolve todos os elementos que fazem parte da comunicação da informação, partindo do emissor, passando pelo caminho percorrido e chegando até o receptor. Além disso, informações têm diferentes graus de confidencialidade, normalmente relacionados a valores. Quanto maior for o grau de confidencialidade, maior será o nível de segurança necessário na estrutura tecnológica e humana que participa desse processo: uso, acesso, trânsito e armazenamento das informações.

Deve-se considerar a confidencialidade com base no valor que a informação tem para a empresa ou a pessoa e os impactos causados por divulgação indevida. Assim, deve ser acessada, lida e alterada somente por aqueles indivíduos que possuem permissão para tal. O acesso deve ser considerado com base no grau de sigilo das informações, pois nem todas as informações importantes da empresa são confidenciais.

Grau de sigilo: As informações geradas pelas pessoas têm uma finalidade específica e destinam-se a um indivíduo ou grupo. Portanto, elas precisam de uma

classificação com relação à sua confidencialidade. É o que chamamos de grau de sigilo, que é a graduação atribuída a cada tipo de informação com base no grupo de usuários que possuem permissões de acesso. O grau de sigilo faz parte de um importante processo de segurança de informações, a classificação da informação[3].

O segundo dos três princípios da SI é a integridade que permite garantir que a informação não seja alterada de forma não autorizada e, portanto, é íntegra. Em suma, uma informação íntegra é uma informação que não foi alterada de forma indevida ou não autorizada.

Para que a informação possa ser utilizada, ela deve estar íntegra. Quando ocorre uma alteração não-autorizada da informação em um documento, isso quer dizer que o documento perdeu sua integridade.

A Integridade da informação é fundamental para o êxito da comunicação. O receptor deverá ter a segurança de que a informação recebida, lida ou ouvida é exatamente a mesma que foi colocada à sua disposição pelo emissor para determinada finalidade. Estar íntegra quer dizer estar em seu estado original, sem ter sofrido qualquer alteração por alguém que não tenha autorização. Se uma informação sofre alterações em sua versão original, então ela perde sua integridade, o que pode levar a erros e fraudes, prejudicando a comunicação e o processo de decisões.

A informação poderá ser alterada de várias formas, tanto em seu conteúdo quanto no ambiente que lhe oferece suporte. A quebra da integridade de uma informação pode ser considerada sob dois aspectos:

- Alterações do conteúdo dos documentos – quando são realizadas inserções, substituições ou exclusões de parte de seu conteúdo.
- Alterações nos elementos que fornecem suporte à informação – quando são realizadas alterações na estrutura física e lógica onde a informação está armazenada.

---

[3] Extraído da apostila desenvolvida pelo Módulo Security e revisada pelo capítulo Brasil da ISSA, em parceria com a Microsoft Informática em dezembro de 2006. Material distribuído em aula.

Buscar a integridade é tentar assegurar que apenas as pessoas ou sistemas autorizados possam fazer alterações na forma e no negócio e no conteúdo de uma informação, ou que alterações causadas por acidentes ou defeitos de tecnologia não corram, assim como no ambiente no qual ela é armazenada e pela qual transita em todos os ativos.

Logo, para proteger a integridade, é preciso que todos os elementos que compõem a base da gestão da informação se mantenham em suas condições originais definidas por seus responsáveis e proprietários.

Além de se trabalhar para que a informação chegue apenas aos destinatários ou usuários adequados e de forma íntegra, deve-se fazer com que esteja disponível no momento oportuno. É disso que trata o terceiro princípio da SI: a disponibilidade.

Refere-se à disponibilidade da informação e de toda a estrutura física e tecnológica que permite o acesso, o trânsito e o armazenamento.

A disponibilidade da informação permite que:

- seja utilizada quando necessário;
- esteja ao alcance de seus usuários e destinatários;
- possa ser acessada no momento em que for;
- necessário utilizá-la.

Para proteger a disponibilidade da informação, é necessário conhecer seus usuários, e criar regras para o uso da informação. A informação deverá ser classificada conforme o seu valor para a organização.

Para proteger a disponibilidade, muitas medidas são levadas em consideração. Entre elas, destacamos:

- configuração segura de um ambiente em que todos os elementos que fazem parte da cadeia de comunicação estejam dispostos de forma adequada para assegurar o êxito da leitura, do trânsito e do armazenamento da informação.

- cópias de segurança – backup. Isso permite que as mesmas estejam duplicadas em outro local para uso caso não seja possível recuperá-las a partir de sua base original

Para aumentar ainda mais a disponibilidade da informação, deve-se:

- Definir estratégias para situações de contingência.
- Estabelecer rotas alternativas para o trânsito da informação, para garantir seu acesso e a continuidade dos negócios, inclusive quando alguns dos recursos tecnológicos, ou humanos, não estejam em perfeitas condições de funcionamento.

Tendo em vista que a disponibilidade é o mais importante dos princípios da SI, a mesma deve servir o usuário final.

Cada informação dentro da empresa possui a necessidade de estar disponível para uma pessoa ou equipe, ao mesmo tempo em que há a necessidade de um controle que garanta que ela estará realmente disponível para os usuários legítimos.

Uma vez que garantimos que a informação está disponível somente para os usuários corretos, é necessário garantir que eles façam o uso adequado dessas informações. Para alcançar este objetivo é necessário que um processo eficiente de classificação da informação seja estabelecido.

A classificação deve levar em conta estas premissas e principalmente o impacto nos negócios pela quebra na disponibilidade, integridade ou confidencialidade das mesmas.

2.4 Ativos de Informação

O ponto inicial para a gestão dos ativos é a identificação do que é um ativo e quais são eles dentro da organização.

Ativo é qualquer coisa que tenha valor para um indivíduo ou uma organização, tais como, hardware de computadores, equipamentos de rede, edificações, software, habilidade de produzir um produto ou fornecer um serviço, pessoas, imagem da organização, etc...

Conforme Martins (2003), ativos são objetos físicos (hardware, prédios e outros) e lógicos (e-mail, softwares, banco de dados, entre outros) que têm algum valor para o processo de negócio da organização. Esses ativos são assistidos pelos seus proprietários, sendo os responsáveis por apontar as pessoas que terão acessos aos mesmos.

Existem vários tipos de ativos associados com sistemas de informação, sendo eles:

- Ativos de informação: base de dados de contratos e acordos, documentação de sistema e infra-estrutura, manuais, material de treinamento, procedimentos de suporte e operação, planos de continuidade de negócio, etc...;
- Ativos de softwares: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- Ativos físicos: equipamentos computacionais, de comunicação, mídias

removíveis;

- Serviços: computação, comunicações, refrigeração, iluminação, eletricidade;
- Pessoas e suas qualificações, habilidades e experiências;
- Ativos intangíveis: reputação, credibilidade e imagem da organização.

Para que os ativos sejam protegidos, é necessário que possua um proprietário. O proprietário pode ser uma pessoa ou entidade autorizada à controlar o uso e a segurança dos ativos, tornando-se o responsável pelos mesmos.

Tendo em vista que o objetivo da SI é salvaguardar os ativos citados, salienta-se que para o desenvolvimento deste trabalho foram detalhados os ativos de informação.

Nos dias atuais, a informação é considerada um bem de capital equivalente aos recursos de produção e financeiros, sendo o mais importante a mudança no significado que a informação assume na nova realidade mundial globalizada: informação enquanto recurso diferencial competitivo e lucrativo no mercado (MORESI, 2000).

Conforme a NBR ISO/ IEC 27002, informação enquanto ativo é todo elemento que compõe os processos que manipulam a informação, a contar a própria informação, o meio que ela é armazenada, os equipamentos em que é manuseada, transportada e descartada. O termo é oriundo da área financeira, por ser considerado um elemento de valor para um indivíduo ou organização, e que, por esse motivo, necessita de proteção adequada.

Segundo Beal (2005, p.15), ativo de informação tem um valor para o negócio e precisa ser protegida independente de seu suporte:

> Ativo de informação é constituído pelos dados ou informações que tenha um valor para o negócio, assim ativo de informação são informação relevantes e mantidas na mente dos tomadores de decisão, em base de dados, arquivos de computadores, documentos e planos registrados em papel.

Tradicionalmente, as empresas dedicam grande atenção à proteção de seus ativos físicos e financeiros, segundo (CARUSO, STEFFEN, 1999, p.22) pouca ou até mesmo nenhuma atenção aos ativos de informação que possuem. De acordo com o autor da mesma forma que seus ativos tangíveis, as informações envolvem os três fatores de produção tradicionais: capital, mão-de-obra e processo.

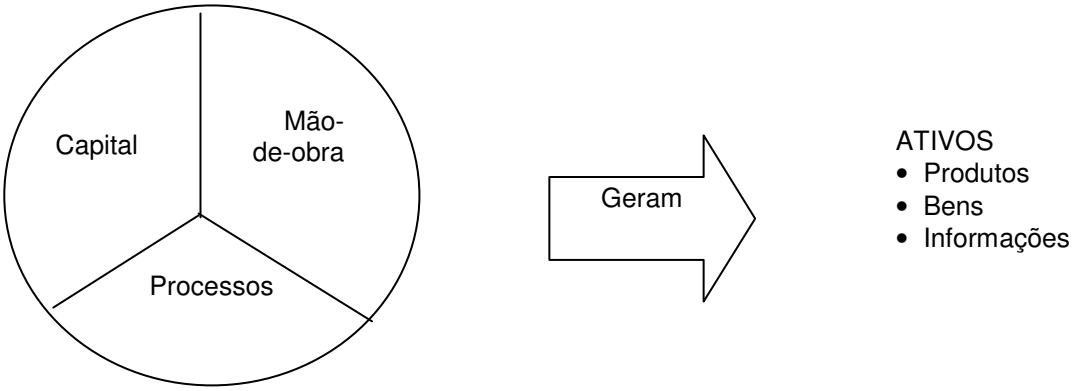


Figura 4 – Fatores econômicos de produção

Fonte: Caruso e Steffen (1999, p.23)

Mesmo que as informações não sejam passíveis do mesmo tratamento fisco-contábil que os outros ativos do ponto de vista do negócio elas são um ativo da empresa e, portanto, devem ser protegidas. Isso vale tanto para as informações como para seus meios de suporte, para todo o ambiente de informações (CARUSO, STEFFEN, 1999, p.23).

Dessa forma, a informação é um ativo que, como qualquer outro é importante e tem um valor para a organização, por conseqüência, necessita ser adequadamente protegida (NBR ISO/ IEC 27002).

Beal (2005) destaca que a informação representa uma classe particular entre os ativos da organização, sendo a sua administração sujeita a desafios específicos. Ao analisar as informações quanto ativos organizacionais relacionam as características que definem o comportamento da informação como um bem econômico, quais sejam:

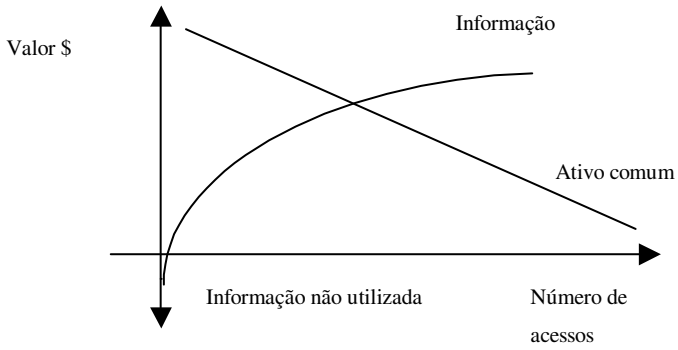


Figura 5 – A informação é (infinitamente) compartilhável.

Fonte: Beal (2005, p.15)

A informação pode ser compartilhada infinitamente e usada simultaneamente por inúmeras pessoas, sem que seja consumida nesse processo ao contrário dos ativos comuns.

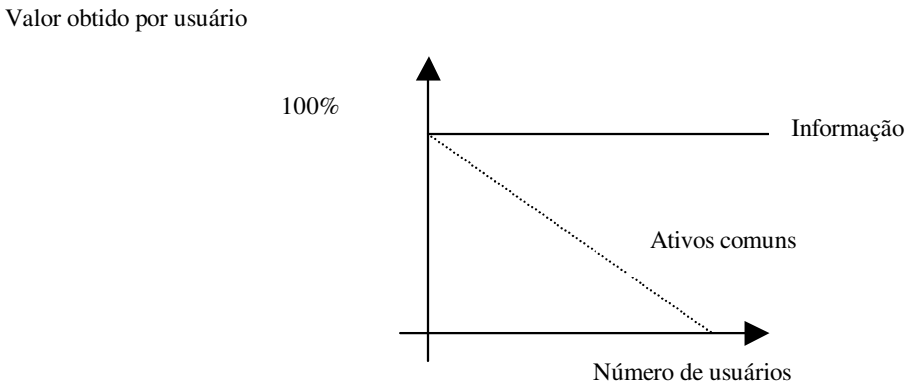


Figura 6 – O valor da informação aumenta com o uso.

Fonte: Beal (2005, p.15)

Quanto mais utilizada, maior o valor a ela associado, diferente dos ativos comuns que perdem valor à medida que são utilizados (pela depreciação).

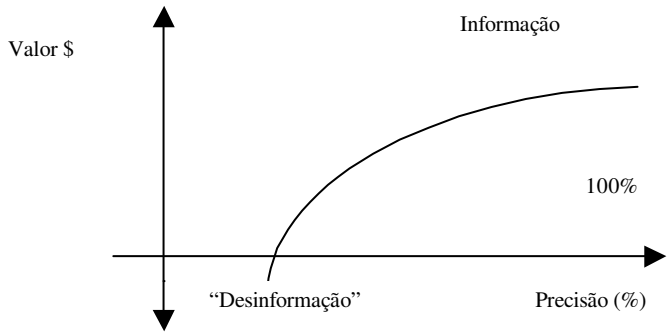


Figura 7 – O valor da informação aumenta com a precisão.

Fonte: Beal (2005, p.15)

Quanto mais precisa for a informação, mais útil se torna e portanto mais valiosa. Informações inexatas podem causar prejuízos, provocando erros operacionais e decisões equivocadas.

Nesse processo, o significado atribuído à qualidade da informação pode ser aplicado em situações distintas. No que se refere ao uso a informação adquire valor potencial na medida em todos os membros da organização são conhecedores de sua existência, onde se encontra e dispõem de recursos informacionais para acessá-la e adaptá-la à medida de suas necessidades (BEAL, 2005).

Observa-se quanto é essencial para os administradores fazerem uso de informações previamente tratadas e utilizarem. Para fazer uso do acúmulo de informações é preciso estabelecer um sistema para organizá-las e aplicá-las na tomada de decisões.

Reconhecendo a informação como um dos principais patrimônios de organização, esta deve ser protegida. A SI é um elemento chave dentro deste conceito e não deve ser vista apenas como guarda de informação, e sim como um conjunto de processos e controles para obter sucesso no SGSI devendo ter política com regras claras, levando em consideração a cultura e o ambiente tecnológico da empresa.

2.5 Classificação e controle de ativos de informações

A classificação dada a informação é uma maneira de determinar como esta informação vai ser tratada e protegida e requer a categorização das informações conforme seu grau de criticidade, independente do seu suporte físico ou lógico.

Apresentamos no item anterior que os ativos são elementos que a segurança busca proteger e possuem valor para a organização como conseqüências precisam receber uma proteção adequada para que os negócios não sejam prejudicados.

