ELAINE CONCEIÇÃO VENÂNCIO

UM ESTUDO DE CASO EM SEGURANÇA DA INFORMAÇÃO

Monografia apresentada à disciplina de Projeto de Pesquisa em Informação II como requisito parcial à conclusão do curso de Gestão da Informação, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná.

Orientador: Prof. José Simão de Paula Pinto.

CURITIBA

2006

SUMÁRIO

LISTA DE ILUSTRAÇÒES

LISTA DE SIGLAS

ABNT	–	Associação Brasileira de Normas Técnicas
BS	–	British Standard
BSI	–	British Standards Institution
COBIT	–	Control objectives for information and related technology
IBL	–	It infrastructure library
IDS	–	Intrusion Detection System
IEC	–	International Electrotechnical Commission
ISO	–	International Organization for Standardization
NBR	–	Norma Brasileira
SSH	–	Secure Shell
SSL	–	Secure Socket Layer
TI	–	Tecnologia da Informação

RESUMO

Baseando-se na literatura pertinente identifica-se através desta pesquisa de caráter exploratório, conceitos e definições a cerca da segurança da informação, e da informação propriamente dita. A informação é um dos "bens" mais valioso dentro das organizações, por isto a importância de primar e zelar pela sua segurança, com vista a seus aspectos: humano, lógico e físico. O estabelecimento e o uso de políticas de segurança da informação a todos os funcionários que atuam na organização é um aspecto a ser destacado na gestão de risco. Entretanto, a divulgação e sensibilização quanto ao tema são escassas, em especial na língua portuguesa, tendo como conseqüência o desconhecimento ou a abordagem equivocada por parte das organizações, neste estudo tratando especificamente as empresas de pequeno porte. Com o intuito de promover maior compreensão e contextualização da abordagem proposta, utiliza o método estudo de caso para identificar a veracidade de tais apontamentos em uma empresa que presta serviços de informações na área geográfica, no município de Curitiba.

Palavras-chave: Segurança da informaçao; política de segurança; gestão de risco; mecanismos de segurança.

1 INTRODUÇÃO

Na Sociedade da Informação ao mesmo tempo em que as informações são tidas como o principal patrimônio das empresas /organizações, estas estão em constantes riscos. Com isto, a segurança da informação tornou-se ponto crucial para a sobrevivência das organizações, pois o vazamento de informações sobre clientes/ usuários compromete a credibilidade e pode dar maiores oportunidades aos concorrentes. Este, portanto, é um dos grandes desafios atuais.

A segurança envolve a proteção das informações, sistemas, recursos e serviços contra desastres, erros e manipulações não autorizadas, de forma a reduzir a probabilidade e o impacto de incidentes de segurança. Envolve também a proteção das informações que são disponibilizadas na rede mundial de computadores, onde a questão da segurança torna-se um item imprescindível para as organizações.

Como já é comprovado que as empresas estão mais focadas no aspecto tecnológico do que cultural pode-se identificar qual é o impacto que uma postura como esta pode causar a uma organização, já que hoje garantir a segurança da informação é uma questão muitas vezes vital às empresas.

Devido ao grau de importância da informação nas organizações a preocupação com segurança da informação precisa estar em todos os segmentos da empresa e, portanto, envolver todos os colaboradores direta ou indiretamente participantes. Por isto, a atenção necessita estar também voltada a política de segurança de informação a ser seguida, esta ao ser definida precisa ter regras claras que estejam de acordo com a cultura e o ambiente tecnológico da organização.

Em face do exposto acima, pretende-se neste trabalho identificar as condições de segurança da informação, tendo como base a literatura pertinente e estudo de caso, refletindo sobre a preocupação em relação a proteção das informações no cenário organizacional.

2 PROBLEMÁTICA E JUSTIFICATIVA

Como este tema no Brasil só começou a ser discutido nos anos 90, a partir da grande expansão do uso e acesso à internet e intranet nas organizações, ainda há muito nesta área que precisa ser explorado em virtude do seu grau de importância. Com base neste contexto este trabalho visa verificar os conceitos de segurança da informação além de auxiliar e alertar principalmente as pequenas organizações sobre este valioso bem ativo.