Estaremos abordando a classificação dos ativos de informação, documento, relatórios, livros, manuais, correspondências, patentes, informações de mercado, plano de negócios, arquivos de configurações etc., independente do tipo do meio em que esteja armazenada.

As informações devem ser classificadas durante sua produção. Não há regras preconcebida para estabelecer a classificação, mais é preciso entender o perfil do negócio e as características das informações que alimentam os processos e circula no ambiente organizacional.

Segundo da descrição da NBR ISO/ IEC 27002 do item que trata da SI:

> O objetivo da Classificação da informação é assegurar que os ativos da informação recebam um nível adequado de proteção. A informação deve ser classificada para indicar a importância, a prioridade e o nível de proteção. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Um sistema de classificação deve ser usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento. (NBR ISO/ IEC 27002, p.9).

De acordo com os requisitos de segurança a classificação da informação possibilita que haja uma diferenciação nos recursos utilizados para a manutenção desses ativos.

A classificação da informação é uma ferramenta essencial para uma boa administração dos recursos informacionais. Devendo estar relacionada com a SI e com as políticas pré-estabelecidas pela organização.

Na literatura da área de SI trazem algumas recomendações para a classificação da informação que é uma das etapas mais importantes para implantação do SGSI sendo assim na NBR ISO/ IEC 27002 apresenta no item 5 recomendação para classificação dos ativos informacionais como:

- Identificar quem são o proprietário da informação;
- Especificar os critérios a serem utilizados para a classificação;
- Categorizar a informação;
- Indicar o nível de segurança necessário para proteger;
- Documentar as exceções;
- Criar rótulos para informação impressa e digital;
- Definir método para a transferência da custódia da informação;
- Treinar e conscientizar usuários.

Esta classificação deve garantir que o nível de privilégio seja aplicado, ou seja, cada usuário somente terá acesso ao que realmente necessita e as permissões conferidas a este serão somente necessárias para execução de sua tarefa relacionada aquela informação. Os proprietários dos ativos são os responsáveis por atribuir as permissões de acesso aos ativos revisá-las periodicamente para assegurar-se que o controle mais apropriado aplicado a informação.

Outra classificação dos ativos é quanto sua integridade as necessidades podem ter vários níveis: baixo, médio, alto, crítico etc. de acordo com a necessidade da organização.

Pela ótica da disponibilidade, a classificação da informação acontece de acordo com a extensão do impacto que sua falta ocasionará, não temos categorias pré-definidas, mas podemos classificar por intervalo de tempo. Esses critérios podem definir também o tempo de retenção de uma determinada informação muitas vezes estabelecido por clausulas legais.

Conforme (CARUSO, STEFFEN, 1999, p.78) apresenta a classificação de informação quanto à necessidade de evitar a destruição:

- Vital – é a informação essencial podem ser consideradas secretas ou confidenciais;
- Criticas – é a informação crucial para execução dos objetivos organizacionais;
- Valiosa – é a informação de valor reconhecido para segmentos ou indivíduos da organização.

A classificação da informação deve ser estabelecida através de um documento formal. A política deve ser personalizada conforme a necessidade de cada departamento ser elaborada e alinhada com o plano de negócio devendo-se tornar de conhecimento de todos os usuários.

2.6 Política de segurança de informação

Escrever uma política de SI envolve comprometimento de diversas áreas de interesse e deve ser abraçada por todos, desde a direção da organização até cada um dos funcionários, clientes e fornecedores com acesso ao sistema de informação, ou que possam de alguma forma comprometer o ativo protegido. O documento de política de SI deve ser elaborado de forma a servir como uma regra a ser seguida, deve ser também de fácil leitura e compreensão e exigirá atualizações que reflitam as necessidades do negócio e a realidade da organização.

A política da informação existente na organização vai influenciar as características dos sistemas de informação utilizados pelos gerentes e deve estar de acordo com a estratégia geral da organização. Deve haver um sincronismo entre o planejamento estratégico da organização e sua política de informação. A organização, e principalmente os responsáveis pelas suas decisões estratégicas, devem pensar na informação como um dos seus patrimônios.

Segundo a norma ISO/IEC2702:2006 objetivo da política é prover à direção uma orientação e apoio a SI. Convém que a direção estabeleça uma política clara e demonstre apoio e comprometimento com a SI através da emissão e manutenção de uma política de SI para toda organização.

Na vida das pessoas e das organizações, tudo gira em tornos de decições politicas, não importando quem tome essas decições. Toda organização sempre estabelece regulamentos, normas a serem cumpridos por todos quanto se relaciona com ela.

Conforme (CARUSO, STEFFEN, 1999, p.49) —política de segurança é um conjunto de diretrizes gerais destinadas a governar a proteção a ser dada a ativos da organização. Deve prover a orientação e apoio da direção para a SI de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Ainda segundo o autor a aplicação de uma política bem definida e equivalente aos objetivos da organização pode ser resumida em três aspectos:

- redução da probabilidade de ocorrência;

- redução dos danos provocados por eventuais ocorrência;
- criação de procedimentos para se recuperação de eventuais danos.

> Para que a empresa possua uma politica de segurança com qualidade não se pode esquecer da segurança física e do ambiente, que nada mais é do que a prevenção de acesso não autorizado, dano e interferência às informações e instalações físicas da organização. Para tanto é necessário que haja um local apropriado.(MENEZES, 2006, p. 64)

As medidas de segurança é uma forma de previnir os eventuais ricos, além disso, a prevenção costuma ser mais barata que a restauração dos danos provocados por falta de segurança. É necessário que as estruturas organizacionais conhecem os limites das atribuições e responsabilidades dentro de suas áreas de atuação e os ricos envolvidos, mesmo quando não existem normas a respeito da segurança.

> Segundo CARUSO; STEFFEN(1999) a política de segurança não constitui exceção, de modo que é preciso seguir as mesmas etapas que seriam seguidas em qualquer outra atividade dentro de uma empresa. Segurança também implica uso de capital, mão-de-obra e recursos, isto é, representa investimento e despesas para a empresa.

A política de segurança deve conter diretrizes claras a respeitos, pelo menos, dos seguintes aspectos:

- Objetivos de segurança - deve explicar de forma rápida e sucinta a finalidade da política de segurança.
- A quem se destina – deve definir claramente quais as estruturas organizacionais às quas as mesmas se aplica.
- Propriedade dos recursos – deve definir de forma clara a regras que regerão os diversos aspectos relacionados com a propriedade de ativos de informações.
- Responsabilidade – deve definir de forma clara qual o tipo de responsabilidades envolvidas com o manuseio de ativos de informações.

- Requisitos de acesso – deve indicar de forma clara quais os requisitos a serem atendidos para o acesso a ativos de informações.
- Responsabilização – deve indicar as medidas a serem tomadas nos casos de infrigência às normas da mesma.
- Generalidades – nesta seção da política podem ser incluidos os aspectos que não cabem nas demais. Pode-se incluir aqui uma definição dos conceitos envolvidos, um glossário e uma indicação das normas acessórias.
- As políticas de segurança devem ter implementação realista, definindo claramente as áreas de responsabilidade de seus utilizadores. Devendo também adaptar-se a alterações na organização, e conhecendo ameaças/fraquezas que a empresa esta exposta.

Segundo Fontes (2000), existem algumas caracteristicas que toda política deve conter para ser entendida por todos os funcionários até o presidente:

- informação como um bem da empresa;
- controle de acesso à informação;
- definição do gestor da informação;
- responsabilidades do usuário, da gerência e do gestor da informação;
- preparação para situações de contigencia, garantindo a continuidade da excução de negocio;
- definição do uso profissional da informação da empresa;
- definição da possibilidade, ou não, da empresa acessar arquivos pessoais do usuário;
- definição da identificação do usuário como pessoal e única, bem como a responsabilidade do sigilo da senha;
- concientização dos usuários;

- medidas disciplinares que serão utilizadas caso a política não seja cumprida.

Para que a política da segurança obtenha sucesso é necessário concientização de todos os usuários da organização. Para tanto é necessário que a empresa se empenhe em divulgar e esclarecer através de campanhas a política de segurança da empresa.

Na elaboração da política de SI deve haver uma área responsável, que se incumbirá de sua criação, implantação, revisão, atualização e designação de funções. Nessa área deve ser escolhido um gestor responsável pela análise e manutenção da política. Para garantir a aplicação eficaz da política, o ideal é que o alto escalão, como diretoria, gerentes e supervisores façam parte dessa área, além de usuários, desenvolvedores, auditores, especialistas em questões legais, recursos humanos, TI e gestão de riscos.

3 SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Aspectos relativos a implantação SGSI eficiente em uma organização vem evoluindo significativamente ao longo dos anos. O procedimento de SI tem alterado bastante desde inicio quando a segurança física junto com um conjunto de back-up compunha então, todos os controles de SI implantado na organização.

Conforme a NBR ISO/ IEC 27001 SGSI é um sistema global, baseado na ISO/ IEC 27002: a adoção de um modelo deve ser uma decisão estratégica para organização no contexto de suas necessidades, objetivos e requisitos de segurança e tamanho da instituição.

O SGSI é uma série de ações tomadas com objetivo na gerenciar a segurança da informação, incluindo pessoas, infra-estrutura, e negócios, reduzindo os riscos a um nível aceitável, enquanto mantêm em expectativa os objetivos do negócio e as expectativas do cliente.

O processo de implantação de um SGSI é semelhante a um processo de qualidade ISO 9001, no qual se aplicam os princípios do PDCA:

- planejar; fazer, checar, agir

Para prover um modelo de gestão dentro de uma perspectiva estratégica, é necessário alinhar todas essas atividades para identificar e gerenciar e para funcionar efetivamente, identificando as atividades como processos que interagem para sustentação a organização.

Seguindo a norma para implementação do SGSI chegamos ao seguinte escopo:

1. SGSI (NBR ISO/ IEC 27001): esse passo é conduzindo na seguinte seqüência:
    a. seleção do modelo através do qual o SGSI irá atuar (tipo de norma: NBR ISO/ IEC 27001, NBR ISO/ IEC 27002 etc...);
    b. planejamento inicial das fases do projeto;

   c. levantamento dos ativos envolvidos (equipamentos, infra-estrutura, sistemas, pessoas e serviços):
2. avaliação dos riscos: identificar e avaliar ameaças e vulnerabilidades. Para cada ameaça deve ser atribuído um nível de risco:
3. tratamento dos riscos: é o gerenciamento dos riscos, envolvendo as atividades que tentarão impedir um ataque antes que ele ocorra ou reduzirão o efeitos da ameaça;
4. definição de controles: a necessidade de controles é um resultado da avaliação de riscos. Sua escolha é feita com base na relação custo-benefício de sua implantação. Os controles podem ser baseados em software, hardware, pessoas ou processos;
5. implementação: implantação em si das contramedidas de segurança;
6. auditoria: verificação se as condições estabelecidas nos passos anteriores ocorrem de maneira satisfatória;
7. melhoria contínua: aprimoramento contínuo do SGSI através da busca assertivas que dêem mais valor às atividades de segurança da informação.

A partir do estabelecimento de mecanismos de controle que enfatizem essa característica no processo de aquisição, desenvolvimento e manutenção dos sistemas de informação é necessário garantir a segurança como parte integrante dos sistemas de informação, desde o primeiro momento do projeto.

O SGSI serve para proteger os recursos da empresa e tem a finalidade de diminuir o nível de exposição aos riscos existentes em todos ambientes, gerando assim liberdade necessária para criação de novas oportunidades de negócio. Para Moreira (2001), os negócios atualmente estão cada vez mais dependentes das tecnologias e estas por sua vez têm que transmitir confiabilidade nas suas transações, o usuário deve acreditar que as informações emitidas para a organização vai ser administrada e salvaguardadas.

Segundo Fontes (2008 p.36) constituir um SGSI é necessário contemplar alguns requisitos como:

- Nomear uma pessoa responsável pelo processo, essa pessoa não é responsável pela segurança em sim pelo processo de SI.

- Recursos financeiros : Recursos financeiros de tempo e operacionais para existencia do processo de segurança e da sua gestão.
- Envolvimento da alta direção:A descisão de existir um SGSI deve ser da alta adminstração da organização. Este processo interfere em muitos aspectos da organização e principalmente interfere em pessoas, na cultura e no poder que as pessoas possuam dentro daorganização.

O SGSI pode e deve ser um processo sustentável. Isto é, podemos ter um processo de proteção de informação que ele proprio gere mais condições para continuidade de vida do proprio processo.

Um processo de planejamento de SGSI pode variar de uma organização para outra devida os diferentes estilos, tamanhos e estrutura o processo deve se adequar ao ambiente em que será usado.

Para obter sucesso na implementação de SGSI é importante conhecer o plano de segurança da empresa para que sua execução seja bem sucedida.

3.1 Administração do Ambiente de Segurança

Para iniciar o processo de administração do ambiente de segurança é imprescindível que as políticas de SI já tenham sido desenvolvidas e implantadas e que todos os usuários da organização estejam conscientizados das mesmas.

A administração do ambiente seguro envolve todo um ciclo do macro atividades.

- 1 Análise de riscos
- 2 Política de segurança
- 3 implementação de segurança
- 4 monitoramento e Feedback

A primeira fase do ciclo é análise de risco, onde se conhecem o ambiente e quais as vulnerabilidades responsáveis pelos maiores riscos.

A segunda conhecer os pontos básicos que devem ser contemplados no plano de segurança da empresa para estruturar e implantar corretamente tal documento dentro da empresa.

Depois de se familiarizar comas ameaças e vulnerabilidades do ambiente, identificados na análise de riscos ou depois da definição formal das intenções e atitudes da organização que estão definidas na política de segurança da informação devemos tomar algumas medidas para implementação das ações de segurança recomendadas e estabelecidas.

Devemos lembrar que as ameaças são agentes capazes de explorar falhas de segurança que denominamos vulnerabilidades e como conseqüência, causam perdas ou danos aos ativos de uma empresa e afetam seus negócios

Não basta conhecer as fragilidades do ambiente ou ter uma boa política de segurança por escrito. Deve instalar ferramentas, divulgar regras, conscientizar os usuários sobre o valor das informações e, configurar os ambientes e implementar cada medida de proteção para contribuir com a redução das vulnerabilidades e, consequentemente, do risco.

Para acontecer a administração da segurança, a organização deverá reconhecer o SGSI como um processo, onde as pessoas responsáveis respondam diretamente a alta administração. Isso é necessário para que a área se torne menos suscetível a pressões e para que ela possa ser incorporada facilmente pela cultura organizacional.

Administração do ambiente de segurança. Inclui:

- Estabelecimento de um processo de gestão de incidentes de segurança;
- Implementação de um sistema de medição, que colha dados para a avaliação de desempenho da gestão de segurança;
- Obtenção de sugestões de melhorias;
- Implementação de melhorias levantadas no processo.

A administração de um ambiente seguro envolve todos os processos e deve ser vista como parte integrante das estratégias de negocio. A aquisição ou desenvolvimento de sistemas leva em conta os princípios de segurança a serem

atendidos desde a etapa de planejamento e investimento em segurança, baseados em análise bem fundamentada de risco, custo e grau de proteção adicional.

3.2 Análise crítica do sistema de gestão de segurança da informação

Analise é o levantamento periódico dos riscos de segurança da informação, identificando as ameaças e vulnerabilidades. Os resultados desse passo irão direcionar a determinação das ações gerenciais que nortearão todo o processo de SI.

Segundo a NBR ISO/ IEC 27001 o item 7 apresenta como estabelecer as análises crítica pela direção:

A direção deverá analisar o SGSI a intervalos planejados (pelo menos uma vez por ano para assegurar a sua continua pertinência adequação e eficácia. Essa análise deve incluir a avaliação de oportunidades de melhoria e a necessidade de mudanças do SGSI, incluindo a política de segurança de informação e objetivos de SI.

Existem alguns princípios para obter a entrada da análise crítica:

- a) resultados de auditorias do SGSI e análises críticas;
- b) realimentação das partes interessadas;
- c) técnica produtos e procedimentos para melhorar o desempenho do SGSI;
- d) situação das ações preventivas e corretivas;e) vulnerabilidades ou ameaças não contempladas na análises e avaliações de riscos;
- f) resultados da eficácia das medições;
- g) acompanhamento de análise criticas anteriores pela direção;
- h) mudanças que possam afetar o SGSI;
- i) recomendações para melhoria;

Saídas da análise crítica descrito no item 7.3:

- Análise/avaliação de riscos para a organização.
- Legislação vigente a que a organização, seus parceiros comerciais e provedores de serviço devem atender.
- Princípios, objetivos e requisitos do negócio.

Segundo a NBR ISO/ IEC 27002 p2. requisitos de segurança são identificados através de uma avaliação sistemática dos riscos de segurança.

Os gastos com os controles necessitam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança. As técnicas de avaliação de risco podem ser aplicadas em toda a organização ou apenas em parte dela, assim como um sistema de informação individual, componentes de um sistema específico ou serviços, quando for viável, pratico e útil.

3.3 Seleção de controles

Com os riscos identificados e com as medidas de tratamento desses riscos já providenciadas é necessário implementar controles que assegurarão a redução dos riscos a níveis aceitáveis. A seleção de controles pode ser feita a partir dessa norma ou de outra que atenda as necessidades da organização. Esses controles incluem:

- Proteção de dados e privacidade de informações pessoais;
- Proteção dos registros organizacionais;
- Direitos de propriedade intelectual;
- Documento de política de segurança da informação;
- Atribuição de responsabilidades;

- Treinamento e educação em segurança da informação;
- Processamento correto nas aplicações a fim de prevenir erros, perdas, modificação não autorizada ou mal uso de informações em aplicações;
- Gestão de vulnerabilidades técnicas;
- Gestão de continuidade de negócios;
- Gestão de incidentes de segurança e melhorias.

Segundo a norma NBR ISO/ IEC 27002 p.3 um número de controles pode ser considerado como princípios básicos, fornecendo um bom ponto de partida para a implementação da SGSI. São baseados tanto em requisitos legais como nas melhores práticas normalmente usadas.

Uma organização pode considerar que objetivos de controle e controles adicionais são necessários, tendo como base que o SGSI tem seus controles específicos a norma recomenda um guia de implementação de controles especificados das seções 5 a 15.

Esses elementos de controle priorizam a aderência aos requisitos de segurança estabelecidos pela política de segurança da organização, tornando-os parte do processo de análise e especificação. Desse modo, os requisitos para controles de segurança nas especificações de requisitos de negócios devem ser estabelecidos e especificados, em consonância com a política de segurança, quer seja para novos sistemas de informação a serem adquiridos, desenvolvidos, ou para a realização de manutenção ou implementação de melhorias em sistemas já existentes.

É importante que esse elemento de controle esteja plenamente integrado aos processos de desenvolvimento interno ou externo, de forma que não apresente complexidade em sua operacionalização e não comprometa os prazos, custos e objetivos dos sistemas de informação, pois, de outro modo, certamente será deixado em segundo plano em caso de necessidade.

4 GESTÃO DA INFORMAÇÃO

A atividade de ‘gestão’ é um conjunto de processos que englobam atividades de planejamento, organização, direção, distribuição e controle de recursos de qualquer natureza, a vista da racionalização e efetividade de determinado sistema, produto ou serviço. (MANUAL..., 1997 apud MARCHIORI, 2002, p.74).

Compreender a GI no contexto das organizações, enquanto processos, ações e atividades de produção, organização, distribuição e uso da informação, pressupõe primeiramente apresentar um breve enunciado sobre o surgimento de seu conceito na literatura científica.

Para Davenport (2000), a GI consiste em um conjunto estruturado de atividades que incluem o modo como as empresas obtêm, distribuem e usam a informação. Choo (2003) afirma que a informação desempenha um papel estratégico no crescimento e na capacidade organizacional, existindo três arenas distintas para sua criação e uso: a organização usa a informação para dar sentido às mudanças do ambiente externo para sua criação e uso: em primeiro, a organização utiliza a informação para entender as mudanças no ambiente externo e se adaptar de forma mais rápida; em segundo, a organização cria, organiza e processa a informação de modo a gerar novos conhecimentos por meio do aprendizado, o que faz com que a mesma desenvolva suas capacidades, crie novos produtos e serviços, aperfeiçoe os já existentes e melhore os processos organizacionais. Por último, as organizações buscam e avaliam informações para tomar decisões importantes, identificando alternativas plausíveis, prováveis resultados e avaliar o impacto desses para a organização.

Place e Hyslop (1982) apud Bouthillier; Shearer (2002) afirmam que a GI focaliza o planejamento e atividades que precisam ser executadas para controlar os registros da organização, podendo ser entendida como responsável por gerenciar o fluxo informacional e o conhecimento que está registrado, ou seja, as informações presentes no ambiente organizacional são ordenadas de forma a facilitar seu uso e assimilação, como estratégia de competitividade no mercado. As

nuanças entre GI, Gestão de Registros (GR) e Gestão de Recursos de Informação (GRI) são sutis, pois todos estes termos podem ser usados mutuamente.

Bergeron (1996) apud Frade et al. (2003) afirma que a GRI foi proposta por Robert Taylor, na década de sessenta do século XX. Para o autor, duas visões emergem na literatura: a perspectiva tecnológica e a perspectiva integrativa. A primeira prevê as seguintes atividades:

- Planejamento de dados, de capacidade e de aplicação;
- Planejamento e desenvolvimento de sistemas de informação;
- Gerenciamento de projetos;
- Aquisição de hardware e software;
- Integração sistema-tecnologia e administração de dados.

As ações previstas pela segunda são:

- Reconhecimento da informação como recurso;
- Gerenciamento do ciclo de vida da informação;
- Informação como apoio dos objetivos organizacionais;
- Existência de um 'agente vinculador' que atue como intermediário de valor entre necessidades e fontes de informação.

A GI em ambientes organizacionais é definida por Valentim (2008, p.2) como um conjunto de atividades que visa a obtenção de um diagnóstico das necessidades de informação, mapeamento de fluxos formais de informação nos vários setores da organização, prospecção, coleta, filtro, monitoramento, disseminação de informações de diferentes naturezas, e elaboração de serviços e produtos informacionais, com o objetivo de apoiar o desenvolvimento das atividades e tarefas cotidianas e o processo decisório nesse ambiente.

A autora complementa que a GI lida com "fluxos formais" e tem como objeto o "conhecimento explícito", alcançando as atividades de base descritas abaixo (VALENTIM, 2008, p.3-4):

- Identificar necessidades/demandas de informação;
- Mapear e reconhecer fluxos formais;
- Desenvolver a cultura organizacional positiva em relação ao compartilhamento/socialização de informação;

- Proporcionar a comunicação informacional de forma eficiente, utilizando tecnologias de informação e comunicação;
- Prospectar e monitorar informações;
- Tratar analisar, organizar, armazenar e agregar valor às informações, utilizando tecnologias de informação e comunicação;
- Desenvolver e implantar sistemas informacionais de diferentes naturezas, visando o compartilhamento e o uso de informação;
- Elaborar produtos e serviços informacionais;
- Elaborar e implantar normatizações visando à sistematização da informação internamente e externamente;
- Retroalimentar o ciclo.

Pinheiro (2008, p.42) afirma que o "processo de gestão da informação está associado aos princípios fundamentais da gestão organizacional". Nesse mesmo sentido, Calazans (2006, p.65) afirma que o "o uso da informação nas organizações acompanhou a evolução das organizações", isto é, a informação é a força motriz das atividades de uma organização, compreendida hoje, enquanto um ativo primordial para garantir a estratégia e a competitividade mercadológica.

Observa-se que, para compreender a GI no contexto das práticas informacionais de uma empresa, é imprescindível o estabelecimento de interfaces teóricas e práticas com as disciplinas da Administração, CI e TI.

Nesse sentido, verifica-se na literatura, com para Marchiori (2002, p.74), que a relação entre essas disciplinas resulta em um conjunto de habilidades e conhecimentos teóricos e práticos que possibilitam a estruturação dos sistemas de informação, assim como o oferecimento de serviços, produtos e atividades de informação, conforme demonstra o quadro abaixo:

Administração	Tecnologia da Informação	Ciência da Informação
A GI está voltada à incrementação da competitividade empresarial e dos processos de modernização da organização bem como a capacitação dos profissionais para o gerenciamento de tecnologias da informação.	Está voltada para a dinamização das atividades por meio da utilização de diferentes arquiteturas de hardware e software, e redes de (tele) comunicações de acordo com as necessidades identificadas.	Está voltada à teoria e à prática que envolve sua criação, identificação, coleta, validação, representação, recuperação e uso.

Fonte: Marchiori (2002, p.74)

Quadro 1 – Enfoques da Administração, TI e CI

Pondera-se que a função da GI é identificar e potencializar recursos informacionais, salientando-se a necessidade do compartilhamento da informação. Marchiori (2002, p.74) destaca ainda que a abrangência da GI, sob a área de CI "corresponde ao núcleo da gestão propriamente dita [...] [pois enfoca] a gestão integral dos recursos de informação das organizações".

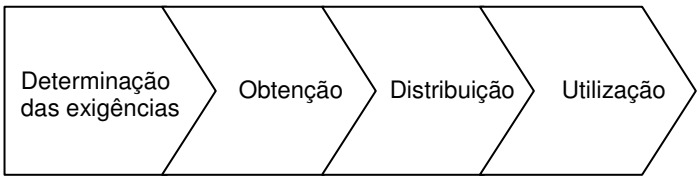
Davenport (2000, p.44), ao desenvolver o princípio de "ecologia da informação", aponta quatro atributos para contribuir no processo de gestão da informação, cada qual valioso à sua maneira:

1. integração dos diversos tipos de informação: envolve a integração de uma diversidade informacional: computadorizada e não computadorizada, estruturada e não estruturada, via texto, áudio e vídeo. A área fornecedora de informação na empresa, ao invés de direcionar o usuário a um tipo particular de informação, deve combinar todas as mídias disponíveis.
2. reconhecimento de mudanças evolutivas: a evolução é um fato da vida organizacional, e isso deve ser um senso comum entre os administradores. A gestão informacional precisa abrir espaço para a transformação.
3. ênfase na observação e na descrição: é necessário que as informações sejam correta e completamente descritas na tratamento do gerenciamento da

informação. Isso significa criar uma compreensão profunda dos processos existentes, possibilitando a projeção de novos.

4. ênfase no comportamento pessoal e informacional: os usuários da informação devem ser observados, a fim de não somente se ofereça a informação, mas também se facilite o uso. Toda ação ou iniciativa gerencial, com foco em informação, deve fazer progredir o comportamento informacional dos usuários.

Além disso, Davenport (2000, p.173) descreve a GI como um processo genérico em quatro passos, conforme a figura a seguir:



Fonte: DAVENPORT, 2000, p.175.

Figura 8 – O processo de gerenciamento da informação.

1. Determinação de exigências: esta fase envolve identificar como os gerentes e os funcionários percebem seus ambientes informacionais, entender desde o princípio as tarefas administrativas, observando-as *in loco,* e conseqüentemente, suas necessidades de informação, destacando-se as ações de estudos conforme a demanda de informações corporativas, buscando conectar e (re)adequar os conteúdos informacionais e as necessidades específicas demandadas pelos usuários da informação;
2. Obtenção de informações: definidas as exigências de informações, é necessário obtê-las, sendo esta uma atividade ininterrupta, sem poder ser finalizada. Esse passo consiste em várias atividades: exploração do ambiente informacional, classificação da informação em uma estrutura pertinente, formatação e estruturação das informações.
3. Distribuição: envolve a ligação de gerentes e funcionários com as informações que necessitam, e estando a informação organizada e havendo uma necessidade

específica, a distribuição é mais efetiva. Esta pode ser feita utilizando qualquer meio ou suporte informacional, dependendo a sua inevitabilidade.

4. Uso da informação: este é a etapa final de todo o processo de gerenciamento informacional. O uso da informação é algo extremamente pessoal, porém pode ser medido através de uma avaliação de desempenho. Já que houve necessidade de informação, a empresa pode questionar ao usuário o uso que se fez dela. Outra maneira é tornar em estatística o uso do material informacional.

Neste sentido, pode-se compreender que a GI tem como objetivos: apoiar a política da empresa, na medida em que torna mais eficiente o conhecimento e a articulação entre vários subsistemas que a constituem, apoiar os gestores na tomada de decisões e, tornar mais eficaz o conhecimento do meio envolvente.

Wilson (1989) pondera que a GI é a gestão eficaz de todos os recursos de informação relevantes para a organização, tanto gerados internamente como os produzidos externamente, utilizando sempre que necessário a TI.

Sob esta perspectiva, a GI deve incluir em dimensões estratégicas e operacionais, os mecanismos de obtenção e utilização de recursos humanos, tecnológicos, financeiros, materiais e físicos. A partir disso, deve ser disponibilizada como ensino útil e estratégico para indivíduos, grupos e organizações (PONJUÁN DANTE, 1998).

Pode-se afirmar que o processo de GI tem como função, desenvolver e conectar estratégias, de acordo com o foco do negócio da organização, para orientar estrategicamente as ações de tecnologias da informação e sistemas de informação. Para atingir seus objetivos desenvolve ações de gestão e mapeamento de processos organizacionais, organização e tratamento da informação, recuperação, representação, armazenamento, políticas e procedimentos de produção, acesso, circulação e distribuição da informação.

Marchiori (2002, p.75-76) salienta que os estudos sobre GI podem incluir ações de:

- Planejamento: identificação das necessidades de informação e de níveis de agregação de valor às demandas realizadas; estudo do impacto da informação no desempenho da organização; o mapeamento e integração das unidades, pessoas e fluxos de informação na organização;

desenvolvimento e aplicação de metodologias para avaliação de fluxos, sistemas, produtos e serviços de informação, assim como a aplicação crítica e criteriosa de sistemas computacionais e redes de dados.

- Comunicação: teorias e modelos da comunicação e sua aplicação em estruturas organizacionais e em sistemas de informação; fluxos de informação, redes de valor agregado e interpessoais/intergrupais; comunicação de dados e interação humano-computador.
- Gerência da Informação e Sistemas de Controle: compreendendo o processo de tomada de decisão e o papel da GI; a localização, coleta e análise de dados; design, especificação e análise de sistemas; aplicação de tecnologia de computadores; gestão de documentos; utilização de informação para controle gerencial e análise de negócios; utilização de técnicas de *workflow* para a identificação de fluxos de informação e dados; sistemas especialistas.
- Gerência de Recursos Humanos: inclui a descrição, análise e avaliação de funções; recrutamento, seleção, treinamento; gerência de pessoal; motivação e relações interpessoais;
- Gerência de Recursos Financeiros: abrange contabilidade; análise e controle de custos; estratégias para suporte à decisão; programação, planejamento e estrutura orçamentária, incluindo estimativa de gastos; julgamento de desempenho (análise de custo-efetividade e de custo-benefício).
- Promoção, Vendas e Marketing: relaciona-se à publicidade e relações públicas aplicadas à produção de bens e serviços de informação; técnicas e estratégias de marketing, incluindo pesquisa de mercado.
- Contexto Político, Ético, Social e Legal.

Sob o ponto de vista da tecnologia são empreendidos estudos nos seguintes âmbitos:

- Sistemas Computacionais (*hardware* e *software*): os conteúdos, neste particular, envolvem os recursos de entrada, processamento, armazenagem e saída de dados; princípios de sistemas operacionais e

programas aplicativos; o estudo e aplicação de pacotes de *software* para o armazenamento e recuperação da informação, mais especificamente a estrutura de bases de dados relacionais, *lay-out* de registros e parâmetros de busca; gerenciamento de sistemas de bases de dados; estudos de aplicação; especificação, design; implementação, avaliação e documentação de sistemas voltados para a GI;

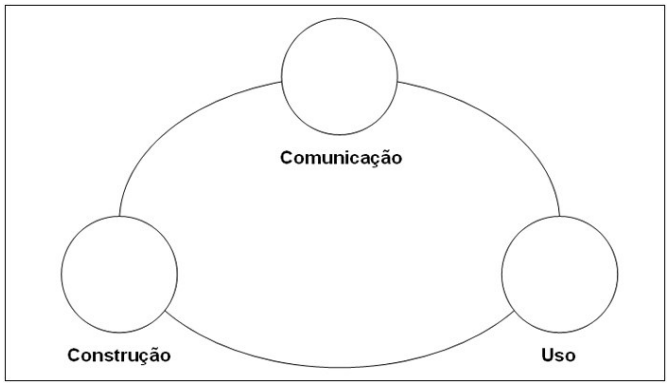
- Telecomunicações: domínio mínimo dos padrões, protocolos, interfaces; tipos de equipamento (modems, dispositivos eletrônicos e óticos de comunicação); redes de telecomunicação (incluindo *lans* e *wans*);
- Aplicações da Tecnologia da Informação: em especial para aquelas relacionadas à coleta, armazenagem e recuperação da informação, desde o vídeo-texto, telex, passando pelas tecnologias COM e COLD1 até o reconhecimento de voz, digitalização, tecnologias de discos compactos, telecomunicações, métodos de publicação eletrônica e de disseminação de documentos via redes, por exemplo;
- Meio ambiente: Princípios de ergonomia, proteção de dados, *copyright*, pirataria, criptografia.

A GI atua também em algumas áreas básicas, indicadas pela CI, a saber:

- Metodologia da pesquisa: devido à necessidade de se identificarem temas e propostas de pesquisa; os métodos de investigação, coleta de dados, amostragem, análises estatísticas, avaliação de resultados e produção de relatórios;
- Lingüística: os estudos com informação implicam conhecimentos básicos da linguagem natural e formal, das classificações lingüísticas, da semântica, sintática e pragmática, por exemplo;
- Línguas estrangeiras: como recursos para a análise de fontes de informação, comunicação em um mundo conectado, e de maneira a oferecer serviços de tradução e resumos.

Pode-se afirmar, dessa forma, que os aportes teórico-conceituais e metodológicos da GI e sua interface com as disciplinas de Administração, CI e TI

contribui consideravelmente às etapas de estudo e desenvolvimento do SGSI, pois coopera na diminuição de riscos e vulnerabilidades tanto procedimentais como metodológicos, visando assegurar a continuidade eficaz do ciclo social da informação: a produção, a comunicação e o uso.



Fonte: LE COADIC, 2004, p.10.

Figura 10. O ciclo da informação

Os três processos do ciclo da informação se sucedem e se alimentam reciprocamente. Qualquer atividade científica ou técnica podem gerar novos conhecimentos, porém as atividades e novos conhecimentos só surgem pela existência de informação, sendo que esta é continuamente produzida, e sem ela, não haveria novo conhecimento. Assim, construção refere-se à geração de conhecimentos que foram registrados, em forma escrita ou oral, impressa ou digital, de informações de qualquer natureza. A comunicação é um processo intermediário que permite a troca de informações entre as pessoas, ou seja, é um mecanismo que assegura o intercâmbio de informações de qualquer interesse e pode se dar de forma oral ou escrita, ou ser formal ou informal. O uso de informação significa trabalhar com a matéria informação para obter um efeito que satisfaça a uma necessidade de informação, ou seja, utilizar um produto de informação é empregar tal objeto para obter, igualmente, um efeito que satisfaça a uma necessidade de informação, no qual esse objeto subsista (utilização), modifique-se (uso) ou desapareça (consumo), transformando-se em qualquer caso, em novo conhecimento (LE COADIC, 2000, p.10-39).

5 CONTRIBUIÇÕES DA CIÊNCIA DA INFORMAÇÃO PARA O SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Este capítulo aborda o SGSI sob a visão da GI, na perspectiva da CI. Discorre-se sobre a CI no contexto social, informação e conhecimento, recuperação da informação e representação e organização do conhecimento.

5.1 Ciência da Informação no contexto social

Diante das alterações ocorridas nas sociedades contemporâneas decorrentes do desenvolvimento e amadurecimento do sistema capitalista desde o início da segunda guerra mundial, o fenômeno mais visível foi o surgimento da explosão informacional, reflexo do acúmulo produtivo da ciência e da tecnologia. Desde então o fenômeno da informação vem adquirindo vital importância em todos os segmentos na sociedade pós-moderna, tornando-se cada vez mais um recurso primordial para gerir as ações, atividades e relações do indivíduo na sociedade.

Aliados á esse fenômeno as revoluções tecnológicas contribuíram significativamente como instrumentos para difundir informações; ao permitirem o armazenamento e distribuição de grandes volumes informacionais em escala global através das tecnologias de informação e comunicação.

Decorrentes desses dentre outros fenômenos configurou-se em escala global o surgimento de uma nova base sócio-técnica pautadas na informação e no conhecimento apoiadas na difusão e uso das emergentes tecnologias de informação e comunicação.

Desse modo, os estudos da informação e seus fenômenos assumiram cada vez mais importância ao permitir melhor compreensão dos fenômenos sociais, econômicos, políticos e culturais da sociedade pós-moderna. Diante do enunciado acima a autoras Kobashi e Tálamo afirmam que

> o estudo da informação, de sua produção, circulação e consumo, assume importância primordial, sendo desenvolvido por várias áreas do conhecimento. assim, ao lado da importância da informação reconhece também a complexidade de abordá-la. Muitas são as disciplinas que a focam e, cada uma deve nela, identificar o seu objeto específico para que uma atividade compreensiva sobre o assunto substitua a explicação mecânica e funcionalista largamente difundida no campo [...].” (KOBASHI, TALÁMO, 2003 p. 8)

Diante das necessidades de estudos decorrentes dos fenômenos ocasionados pela informação, a ciência da informação inscreve-se como uma disciplina direcionada para solucionar os problemas concernentes as atividades de produção, tratamento, recuperação, circulação e uso da informação.

Não se trata de qualquer tipo de informação, ela direciona seu olhar para propor soluções para a informação registrada.

A ciência da informação no contexto da pós-modernidade adquire um compromisso social, já que sua missão é direcionar respostas teóricas, conceituais, instrumentais e metodológicas para resolver os problemas ocasionados pelos fenômenos da informação, decorrentes da explosão, dispersão e despersonalização informacional. Nesse sentido os autores WERSIG & NEVELLING (1975) afirmam que “atualmente, transmitir o conhecimento para aqueles que dele necessitam é uma responsabilidade social, e essa responsabilidade social parece ser o verdadeiro fundamento da Ciência da informação”.

No contexto da gestão da informação, a CI deve contribuir com aportes teóricos, conceituais e instrumentais para aprimorar os mecanismos de organização, representação, busca e recuperação da informação. Contribuirá em especial para otimizar a eficácia da comunicação entre a memória de conhecimentos armazenados pelos sistemas de informação e o usuário. De modo a contribuir socialmente para instigar a produção de novos conhecimentos, baseados na modelização social do ciclo da informação onde os “processos de construção, comunicação e uso se alimentam reciprocamente”. (LE COADIC, 2004, p. 9).

A CI constitui-se pela sua característica interdisciplinar, já que para desenvolver-se e garantir cientificidade empresta de outras disciplinas saberes e

bases teórico-conceituais, corroborando com essa idéia o autor Saracevic (1996) afirma que a “ciência da informação é uma das novas interdisciplinas, um desses novos campos de conhecimento onde colaboram entre si: psicologia, lingüística, sociologia, informática, matemática, lógica, estatística, eletrônica, economia, direito, política e telecomunicações”. (SARACEVIC, 1996, p. 20)

A proposta pós-moderna demarca mudanças paradigmáticas concernentes ao modo de fazer ciência. Para Santos (1996) entende-se a ciência pós-moderna como um movimento de superação da crise do paradigma científico dominante desde o século XVII, pela superação do modelo de racionalidade cartesiana, de separação do sujeito e do objeto, a busca da ordem, a separabilidade dos elementos constituintes da realidade. Ou seja, o novo contexto social pós-moderno exige uma responsabilidade social das ciências para com a sociedade, não é possível mais fazer ciência instaurado na fixação de saberes rígidos e fechados, é necessário que ela tenha compromisso com a praticidade, orientada a resolver problemas demandados pelos problemas sociais.

Portanto a CI postula uma forte relação com a interdisciplinaridade, no sentido de construir coletivamente com outras disciplinas do saber humano, esquemas conceituais, postulados teóricos com a intenção de contribuir para o bem estar do homem na sociedade em que vive.

Para elucidar o comprometimento social da Ciência da Informação Wersig (1993) relaciona a CI com a perspectiva pós-moderna, ao relacioná-la com a abordagem orientada para soluções e a resolução de problemas. Saracevic (1995, p.1) ressalta que a “ciência da informação, como qualquer outro campo, é definida pelos problemas que apresenta e pelos métodos que escolhe para resolvê-los”.

Reafirmando as idéias expostas acima não é demais afirmar que a CI orienta-se pela resolução de problemas e temáticas complexas, em especial, propõe soluções para demandas específicas de informação.

O crescimento desordenado de informações conhecimentos, desencadeou um fenômeno social conhecido como problemas inerentes á recuperação da informação. Corroborando com esta afirmação (Saracevic 1996, p.2)

ressalta que a “explosão da informação é um problema social que teve seu início com o desenvolvimento das ciências, e hoje se estende para todas atividades humanas”.

A explosão informacional aliada ao desenvolvimento e a aplicabilidade das Tecnologias de Informação e Comunicação (TICs) é considerado por muitos autores como o surgimento da sociedade da informação, pós-moderna, pós-indústrial, pautada na informação e nas tecnologias, desse modo afirma (FERREIRA, 2003, p.5) “vivemos uma época em que as condições de vida e a tecnologia estão se desenvolvendo contínua e exponencialmente e em uma sociedade na qual a informação e a tecnologia estão intimamente ligadas á vida das pessoas [...]”.

O surgimento do fenômeno das tecnologias na perspectiva da ciência da informação é interpretado por Saracevic (2002, p.) como decorrente do “imperativo tecnológico”, está estreitamente relacionada com a própria evolução do campo. Corroborando com o ponto de vista de Saracevic os autores (GARCIA GUTIERREZ, 1999, p.52 apud KOBASHI, TÁLAMO, 2003, p.7) afirmam que o

> O marco tecnológico é indissociável e indispensável na teoria e nas práticas informacionais, não somente pelos aspectos pragmáticos de ambas, mas também porque sua ausência torna inservível qualquer proposta de ação. A tecnologia é elemento conceitual e constitutivo [da Ciência da Informação]. a tal ponto que, atualmente, não é possível a pesquisa de procedimentos informacionais fora desse quadro.

No sentido de garantir sua institucionalização social a CI, vem ampliando o diálogo coletivo com diversos atores sociais. Consolida a área dialogando em diversos espaços institucionais e organizacionais através de práticas investigativas, grupos de pesquisas, práticas profissionais, práticas de formação, no sentido afirmar marcos teóricos, técnicos e conceituais concernentes ao uso social da informação, envolvendo as práticas e atividades de produção, organização, representação, recuperação e uso da informação.

Diante da complexidade informacional demandada pelo contexto da sociedade da informação sua missão é contribuir na construção de aportes teóricos, conceituais para aplicabilidade nos recursos, produtos, serviços, mecanismos e

processos que envolvam contextos e práticas informacionais, auxiliando a sociedade a compreender o fenômeno informacional. Já que tem como objeto “o estudo das propriedades gerais da informação (natureza, gênese, efeitos), e análise de seus processos de construção, comunicação e uso”. (LE COADIC, 2004, p. 25). Visando garantir a participação ativa da sociedade nos processos de produção e uso da informação.

Na perspectiva pragmática a CI configura-se para resolver os problemas informacionais ocasionados pelo crescente avanço da produção técnico-científica, e do surgimento de diversas formas de canais de publicação de informação registrada.

Assim, ela surge para propor soluções práticas no sentido de possibilitar o acesso à informação relevante condizentes com as demandas e necessidades informacionais dos cidadãos, dos contextos organizacionais e dos pesquisadores, ou seja, o auxílio é refletido na disponibilização de meios, técnicas, métodos e práticas para assegurar a eficácia nos processos que envolvam a gestão, produção, acesso e uso da informação.

No entanto para garantir a participação dos atores organizacionais é necessário que a informação seja validada para que possa ser circulada e usada, ou seja, é preciso dar sentido e contexto, organizá-la física e tematicamente para prover seu uso em contextos específicos.

5.1.2 Informação e Conhecimento

A informação na acepção pós-moderna cumpre um papel decisivo nas práticas sociais da sociedade e dos contextos organizacionais, isso porque, ela está diretamente relacionada ao conhecimento.

A discussão travada por autores de diversas disciplinas, especificamente pela CI no sentido de postularem um único sentido para o significado do termo informação tem produzido inúmeras conceituações e acepções ao termo.

A informação é entendida em alguns contextos como processo, fluxo, dados elaborados, mensagem, produto, registros contendo estruturas significantes e significados, insumo para competitividade, registros inscritos num suporte qualquer, dentre outras acepções.

Vale destacar que a Informação vista como processo é entendida como um componente que reduz a incerteza, modificando o estado anômalo do conhecimento de cada indivíduo. Entretanto para que haja modificações nas estruturas mentais de um indivíduo, é necessário que o indivíduo perceba e assimila a informação. Porque nem sempre o que constitui uma informação para um indivíduo, é também percebido e assimilado como informação pelo outro indivíduo, isto é o processo de reconhecimento e de apropriação de informações dependem de operações e capacidades cognitivas.

Nessa perspectiva é pertinente a construção de modelos organizativos da informação que potencializem os processos de tratamento, organização, representação, recuperação, transferência e uso social.

No sentido de delinear o conceito de informação utilizado nessa pesquisa, destaca-se o consenso de alguns autores da CI ao definirem informação como sendo um registro inscrito em suporte passível de significante e significado, dessa forma o autor Le Coadic (2002), afirma que

> Informação é um conhecimento inscrito (gravado) sob a forma escrita (impressa ou numérica), oral ou audiovisual. A

> informação comporta um elemento de sentido, É um significado transmitido a um ser consciente por meio de uma mensagem inscrita em um suporte espacial-temporal: impresso, sinal elétrico, onda sonora, etc. Essa inscrição é feita graças a um sistema de signos (a linguagem), signo este que é um elemento da linguagem que associa um significante a um significado: signo alfabético, palavra, sinal de pontuação (LE COADIC 2005, p. 4)

Outra definição é descrita pelo autor Buckland (1991), ao denominar *informação-como-coisa* e ao afirmar que informação "é também atribuído para objetos, assim como dados para documentos, que são considerados como "informação", porque são relacionados como sendo informativos, tendo a qualidade de conhecimento comunicado, ou comunicação, informação, algo informativo". (BUCKLAND, 1991, p. 352)

Nota-se que é crucial a contextualização do sentido da informação para melhor adequar e aplicar coerência conceitual. Isso porque, diversas áreas do conhecimento possuem interface com a informação e alimentam-se dela. No entanto é necessário que a CI dê conformação conceitual, já que a informação é seu objeto de estudo, e conseqüentemente a CI é uma

> disciplina que investiga as propriedades e o comportamento da informação, as forças que governam seu fluxo e os meios de processamento para otimizar sua acessibilidade e utilização. Relaciona-se com o corpo de conhecimentos relativos à produção, transmissão, transformação e utilização da informação. (BORKO, 1968)

A característica multifacetada da informação, deve-se ao fato da CI obter alto grau de interdisciplinaridade com outras áreas, utilizando-se de princípios, teorias, metodologias e construtos emprestados de diversas disciplinas do saber humano. (PINHEIRO, 200-)

Dessa forma, os enfoques perpassam desde o aspecto cognitivo, relacionando informação e conhecimento, informação para negócios, tomada de decisões, informação como insumo, ou sua dimensão política e social. (PINHEIRO, 200-).

Para Wersig e Nevelling citada pela autora Ribeiro ressalta que

> informação como objeto da ciência da informação não é uma certeza, na medida que é "um possível objeto [...]", e o termo, marcado por ambigüidade, "e o mais extremo caso de polissemia na comunicação técnica da informação e documentação". Esses teóricos identificam pelo menos seis abordagens [...]. abordagem estrutural (orientada a matéria); abordagem do conhecimento; abordagem da mensagem; abordagem do significado (orientada à característica da mensagem); abordagem do efeito (orientada ao receptor); e abordagem do processo.

Percebe-se a geração de uma variação conceitual, fala-se do conceito de informação sob diversas abordagens, em diferentes áreas do conhecimento.

Porém o autor BARRETO (2002, p. 1) traz uma contribuição no sentido de entender as relações imbricadas sobre informação e conhecimento, ao considerar o conceito de assimilação da informação como "agente mediador da produção do conhecimento" (BARRETO, 2002, p. 1).

MIRANDA (1999, p.285) define o conceito de informação no cotidiano das organizações, como sendo "dados organizados de modo significativo, sendo subsídio útil à tomada de decisões" (MIRANDA, 1999, p. 285).

Beal (2004) define a informação como dados dotados de relevância e propósito, o conhecimento também tem como origem á informação quando a ela são agregados outros elementos.

Percebe-se a inclusão para definir informação, do termo dado, como necessário à constituição da informação; sendo um elemento fora do alcance de sentido e compreensão, ou seja, seria o estado bruto da informação.

Pondera-se que nas acepções conceituais sobre informação fica evidente o inter-relacionamento da tríade: dados, informação e conhecimento.

Portanto, para instituir modelos de SGSI é imprescindível compreender a dinâmica dos fluxos de informação e de conhecimentos nas organizações. Sendo necessário (re)conhecer as especificidades dos conceitos: dados, informação e conhecimento.

Para melhor elucidar esta relação o autor Barreto define informação como sendo, “estruturas simbolicamente significantes com a competência e a intenção de gerar conhecimento no indivíduo, em seu grupo, ou a sociedade”. (Barreto, 2002, p. 1)

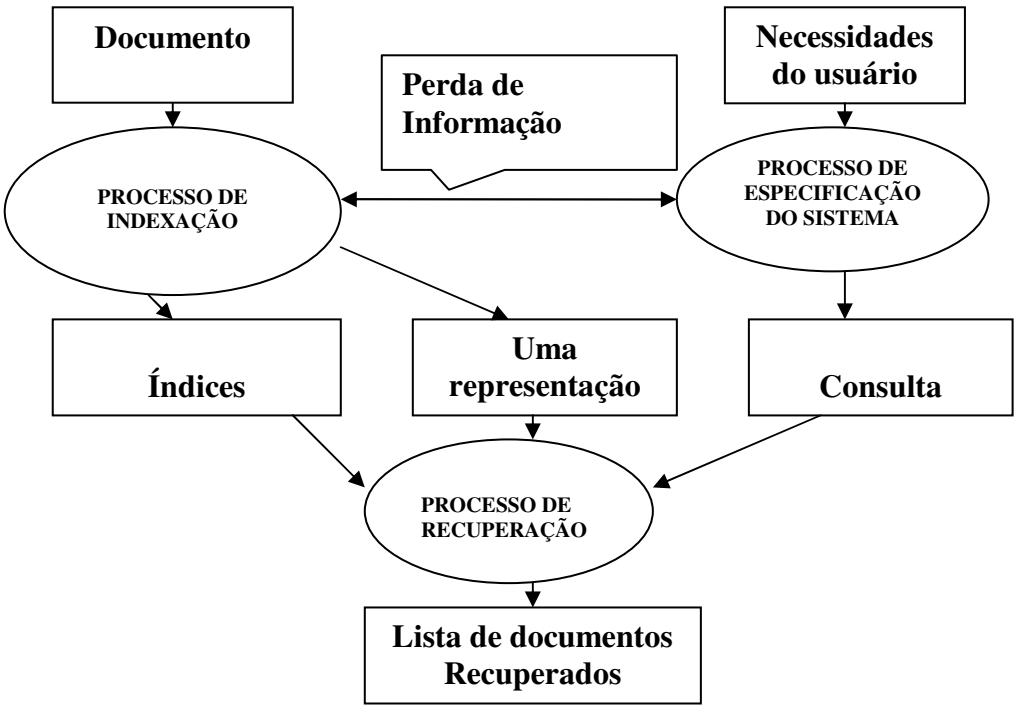
Parra Barreto (2002) a relação entre informação e conhecimento é entendida como componente modificador do estoque mental do indivíduo. Deixa de ser apenas uma medida de organização para reduzir incertezas.

Na tentativa de melhor adequar a abordagem em torno da acepção de informação, utilizaremos o conceito de *“informação como coisa*”, Buckland (1991, p. 2). Ao considerar os documentos, livros, objetos, artefatos, imagens, sons, bases de dados, arquivos digitais no contexto dos sistemas de informação, designando teor informativo relativos a coisas com a intenção de informar. Além do conceito enunciado pelo Le Coadic (2004) ao definir informação como estruturas contendo significante e significado, inscrito sob a forma escrita, impressa ou numérica composta de sentidos.

5.1.3 Recuperação da Informação

O aumento, a proliferação e a diversificação das fontes de informação no contexto dos sistemas de informação, entendida como bibliotecas, centros de documentação, arquivos, museus, bases e banco de dados exigem cada vez mais sistemas de recuperação de informação sofisticados.

Os sistemas de recuperação da informação é um componente central nas organizações sociais que acumulam, organizam e transferem informações. Um sistema de recuperação de informação (SRI) pode ser estruturado, conforme a figura de (GEY 1992 citado por ROBINS, 2002).



Fonte: GEY, 1992

Figura 12: Componentes de um sistema de recuperação de informação

Diante da figura ilustrada acima, é visível a complexidade que envolve as etapas, operações e atividades para organizar, representar e recuperar documentos/informações no contexto dos SRIs.

Nesse sentido, as atividades de organização, armazenagem e transferência de informações necessitam de aportes metodológicos, normativos e representacionais em cada uma das etapas elucidadas na figura acima.

Na perspectiva de dotar SRIs condizentes com as demandas e necessidades de contextos específicos, vale destacar a importância das linguagens de representação, ao oferecerem oportunidades para retificar as dissonâncias e ruídos lingüísticos, semânticos e terminológicos provocados pelas multiplicidades das operações e etapas que envolvem as atividades de organização e transferência de informação nos sistemas de recuperação da informação.

A ausência de métodos, ferramentas e mecanismos adequados para descrever e representar informações impactam negativamente nos processos de recuperação de informações.

Portanto, faz-se necessário preocupar-se com as operações que envolvem os processos de descrição e de indexação, utilizando-se de linguagens de representação da informação e do conhecimento.

Desse modo, as linguagens de representação são cruciais para assegurar o sucesso de um sistema de recuperação da informação, já que são desenvolvidas no sentido de descrever fisicamente e tematicamente informações e conhecimentos, além compatibilizar a terminologia do usuário com a linguagem de representação de um sistema de recuperação da informação.

Podemos afirmar que os sistemas de recuperação da informação tendem a serem imprecisos, por não considerar as linguagens de representação como conceito central nos sistemas de recuperação da informação.

Para melhor entendimento do conceito recuperação da informação Calvin Mooers define:

> A recuperação da informação é uma disciplina interessada nos processos pelos quais questões são apresentadas a sistemas de informação [...] O resultado final desses processos é uma lista de documentos que são um subconjunto dos sistemas de informação. O processo pode ser realizado por qualquer meio, mas essencialmente, quando atributos específicos de uma questão são correspondidos com atributos de um documento, o documento é incluído na lista. (ROBINS, 2000 p. 57).

A recuperação da informação (RI) é considerada por diversos autores o núcleo da Ciência da Informação.

Mooers é considerado autor fundador do termo recuperação da informação (Information Retrieval). Difundida durante as décadas de 1950 e 1960, no sentido de propor soluções eficazes para a recuperação de informações, decorrente do desenvolvimento científico e tecnológico, e o aumento das dificuldades para armazenar e recuperar informações, ocasionada pela "explosão da informação", como "irreprimível crescimento exponencial da informação e de seus registros, particularmente em ciência e tecnologia" (SARACEVIC, 1996, p. 42).

Nesse contexto surge uma disciplina preocupada com a recuperação da informação (SARACEVIC,1996, p. 42). Ela surge para tratar "dos aspectos intelectuais da descrição da informação e sua especificação para busca, e também de qualquer sistema, técnicas ou máquinas que são empregados para realizar esta operação". (MOOERS, 1951)

A disciplina, desde seu início preocupa-se em responder algumas questões "como descrever intelectualmente a informação?; como especificar intelectualmente a busca?; que sistemas, técnicas ou máquinas devem ser empregados?; (MOOERS, 1951). O autor Saracevic (1996) aponta que tais questões elucidados por Mooers ocasionou o surgimento de

> Uma grande variedade de conceitos e construtos teóricos, empíricos e pragmáticos, bem como numerosas realizações práticas. Muitos exemplos históricos podem ilustrar a marcante evolução dos sistemas, técnicas e/ou máquinas utilizadas para recuperação da informação. Sua variedade vai dos cartões perfurados aos CD-ROMs e acesso on line; dos sistemas não-interativos àqueles de

> recuperação de informação em um processo altamente interativo; de bases documentais para bases de conhecimento; dos textos escritos aos multimídias; da recuperação de citações à recuperação de textos completos; e ainda aos sistemas inteligentes e de respostas a perguntas. (MOOERS, 1951 apud SARACEVIC 1996)

Pode-se afirmar as preocupações elucidadas pelo autor Mooers, aponta a necessidade de prover meios eficazes para a organização e representação da informação, além da necessidade de compreender melhor os processos e operações cognitivas nas atividades de representação e recuperação da informação.

Os problemas relacionados á recuperação da informação, já era uma preocupação social para muitos pesquisadores, cientistas, bibliotecários, documentalistas, desde o final do século XIX. Podemos citar os visionários Paul Otlet e La Fontaine, sendo o primeiro considerado por muitos autores da área como percursor e fundador da Documentação e da Ciência da Informação.

Paul Otlet identificou um problema social, o de prover meios eficazes para recuperação da informação. Na tentativa de resolver os problemas de recuperação e acesso á informação, surge a Documentação, preocupada em fomentar e institucionalizar práticas profissionais, mecanismos, ferramentas e técnicas para gerir os processos de produção, organização, armazenamento, representação e recuperação de informações e documentos. Otlet “cunhou o termo “documentação” pra expressar uma abordagem mais ampla à organização de fontes de conhecimento do que a tradicionalmente associada ao termo “bibliografia” (RAYWARD,1997, p. 18).

Ou seja, ela é dotada de técnicas, métodos e práticas para resolver os problemas ocasionados pelo crescente avanço da produção técnico-científica, conhecida na época como “explosão da documentação”.

Na atualidade, os problemas de recuperação da informação são identificados devido ao aumento desordenado do conhecimento, aliado ao surgimento de diversos canais de publicação da informação registrada, além da dispersão e despersonalização da informação e do conhecimento.

A Documentação enquanto disciplina científica surge para propor soluções práticas para acessar informação relevante e pertinente de acordo com as necessidades demandadas pelos pesquisadores e cientistas.

Na perspectiva dos SRIs, pode-se afirmar que a preocupação central da Documentação é a recuperação da informação de grandes massas de documentos, para tal utiliza-se de recursos tecnológicos da época, incluindo a fotografia e especificamente o microfilme, além de práticas de busca mecânica de publicações.

Em 1895 Paul Otlet e La Fontaine fundaram o IIB – Instituto Internacional de Bibliografia, com a intenção de elaborar um catálogo bibliográfico universal, foi criado o RBU denominado de Repértoire Bibliographique Universal, um grande banco de dados, contendo diversas coleções, bibliografias, imagens, textos entre outros objetos. Com finalidade de sintetizar todo conhecimento registrado. (RAYWARD, 1997).

Dentre as tecnologias desenvolvidas no contexto da Documentação para gerir o processo de representação no sistema de recuperação de informações e documentos – RBU, foi utilizada a CDU – Classificação Decimal Universal.

Podemos afirmar que a Documentação contribuiu significativamente para a consolidação/institucionalização social e cognitiva do campo da Ciência da Informação, importando para a CI as bases teóricas, marcos conceituais e técnicas concernentes á práticas e atividades de organização, armazenamento, acesso, recuperação e transferência de informações. Corroborando com esta afirmação o autor Rayward (1997) afirma que as idéias e práticas desenvolvidas pela Documentação no período de 1895 até o início dos anos 30, fossem discutidas hoje, receberiam rubricas de

> informação tecnológica, recuperação de informação, estratégias de busca, centros de informação, serviços de informação pagos, bases de dados online, software de gerenciamento de banco de dados, redes acadêmicas de comunicação, e até mesmo a moderna difusa de informação. (RAYWARD, 1997, p. 2)

Desse modo é perceptível à relação histórica e a interface natural que a Documentação possui com a Ciência da informação, pois os tópicos elucidados acima, refletem na atualidade temas centrais da área.

Em 1945, Vannevar Bush escreveu artigo intitulado “As we may think”, denunciava o problema da explosão informacional em ciência e tecnologia e as dificuldades para organizar, armazenar e transferir o conhecimento técnico-científico acumulado durante a guerra e pós-guerra, e as dificuldades em repassar essa avalanche de informações para a sociedade.

No sentido de solucionar os problemas suscitados pelo surgimento de grandes volumes de massa informacional produzidas no período guerra e pós-guerra, ele propõe uma tecnologia compatível com a inteligência e base tecnológica da época, denominado por ele de “Memex”, dispositivo para tornar acessível o emaranhado estoque de conhecimento, definida por ele como “um dispositivo futuro de uso individual que é uma espécie de arquivo e biblioteca privados mecanizados”(BUSH, 1945).

A preocupação de Vannevar Bush perpassa pela organização, armazenamento, preservação e recuperação de estoques informacionais em contextos especializados. Isso porque até o momento, as praticas de organização do conhecimento eram baseadas em esquemas de organização hierárquica, linear e artificial.

Sua proposta para organizar e recuperar informações questiona o modelo de organização e recuperação vigente na época, baseado em estruturas lineares e estáticas.

Propõe um novo paradigma, de organização, gestão e recuperação da informação baseada num modelo associativo, ao afirmar que “a mente humana não trabalha por indexação, e sim por associação [...] a seleção por associação, e não por indexação pode ser mecanizada [...]". (BUSH, 1945). Isto é, propôs um modelo para estender a memória humana, criando meios para organizar a informação de forma associativa através de um dispositivo mecânico que permite a uma pessoa organizar, armazenar, e consultar seus livros,

arquivos e comunicações, de forma associativa. Permitindo ao usuário tomar nota de cada fragmento de informação, bem como agregar informações e ligá-la a essa rede já existente, onde “a característica essencial do Memex é o processo de relacionar dois elementos diferentes entre si” (BUSH, 1945).

Percebe-se que o fenômeno da recuperação da informação não é uma preocupação recente. Desde a invenção da escrita, o homem utilizou-se do registro em suportes documentais e viu-se obrigado a desenvolver meios para auxiliá-lo nos processos de armazenamento, organização e recuperação futura. Constata-se essa preocupação desde a Antiguidade pelas evidencias encontradas nas práticas de organização, armazenamento e recuperação de objetos documentais custodiados nos arquivos e bibliotecas.

É uma preocupação recorrente, é verificada na atualidade, pois é perceptível o aumento dos transtornos e problemas em acessar e recuperar informações relevantes e pertinentes. É uma preocupação central da Ciência da Informação.

Pois na atualidade nunca se teve tanta circulação da informação, no entanto não há usabilidade porque não há formas consistentes e pertinentes para recuperação da informação.

O fenômeno agrava-se ainda mais na atualidade devido o impacto das tecnologias de informação e comunicação nos sistemas de recuperação da informação ao modificarem as praticas informacionais dos usuários ao impor novas formas de interação e interlocução com os sistemas de recuperação nos contextos digitais, nesse sentido o autor Barreto (1999, p.376), afirma que “a importância do instrumental da tecnologia da informação forneceu a infra-estrutura para modificações sem retorno, das relações da informação com seus usuários”. Ao mesmo tempo essas transformações também potencializaram o acesso a grandes massas de informações, possibilitando dessa forma “a interação [...] com as memórias de informação e a conectividade aos diferentes espaços de acesso a [...] informação”. (BARRETO, 2002, p.4)

5.1.4 Organização e representação da Informação

No sentido de contribuir para o avanço de conhecimentos técnicos e científicos na pós-modernidade, é primordial dotar os sistemas de recuperação da informação com instrumentos e mecanismos para organização, estruturação e representação da informação, visando facilitar a comunicação entre estoques de informação e usuários.

Na perspectiva da recuperação da informação, vê-se o aumento desordenado em torno de definições conceituais e terminológicas em diversas áreas, sendo necessário á construção e uso de instrumentos representacionais para contextualizá-las e garantir sua univocidade conceitual dentro de uma área.

Desse modo à organização e representação da informação é preocupação marcante na nas práticas históricas das áreas da biblioteconomia, documentação e da ciência da informação.

Podemos citar o visionário Otlet ao desenvolver entre 1904 e 1907 a CDU – sistema de classificação para representar e recuperar informações armazenadas do RBU – Repertório Bibliográfico Universal.

Desse modo, ao considerar a informação como “agente mediador da produção do conhecimento” (BARRETO, 2006). É fundamental prover meios eficazes para sua organização e representação, só dessa forma será possível Inseri-la no processo do ciclo de produção de conhecimento.

Nesse contexto destaca-se o importante papel desempenhado pelos instrumentos de representação documentárias, as chamadas Linguagens Documentárais (LDs).

São elas que irão ativar de forma consistente as informações armazenadas nos sistemas de recuperação de informação, cumprindo ação comunicativa entre o documento e o usuário, exigidas no processo de transferência da informação.

No processo documentário, elas traduzem a linguagem natural para linguagem utilizada pelo sistema.

> Dito de outro modo, uma LD é utilizada na entrada do sistema, quando o documento é analisado para registro. Seu conteúdo é identificado e “traduzido”, de acordo com os termos da LD utilizada pelo sistema e segundo a política de indexação estabelecida. É da mesma forma utilizado à saída do sistema, quando a partir da solicitação da informação pelo usuário, é feita a representação da busca. Assim, seu pedido é analisado, seu conteúdo é identificado e

> devidamente “traduzido” nos termos da LD utilizada (CINTRA et al, 2002, p. 40)

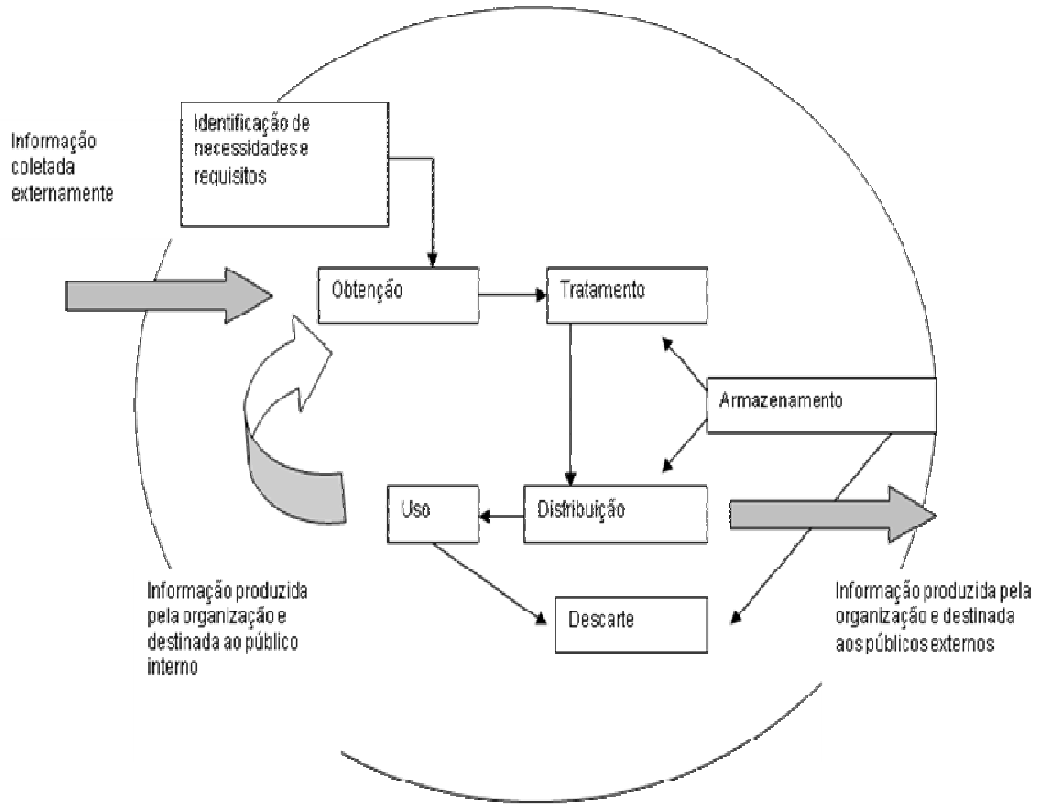
Observa-se também que os requisitos enunciados pelas normas e procedimentos da SI, enfatizam muito mais os aspectos procedimentais e tecnológicos. Verifica-se na maioria das normas a ausência de requisitos específicos aos aspectos inerentes de Organização e Tratamento da Informação, Representação e Recuperação da Informação.

De modo geral, entendemos que Gestão da Informação (GI) na perspectiva da Ciência da Informação (CI) poderá subsidiar o processo de desenvolvimento e sistematização de requisitos para melhor compreensão das especificidades que envolvem as práticas de organização, tratamento, representação e recuperação de ativos de informação ausentes nas normas de Segurança da Informação (SI).

5.1.5 Atribuições da área de Gestão da Informação

Partindo do princípio que a gestão da informação é conjunto de processos que visa a obtenção de um diagnóstico das necessidades de informação e mapeamento de fluxos formais de informação nos vários setores da organização e que englobam atividades de planejamento, organização, direção, distribuição e controle de qualquer recurso.

Para Beal (2005), a GI relaciona-se ao fluxo de informação seguido pela organização, em que a identificação de necessidades e requisitos de informação é como um elemento impulsionador deste fluxo, fazendo com que haja um ciclo contínuo de coleta, tratamento, distribuição/armazenamento, e uso com o fim de tomada de decisão dos usuários internos, como a disseminação de informação para o público externo à empresa. A figura a seguir demonstra o fluxo de informação proposto pela autora:



Fonte: BEAL, 2004, p.29

Figura 11. Modelo de representação do fluxo da informação nas organizações.

As etapas do ciclo de informação são:

1. Identificação das necessidades de informação – verificar as informações disponíveis no grupo interno ou externo, para que se possam expandir os produtos e serviços informacionais, e ter a visão da necessidade informacional.
2. Obtenção: nesta etapa, são desenvolvidas as atividades de criação, recepção ou captura da informação, proveniente de qualquer meio ou fonte, mas que seja confiável.
3. Tratamento: Para que a informação possa ser usada, é preciso que a mesma passe por um processo de organização, formatação, estruturação, classificação análise, síntese, aprendizagem e reprodução.

4. Uso: Esta etapa é a mais importante da GI, pois ter informação necessária e disponível não significa que está sendo usada, ou seja, não é a existência da informação que garante melhores resultados, e sim o uso que é feito da mesma.
5. Armazenamento: Há a necessidade de se guardar as informações úteis à empresa, permitindo seu uso ou reuso. Deve-se atentar para qual mídia a informação está sendo armazenada, fazendo sempre uma cópia de segurança, e no caso de dados sigilosos, é necessário criar mecanismos de proteção impedindo o acesso de pessoas não autorizadas.
6. Descarte: Quando uma informação perde o seu valor ou torna-se obsoleta para a organização, ela deve ser descartada. Isto faz com que se economizem recursos de armazenamento, aumentando a rapidez e eficiência na localização de informações necessárias.

Considera-se, portanto, que a GI no contexto das organizações deve atuar em conjunto com os princípios da SI para assegurar os ativos de informação corporativa, e modelar sistemas de informação pautados nos pilares confidencialidade, integridade e disponibilidade.

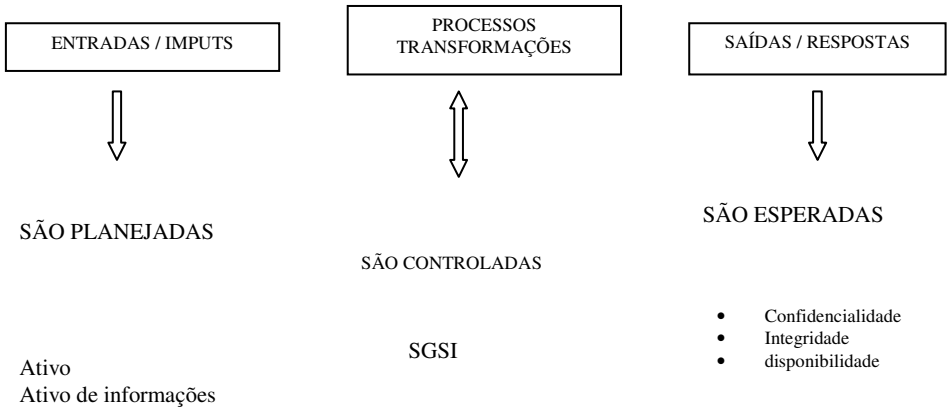
5.2 Atribuições da área de Segurança da Informação

A segurança da informação é obtida através de implantações de controles adequados, políticas, processos, procedimentos, estruturas organizacionais. Com o objetivo de garantir o funcionamento da organização frente as ameaças a que esteja vulneráveis.

A NBR ISO/ IEC 27002 estabelece diretriz, ela provê orientação para iniciar o processo de controles para manter e melhorar a segurança da informação em uma organização é um guia prático onde trás conceitos e diretrizes de melhores práticas exercidas pelo mercado.

Toda e qualquer informação deve ser protegida, esteja armazenadas em qualquer suporte, escrito, desenhado, em papel ou em meios magnéticos em filmes ou falado.

Para melhor elucidar sobre SI enquanto um conjunto de elementos ou componentes que se interagem para alcançar os objetivos e requisitos do sistema. Apresentamos na figura abaixo os principais componentes de um sistema ou sub-sistema de controle de processos, isto é constituído das etapas de entradas, processamento e saídas.



Fonte: Maranhão, Mauriti, (2006, p. 15)

Figura 13– processo sob controle (adaptado pela autora)

A figura acima demonstra que, caso as etapas de imput, processamento e saída estiverem ancorados sob o prisma procedimental da SGSI, isto é, assegurado o controle do processo. Podemos inferir que é possível ter o domínio situacional do contexto onde está inserido o SGSI, podendo determinar ou prever os resultados uma vez que os estímulos (entradas), bem como mecanismos de transformação estão sob o nosso controle. Visto que a finalidade de um SGSI é "projetado par assegurar a seleção de controles de segurança" (NBR ISO/ IEC 27001, p.1).

Conceber um SGSI enquanto processo nos ajuda construir uma visão holística da SI, uma vez que, a compreensão das especificidades de cada processos e sub-processos, nos auxiliará a fazer uma gestão completa do sistema. Isto porque, a tendência da maioria dos modelos de gestão SI é enxergar de modo fracionado o sistema, aplicando os requisitos da SI somente em algumas etapas do processo, como por exemplo, a aplicação de permissão ou restrição lógica do sistema conforme estabelecidos pelo perfil de acesso do(s) usuário(s), ou seja, a sobrevalorização das tecnologias da informação para gestão da SI.

Numa abordagem sistêmica de um SGSI é necessário garantir a efetividade comunicacional da informação para assegurar que os objetivos organizacionais sejam alcançados.

Portanto garantir a funcionalidade da segurança do processo de comunicação num contexto organizacional é imprescindível o desenvolvimento de procedimentos de produção, disseminação e distribuição de conteúdos corporativos que garantam a sua fidedignidade, confidencialidade e autenticidade, com vista a diminuir os riscos e problemas de alterações fraudulentas ocorridas durante as etapas de transferência e distribuição.

Visto que a efetividade dos processos de comunicação da informação é um fator determinante para o sucesso ou fracasso de um SGSI, é imprescindível conhecer em profundidade quais são os processos, sub-processos que compõem um SGSI. É necessário também identificar os ruídos comunicacionais para posteriores ações corretivas.

Para obter um ambiente informacional seguro é necessário um conjunto de requisitos para serviços de segurança: cópias de segurança, controle de acesso, classes de sigilo, trilha de auditoria de sistemas, criptografia para sigilo, assinatura digital etc...

Quanto ao uso de criptografia, tanto para sigilo tanto para autenticação, o rigor dos requisitos está sujeito à legislação vigente e a política de segurança específica. Muitas vezes, a criptografia é usada como mecanismo de apoio ao controle de acesso para reforçar o sigilo de informações. Os requisitos de assinatura digital e certificação digital são necessários para aquelas organizações em que documentos são assinados digitalmente ou verificações eletrônicas de autenticidade são necessárias.

- cópias de segurança têm por objetivo prevenir a perda de informações, e garantir a disponibilidade do sistema. Os procedimentos de backup devem ser feitos regularmente e, pelo menos uma cópia deve ser armazenada preferencialmente off-site.
- classificação da informação quanto ao grau de sigilo e restrição os requisitos descritos nesta pela norma NBR ISO/ IEC 27002 seção referem-se ao acesso com base na classificação do grau de sigilo bem como restrição de acesso à informação sensível. Informação sensível pode estar relacionada à honra e à privacidade de pessoas ou a questões estratégicas e de segredo corporativo.
- trilha de auditoria consiste num histórico de todas as intervenções, ou tentativas de intervenções, feitas nos registros informacionais. Nesse sentido, é também um metadado sobre os documentos digitais e informa sobre a sua autenticidade.
- assinatura digital é uma seqüência de bits que usa algoritmos específicos, chaves criptográficas e certificados digitais para autenticar a identidade do assinante e confirmar a integridade de um documento. Certificação digital é uma técnica, baseada em uma infra-estrutura de chaves públicas, de garantia da validade de assinaturas digitais. O uso de assinaturas digitais e de certificação digital na administração pública foi padronizado e normalizado com a criação da Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil.

Esses requisitos não esgotam o tema SI, pois a segurança integral é sistêmica e abrange não somente a tecnologia, mas também pessoas, processos e legislação.

5.3 Contribuições da GI para o SGSI

O insumo básico da CI é a informação, e como área de formação, possui profissionais que possuem competências e habilidades específicas para contribuir nos processos relativos ao uso da informação e do conhecimento, sendo este o profissional da informação. Tal profissional é capaz de coletar, processar e disseminar informação, atendendo prontamente às necessidades de informações críticas, e possibilitando que a informação atue como uma vantagem competitiva para qualquer organização em que o mesmo estiver inserido.

A GI é base para se fazer uma administração e o gerenciamento de todos os ativos de informação, pois objetivo é obtenção, tratamento e organização da informação com o intuito de fomentar a recuperação e a disseminação, com economia de tempo e de recursos financeiros, visto que se opõe à 'reinvenção de roda', de coisas que já são conhecidas e diagnosticadas através da socialização, as suas melhores práticas.

A finalidade é apresentar o aporte teórico conceitual das principais atividades a serem desenvolvidas tanto pela GI como a de SI buscando como norteador as principais ferramentas da GI para elucidar a contribuição do tratamento e organização da informação para salvaguardar os ativos informacionais de uma organização e auxiliar na constituição do SGSI.

A identificação das necessidades de informação e a incorporação no sistema de gestão informação quando passará a seguir as rotinas de tramitação e arquivamento. Uma vez identificada a informação tanto poderá ser incluído num fluxo de trabalho e posteriormente arquivado, como ser imediatamente descartado após a classificação da informação e reconhecimento de quais informações realmente precisará de tratamento, uma vez que para obter a SI faz-se necessário iniciar pela classificação dos ativos que vai determinar todo o seu fluxo.

Tradicionalmente, nos sistemas de GI, a captura informação é feita no momento em que o documento é registrado, classificado e/ou identificado. Na GI a informação tanto pode ser produzida diretamente dentro do sistema e então capturada automaticamente no momento do registro, como pode ser produzido fora do sistema e capturado e registrado posteriormente.

Portanto, ao pressupor que na gestão da informação corporativa é imprescindível o gerenciamento dos fluxos de produção e uso dos conteúdos corporativos, isto é, a gestão de documentos propriamente dita. É necessário estabelecer uma política de gestão documental pautada no tripé da segurança da informação: confidencialidade, integridade e disponibilidade. Pensamos ser oportuno apresentar como contribuição para o processo de concepção de um SGSI os aportes metodológicos da gestão de documentos.

Sendo assim, encontramos na gestão documental aportes para dotar com mais eficácia a gestão de ativos de informação.

No sentido de compreender a natureza da gestão da informação no contexto das organizações. Concluímos ser oportuno ressaltar que as informações produzidas no âmbito de uma organização, refletem o seu funcionamento; a sua natureza; as atividades; a sua estrutura, a funcionalidade e o seu propósito, portanto podemos caracterizá-la como “informação orgânica”.

Nesse sentido Lopes corrobora (2003, p.33) ao afirmar que a natureza da informação orgânica é composta de um conjunto de recursos e suportes de registros convencionais ou no formato eletrônico produzidas, recebidas e acumuladas por uma organização, como resultado de suas atividades administrativas.

Sendo assim, pretendemos superficialmente aproximar conceitualmente os termos documento e informação. Desse modo, podemos afirmar que um documento evoca um suporte e um registro, elementos indissociáveis para conceber a materialidade da informação compreendida enquanto um objeto documental.

Numa abordagem orientada pelo paradigma da informação para compreensão conceitual do documento, os autores (MOSTAFA; PACHECO, 1995, p.10) afirmam que se for “alargada a compreensão do documento, constatar-se-á não existem diferenças fundamentais [....] são todos suportes de informação”.

Não é nosso objetivo discutir as concepções conceituais em torno dos termos: documento e informação; documento arquivístico; informação arquivística; gestão documental e gestão da informação. É nossa pretensão apenas evocar.

Embora a gestão documental seja uma disciplina da Arquivologia é possível o estabelecimento de um diálogo com a GI, já que a mesma é considerada por muitos autores da CI como disciplina aplicada da Ciência da Informação. E que tanto a CI quanto a Arquivologia compartilham do mesmo objeto de estudo: a informação, e tem como missão propor aportes teóricos, conceituais e metodológicos para possibilitar a transferência da informação em contextos específicos.

Desse modo achamos oportuno uma aproximação do corpus teórico e metodológico da gestão documental por apresentar uma abordagem sistêmica da gestão do ciclo de um ativo de informação.

Sendo assim, compreendemos que a gestão documental é um sub-processo da gestão da informação no contexto das organizações.

Encontramos no modelo de requisitos para sistemas informatizados de gestão de conteúdos corporativos - e-ARQ Brasil que foi elaborado no âmbito da Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de arquivos subsídios metodológicos e a indicação de instrumentos, mecanismos e ferramentas para gerenciar o ciclo de vida de ativos de informação, compreendido aqui, enquanto informação orgânica, materializada num documento.

Essa aproximação se deu ao comparar os objetivos enunciados pelo e-ARQ Brasil ao apresentar especificações de requisitos e estabelecer um conjunto de condições a serem cumpridas pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos a fim de garantir a sua confiabilidade e autenticidade, assim como seu acesso.

Diante do exposto podemos afirmar que os objetivos do e-ARQ Brasil estão alinhados com os princípios da SI que é a confidencialidade, integridade e a disponibilidade.

É um conjunto de procedimentos e operações técnicas, característico do sistema de gestão arquivistica de documentos, processado por computador, aplicável em sistemas híbridos, isto é, que utilizam documentos digitais e documentos convencionais.

Um SIGAD inclui operações de como: capturar documentos, aplicação do plano de classificação, controle de versões, controle sobre os prazos de guarda e destinação; armazenamento seguro e procedimentos que garantam o acesso e a preservação a longo e a médio prazo de documentos arquivisticos digitais e não digitais confiáveis autênticos.

Para cumprir a proposta enunciada nessa pesquisa, segue abaixo alguns princípios norteadores para a construção de um Sistema de Gestão da Segurança da Informação (SGSI) sob a perspectiva da GI, pressupondo que para se fazer de modo sistêmico a gestão da informação é necessário conceber metodologias e procedimentos para organizar e tratar conteúdos de documentos:

A principal etapa para iniciar o SGSI é a classificação dos ativos de informação conforme Santos (2003 p.60) é,

> O processo de agrupar as informações segundo os assuntos, que abrangem, enquadrando dentro de um sistema pré-estabelecido, dando-lhes ao mesmo tempo um lugar certo na coleção e uma localização relativa.

Além do código de classificação, descritores, número de protocolo e número de registro, a captura pode prever a introdução de outros metadados tais como: data e hora da criação, da transmissão e do recebimento da informação; nome do autor, do originador, do digitador e do destinatário, entre outros. Esses metadados podem ser registrados em vários níveis de detalhe, dependendo das necessidades geradas pelos procedimentos da organização dentro do seu contexto jurídico administrativo. Os metadados são essenciais para identificar as informações de um modo inequívoco e mostrar sua relação com os outros, nesse caso podemos aplicar o metadados para garantir integridade das informações.

A utilização dessa ferramenta possibilitará a rastreabilidade dos ativos de informação e auxiliará no gerenciamento do SGSI. Levar em conta a análise da legislação vigente, exigências quanto à transparência e ao exercício das atividades, bem como grau de risco que correm caso não recuperem a informação que principalmente responsabilizam uma organização ou indivíduo por uma ação, obrigação e responsabilidade das informações que estão relacionados à prestação de contas do órgão ou entidade.

Para corroborar com a importância da classificação trazemos o conceito do e- ARQ Brasil(2006) é o ato ou efeito de analisar e identificar o conteúdo dos documentos e de selecionar a classe sob a qual serão recuperados. Essa classificação é feita a partir de um plano de classificação elaborado pelo órgão ou entidade que poderá incluir, ou não, a atribuição de um código aos documentos.

A classificação determina o agrupamento de documentos em unidades menores (processos e dossiês) e o agrupamento destas em unidades maiores, formando o arquivo do órgão ou entidade. Para tanto, deve tomar por base o conteúdo do documento, que reflete a atividade que o gerou e determina o uso da informação nele contida. A classificação também define a organização física dos documentos, constituindo-se em referencial básico para sua recuperação.

A classificação deve se basear no plano de classificação envolve os seguintes passos:

- identificar a ação que informação registra;
- localizar a ação ou atividade no plano de classificação;
- comparar a atividade com a estrutura organizacional para verificar se é

apropriada à unidade que gerou a informação;

- aplicar a classificação a informação independente de seu suporte físico ou lógico.

É através da classificação da informação que deverá se iniciar todo o processo de gestão da SI, pois é nessa faze onde se evidencia quais os ativos de informação e também quais necessitam de proteção, quem são os seus “donos” custodiantes e principalmente para a SI ser classificada quanto ao grau de sigilo.

Após a classificação outro passo muito importante para a GI é a indexação onde é atribuído aos termos à descrição do documento[4], utilizando vocabulário controlado e/ou lista de descritores, tesauro e o próprio plano de classificação. Essas atividades em conjunto auxiliarão o cumprimento dos requisitos na norma NBR ISO/ IEC 27002 principalmente na concepção da Política de segurança, classificação e controles dos ativos de informação, segurança física e do ambiente, gerenciamento das operações e comunicações, controle de acesso,

[4] Documento. Informação registrada independente do seu suporte

desenvolvimento e manutenção de sistemas, gestão da continuidade do negócio e conformidade. Atingindo todos esses passos a organização estará apta a constituir o SGSI.

A seleção dos termos para indexação normalmente é feita com base em:

- tipologia, título ou cabeçalho, assunto, datas associadas com as transações registrada, nome de clientes, órgãos ou entidades envolvidas;

O objetivo da indexação é ampliar as possibilidades de busca e facilitar a recuperação das informações, podendo ser feita de forma manual ou automática.

Os ativos de informação devem ser analisados com relação às precauções de segurança, ou seja, se são considerados ostensivos ou sigilosos. Nos casos sigilosos, a legislação estabelece diferentes graus a serem atribuídos a cada informação.

- as informações que dizem respeito à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas estarão sujeitos às restrições de acesso, conforme legislação em vigor.
- a atribuição de restrições deve ser feita no momento da classificação de segurança e sigilo elaborado pelo órgão ou entidade e envolve os seguintes passos:
- identificar a ação ou atividade que a informação registra;
- identificar a unidade administrativa à qual o documento pertence;
- verificar a política de classificação da informação conforme o plano de SI e o grau de sigilo.

A avaliação é uma atividade vital em um programa de GI pois permite racionalizar o acúmulo de informação nas fases produção, acesso e uso facilitando a constituição do SGSI. A avaliação é o processo de análise das informações, visando estabelecer diretrizes para a destinação, de acordo com a política de classificação da organização e também poderá ser formalizados na tabela de temporalidade e destinação.

Os prazos de guarda referem-se ao tempo necessário para o arquivamento das informações independentes do seu suporte, é necessário aplicar a política de para otimizar os recursos empregados pela organização. Visando atender exclusivamente às necessidades da administração que os gerou, baseado em estimativas de uso.

Recomenda-se nessa etapa que haja uma política de descarte de dados e informações. Para cumprir essa operação é necessário categorizar a natureza dos dados e informações, estabelecendo a priori a natureza dos conteúdos, sua função e contexto, classificando-as conforme sua função e uso organizacional. Estabelecer plano de avaliação de conteúdos, tendo como base algumas características e função desses conteúdos. Podem ser categorizadas tendo como base seu ciclo de vida: valor primário (cumpre ainda uma função informativa atrelada ao uso no cotidiano das organizações); valor secundário (cumpre uma função orientada para o uso, porém é menos utilizada no dia-a-dia); valor terciário (transferência, armazenamento e preservação permanente, ou seja, cumpre função informativa retrospectiva e poderá servir para subsidiar na tomada de decisões e no desenvolvimento de planejamento estratégico, nessa etapa é assegurado a informação e o conhecimento através de ações para ativar a memória organizacional. A política de descarte deve ser estabelecida a partir dessas premissas.

Nesse sentido, nenhuma informação deverá ser conservada por tempo maior que o necessário, pois manter esses recursos custa caro.

O ativo de informação deverá ser classificado no momento da sua criação possibilitando assim o seu gerenciamento e monitoramento conforme o SGSI, identificar a temporalidade e a destinação prevista para a informação no momento da captura e do registro, de acordo com os prazos e as ações previstas na tabela de temporalidade e destinação do órgão ou entidade.

Uma vez que os controles de SI são aplicados muitas vezes somente no ambiente lógico e no que tange a restrições pelo controle de acessos, é oportuno ressaltar a importância de fazer a GI com os aportes e ancorados pelas normas da SI, assim também como através das ferramentas utilizadas para o tratamento e organização da informação ajudará na constituição e manutenção do SGSI e podendo assim trazer grandes benefícios para a organização que enxergar

essas atividades como um macro processo, podendo assim ser administradas e gerenciadas em conjunto em pró de uma gestão efetiva e acima de tudo assegurar seus ativos de informação que hoje é reconhecido como um bem e patrimônio que deve ser protegido.

Observamos também que os requisitos que orientam as normas de SGSI estão em conformidade com a literatura da área, e não apresentam detalhamento de como e quais são as ferramentas e mecanismos para efetivar as atividades de organização e tratamento de ativos de informação. Em resumo só apresentam de modo genérico as medidas e apenas sugerem as normas como requisitos para concepção de SGSI.

6 CONSIDERAÇÕES

Atualmente, o mercado menciona, cada vez mais a segurança da informação, embora a maior parte das organizações não utilizem os recursos referentes a ela de forma conveniente, valem de outras. Muitos dos desperdício dos recursos são motivados pela própria cultura da empresa, ou seja, a perda das informações por descuido, e ameaças simples continuam em patamares elevados como vírus e roubo de equipamentos. Também não podemos nos esquecer de ressaltar os problemas causados pelo excesso de informação (papel/imagem) e a não recuperação da informação na hora exata. Desde que vez a informação seja reconhecida como ativo informacional, faz-se necessário a contemplação de um sistema efetivo para gerencia- la

As informações disponíveis que são armazenadas nas organizações são manipuladas entre os mais diversos setores e sistemas de informação. As decisões e ações são tomadas decorrente dessas informações que devem ser correta, precisas e estarem disponíveis.

Com todo o avanço tecnológico que se delineou nas últimas décadas, as organizações também vêm sendo forçadas a pensarem não só na aquisição e na utilização desses recursos informacionais, mas também quanto à forma de protegê-los.

Nesse contexto, é oportuno ressaltar que, na concepção de um SGSI, através de dispositivos metodológicos no contexto da Gestão da Informação (GI), na perspectiva da Ciência da Informação (CI), deve se utilizar do tratamento da informação no seu ciclo de vida, ou seja, no contexto de coleta, organização, armazenamento, recuperação e disseminação. O processo de SGSI será contemplado em todo o seu ciclo desde o reconhecimento dos ativos de informação até seu descarte, e auxiliara a alta administração a gerir seus ativos de informação.

Podemos afirmar que, para obter um ambiente inteiramente seguro, faz-se necessária a aplicação dos mesmos cuidados com toda a informação da organização, independente do suporte em que esteja armazenada.

Para ocorrer administração da segurança, a organização deverá reconhecer o SGSI como um processo,em que as pessoas responsáveis respondam ,diretamente, à alta administração. Tal fato é necessário para que a área se torne menos suscetível a pressões e para que ela possa ser incorporada, facilmente, pela cultura organizacional.

Sob essa perspectiva, a GI deve incluir, em dimensões estratégicas e operacionais, os mecanismos de obtenção e de utilização de recursos humanos, tecnológicos, financeiros, materiais e físicos.

O mercado cada vez mais à procura de profissionais capacitados para lidar com essas situações pertinentes ao excesso de informações torna-se também pessoas com habilidades e conhecimento na área de segurança física.

Na modernidade os profissionais que atuam em segurança da informação na sua maioria, são provenientes da área da tecnologia, o que, aos poucos, está mudando pois as organizações estão percebendo que só conhecimento técnico (em tecnologia), só aplicações de controles não são suficientes para fazer a gestão de seus ativos, sejam eles tangíveis ou intangíveis. Dessa forma isso cada vez mais, nesse mercado de segurança da informação, contamos com o numero cada vez maior de profissionais de outras áreas como: administração, contabilidade e biblioteconomia.

Compreensão clara das características da organização, sua estrutura, suas capacidades, objetivos, estratégias, restrições legais de atuação e natureza dos ativos de informação, em termos de seus valores tangíveis e intangíveis, é fundamental para que se possam definir critérios adequados para selecionar as melhores alternativas entre as medidas de proteção.

Os processos de produção, armazenamento e teste de recuperação de Backup ou cópias de segurança são fundamentais para garantia a negócio. Além disso, identificação de necessidades e estabelecimento de um ciclo contínuo de coleta, tratamento, distribuição/armazenamento e uso para alimentar os processos decisórios e /ou operacionais da organização também são imprescindíveis.

Após o desenvolvimento deste estudo, pode-se indicar alguns aspectos teórico-metodológicos devem ser levados em consideração pela organização que busca implantar um SGSI, tais como: classificação e controles dos ativos de

informação, avaliação dos níveis de riscos, identificação e avaliação das opções para o tratamento de riscos.

Os desafios para implantação de um ambiente de segurança em qualquer empresa, independente de seu tamanho, são enormes.

Com base em sua experiência, a autora identificou duas dificuldades qe geralmente ocorrem na implementação de um SGSI:

- o não cumprimento das políticas de normas estabelecidas: a organização acha que, com o estabelecimento de algumas políticas de segurança, que, muitas vezes, são mandatórias (isto é, as pessoas são "obrigadas" ou "coagidas" a respeitar o que está escrito no documento, independente se tal faz parte da sua realidade), serão automaticamente aceitas. Uma vez definidas essas políticas na organização, a alta administração e, principalmente, os administradores tecnológicos acham que, com esse procedimento, a empresa está livre de ameaças e vulnerabilidades, o que nem sempre acontece.

  A dificuldade está em estabelecer as políticas e normas de acordo com as necessidades reais da organização, ou seja, antes da implementação deve ocorrer a gestão que compreende o planejamento, o projeto, a construção, a implementação, a utilização, o monitoramento, a identificação de melhorias e a realização de ajustes.

- segurança apenas nos ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários. A empresa investe ,absurdamente, apenas em ferramentas de aplicação de ambientes lógicos como os Firewall e controle de acesso, e os perfis de acesso são categorizados a partir da função e das atividades desenvolvidas.

  Um sistema de gestão de segurança da informação abrange muito mais do que a segurança da informação de TI, pois ele cobre a segurança de toda e qualquer informação da empresa, esteja ela em meios eletrônicos, papel ou, até mesmo, na mente dos funcionários.

Ao analisar os princípios básicos dos controles de segurança, do tratamento da informação, da classificação dos controles e dos ativos de informação enquanto componentes de um SGSI, salientamos que é oportuno contemplar ,durante a GI, os princípios da SI, assim como a implantação do SGSI com o auxilio e ferramentas da GI.

Da mesma forma, corrobora-se a colaboração da GI para SI e o SGSI, considerar-se que o insumo básico da CI é a própria informação base para os referidos processos. Além disso, a atuação do profissional da informação é um diferencial, uma vez que ele é capaz de agregar valor à informação visto que promove uma exploração superior desses processos, ou seja, usufrui deles o máximo possível.

É importante salientar que, apesar da importância da GI e do SGSI, é difícil para a empresa manter sempre o processo e investimentos. Dessa forma, é necessário que se promovam oportunidades para tornar esse processo um diferencial competitivo diante do mercado.

Evidentemente que, por se tratar de assunto incipiente, demandam-se estudos futuros, para que essa discussão seja complementada, de forma a consolidar a proposta desta pesquisa.

REFERÊNCIAS

NBR ISO/ IEC 27001. Associação Brasileira de Normas Técnicas (ABNT). Norma ISO/ IEC 27001-2006 -Sistemas de Gestão da Segurança da Informação – Requisito, 2006.

NBR ISO/ IEC 27002. Associação Brasileira de Normas Técnicas (ABNT). Norma NBR ISO/IEC 17799:2005-código de prática para a Gestão da Segurança da Informação, 2005.

ABREU, Aline França de; REZENDE, Denis Alcides. **Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas.** 2. ed. São Paulo: Atlas, 2001.

ASCENÇÃO, Braga. **A gestão da informação**. Mestrado em Gestão - Universidade da Beira Interior (1996), Disponível em: http://www.ipv.pt/millenium/19_arq1.htm. Acesso em 08 dez. 2008.

BARRETO, Aldo. **A transferência da informação para o conhecimento**. Disponível em <http://www.e-iasi.org/cinfor/transfkk.htm>. Acesso em 09 de jun. de 2006.

BARRETO, Aldo. A condição da informação. **Revista São Paulo em Perspectiva**, São Paulo, v.16., n.3, p.67-74, 2002.

BEAL, Adriana. **Gestão estratégica da informação**. São Paulo: Atlas, 2004.

BEAL, Adriana. **Segurança da informação**. São Paulo: Atlas, 2005.

BEDA, Ednelson. **A importante arte de administrar a informação.** Disponível em: <www.unescnet.br/artigos/artigo%20arte%20informacao2.htm>. Acesso em: 20 mar. 2008.

BORKO H. **Information Science: what is it?. American Documentation**, v.19, n.1, p.3-5, 1968.

BOUTHILLIER, France; SHEARER, Kathleen. Understanding knowledge management and information management: the need for an empirical perspective. **Information Research**, Montreal, v.8, n.1, paper n.141, 2002.

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

BUCKLAND M. K. What is a “document”?. **Journal of the American Society of Information Science**. V.48, n.9, p.804-809.

BUCKLAND, M. **Vocabulary as a central concept in library and information Science**. Disponível em: <http://www.sims.berkeley.edu/coliscov.htm>. Acesso em: 12 dez. 2007.

BURKE, Peter. **Uma história social do conhecimento**: de Gutember a Diderot. Rio de Janeiro: J. Zahar.

BUSH, Vannevar. As We May Think. **The Atlantic Mounthly**, vol. 176, n. 1, p. 101–108, july 1945.

CARUSO, C.A.A.; STEFFEN, F.D. **Segurança em Informática e de Informações**. 2. ed., São Paulo: SENAC, 1999.

CINTRA, Anna Maria Marques et al. **Para entender as linguagens documentárias.** São Paulo: Polis, 2002. (Coleção Palavra Chave).

CHOO, Chun Wei. **A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões**. 2.ed. São Paulo: SENAC, 2003. 425p.

COADIC, Yves-Francois Lê. **A ciência da informação**. 2. ed. Brasília: Brinquet Lemos, 2004.

CONARQ (Rio de Janeiro) (Org.). **Modelo de requisitos para sistemas informatizados de gestão arquivistica de documentos:** Moreq. Rj, 2006. 130 p. Disponível em: <http://www.unicamp.br/siarq/doc_eletronico/e_arq_v1.pdf>. Acesso em: 20 out. 2008.

DAVENPORT, Thomas H. **Ecologia da informação**. 2.ed. São Paulo: Futura, 2000.

DELOITTE TOUCHE TOHMATSU. **Lei Sarbanes-Oxley:** Guia para melhorar a governança corporativa através de eficazes controles internos. 2005. 28 p.

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

DIAS, Eduardo Wense. **Contexto Digital e Tratamento da Informação**. Revista de Ciência da Informação, v.2, n.5, out. 2001. Disponível em: http://www.dgz.org.br/out01/Art_01.htm. Acesso em: 19 dez. 2008.

DUCHEIN, Michel. O respeito aos fundos em arquivística: princípios teóricos e problemas práticos. **Arquivo & Administração,** Rio de Janeiro, v.10-14, n.1, abr. 1983.

DRUCKER, Petr. **A Sociedade Pós-Capitalista**. São Paulo: LTC, 1994.

INFORMATIO SECURITY FORUM. **ISF Report Library. United Kingdom, 1993.** Disponível em: http://www.securityforum.org/html/frameset.htm. Acesso em: 12 dez. 2007.

FERREIRA, Daniela Assis Alves. Tecnologia: fator determinante no advento da sociedade da informação. **Revista Perspectiva Ciência da Informação**, Belo Horizonte, v.8, n.1, p.4-11, jan./jun. 2003.

FOINA, Paulo Rogério. **Tecnologia da informação**: planejamento e gestão. São Paulo: Atlas, 2001.

FONTES, Edison. **Segurança da informação:** o usuário faz a diferença. São Paulo: saraiva, 2000.172p.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 1991. 175p.

KAHN, David. **História da criptologia :** História antiga**.** Disponível em: <http://www.numaboa.com.br/criptologia/historia/antiga.php>. Acesso em: 16 fev. 2008.

KOBASHI, Nair Yumiko; TALÁMO, Maria de Fátima Gonçalves Moreira. Informação: fenômeno e objeto de estudo da sociedade contemporânea. **Transinformação**, Campinas, v.15 (Edição especial), p. 7-21, set./dez. 2003.

MARTINS, José Carlos Cordeiro. **Gestão de projetos de segurança de informação.** Rio de Janeiro: Brasport, 2003.

MARCHIORI, Patrícia Zeni. A ciência e a gestão da informação: compatibilidades no espaço profissional apud **Ciência da informação**, Brasília, v.31, n.2, p.72-79, maio-ago. 2002. Disponível em: <revista.ibict.br/index.php/ciinf/article/viewArticle/159>. Acesso em: 15 mar. 2008.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia científica**. 3.ed. São Paulo: Atlas, 2000. 289p.

MENEZES, Josué das Chagas. **Gestão da segurança da informação**.Leme: Mizuno, 2006.114p.

MODULO, Security Solutions. **6ª pesquisa nacional sobre segurança da informação**, junho 2000. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em: 02 jan. 2007.

MOOERS, Calvin N. Zatacoding applied to mechanical organization of knowledge. **American Documentation**, v.2, p. 20-32, 1951.

MOREIRA, Nilton Stringanci. Segurança mínima: uma visão corporativa da segurança de informação. Rio de Janeiro: Axcel Books, 2001.

MORESI, Eduardo Amadeu Dutra. Delineando o valor do sistema de informação de uma organização**. Ciência da Informação**, Brasília, v. 29, n. 1,

ODDONE, Nanci; GOMES, Maria Yêda F.S. Filgueiras. Os temas de pesquisa em ciência da informação e suas implicações político-epistemológicas. 200-. Disponível em http://ww.cinform.ufba.br/v_anais/artigos/nancioddone.html. Acesso em 18 mar. 2006

PINHEIRO, Lena Vânia Ribeiro. Informação - Esse obscuro objeto da Ciência da Informação. **Morpheus,** v.2, n.4, 2004. Disponível em: http://www.unirio.br/cead/morpheus/Numero04-2004/lpinheiro.htm.

PONJUAN DUARTE, Gloria. **Gestión de información em las organizaciones**: princípios y conceptos y aplicaciones. Santiago, 1998. 222p. XI seminário latino-iberoamericano de gestión tecnológica, 25 a 28 out. 2005. Disponível em: <http://www.pg.cefetpr.br/ppgep/Ebook/ARTIGOS2005/E-book%202006_artigo%2082.pdf>. Acesso em: 02 out. 2008.

RAYWARD, W. B. The origens of information science and the International Institute of Bibliography/International Federation for Information and Documentation (FID). **Journal of the American Society for Information Science**. V.48, N.4, P. 289-300, 1997.

RICHARDSON, Roberto Jarry et al. **Pesquisa social**: métodos e técnicas. 3.ed. rev. ampl. São Paulo: Atlas, 1999. 334p.

ROBINS, David. Interactive information retrieval: context and basic notions. **Informing Science: Special Issue on Information Science Research**, v.3, n.2, p. 57-61, 2000.

SANTOS, Boaventura de Sousa. **Um discurso sobre as ciências**. 8. ed. Porto: Afrontamento, 1996.

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

SARACEVIC, Tefko. Interdisciplinary of nature information science. **Ciência da Informação**, Brasília, v.24, n.1, 1995

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

SERAPIONI, M. Métodos qualitativos e quantitativos na pesquisa social em saúde. **Ciência e Saúde Coletiva**, Rio de Janeiro, v. 5, n.1, 2000.

WERSIG, Gernot. Information science: the study of postmodern knowledge usage. Great Britain. **Information Processing and Management**, v.29, n.2 p. 229-239, 1993.

WERSIG, G., NEVELING U. The phenomeno of interest to information science. **Information Sciense**, v.9, p. 127-140, 1975.