Devido a defasagem de material em português nesta área de estudo e em contrapartida o risco cada vez maior que a informação esta exposta nas organizações, esta área tornou-se um ambiente rico e que precisa ser explorado e dedicado esforços para que os riscos informacionais sejam amenizados. Sabe-se que não existe uma solução adequada para o tratamento do problema que esta temática aborda e nem tão pouco não há mecanismos de segurança que possam garantir completamente a salvaguarda das informações.

Tendo em vista que a informação é o bem ativo[1] mais valioso de uma empresa, garantir sua segurança passa a ser um requisito estratégico, interferindo diretamente na capacidade/ potencial das organizações quer seja nas negociações ou no valor dos seus produtos/ serviços no mercado.

Além da segurança da informação envolver aspectos tecnológicos, envolve também aspectos humanos e relacionados à cultura organizacional. Desta forma, este trabalho visa nortear quais os cuidados que uma organização precisa identificar para que possa garantir segurança as informações produzidas ou armazenadas.

Os problemas relativos à segurança da informação são complexos. Portanto, a fim de garantir um nível de proteção adequado para os recursos informacionais as organizações devem ter uma visão clara de quais ativos precisam de proteção, selecionando as soluções de segurança que possam identificar e neutralizar as possíveis ameaças as quais os recursos identificados estão sujeitos.

---

[1] SÊMOLA (2003) aborda ativo colocando que "a informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvo de proteção da segurança da informação".

De acordo com a problemática exposta, têm-se como motivadores desta pesquisa os seguintes objetos de estudo:

a) quais são os requisitos básicos para assegurar a segurança das informações de forma eficaz?

b) que procedimentos e ações devem ser observados no estudo da segurança das informações nas organizações?

c) qual/ quais o(s) aspecto(s) de segurança precisam ser avaliados para alcançar o objetivo de proteção dos ativos informacionais?

Desta forma, espera-se que a realização desta pesquisa possa auxiliar responsáveis pela segurança da informação (profissionais de tecnologia da informação, administradores de sistemas, gestores de informações, entre outros) nos procedimentos e cuidados a serem tomados para a segurança informacional, demonstrando também que não há soluções prontas e que é primordial reconhecer o valor da informação e utiliza-la da melhor forma estratégica possível para alcance de bons resultados na proteção das informações. Não existe a pretensão de assegurar total sucesso, mas sim, de reduzir as possibilidades de risco e perda.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Realizar estudo exploratório baseando-se na literatura pertinente sobre a Segurança da Informação, com o propósito de aprofundar o tema e identificar as condições ideais para a redução de riscos que a informação esta exposta.

3.2 OBJETIVOS ESPECÍFICOS:

Para alcançar o objetivo principal da pesquisa, foram definidos os seguintes objetivos específicos:

a) levantar a literatura pertinente sobre informação e a segurança da informação;
b) traçar os meios aconselháveis para garantir a segurança da informação;
c) realizar estudo de caso sobre segurança da informação na organização que desenvolve serviços de informações geográficas.

4 LITERATURA PERTINENTE

Nas próximas seções aborda-se a importância da informação e por conseqüência é apresentado o tema da segurança da informação, descrevendo suas características e, sucintamente, a norma brasileira da área. Posteriormente, comenta-se sobre o estudo de caso realizado na GeoPlus, empresa situada em Curitiba a qual presta serviços de informação na área geográfica.

4.1 INFORMAÇÃO COMO RECURSO ESTRATÉGICO

A informação é uma criação essencialmente humana e é o principal e mais valioso bem ativo dentro de qualquer organização. Portanto, para administrar e garantir a segurança deste recurso não pode-se sugerir ou selecionar soluções baseadas apenas na tecnologia mas também nas pessoas.

Entretanto, os responsáveis por administrar a tecnologia da informação (TI) [2] em geral não têm esta preocupação que é imprescindível para com quem realmente utiliza o sistema, ou seja, o usuário-final. Identificar perfis e conhecer o que os usuários precisam de um sistema apesar de ser algo essencial é muitas vezes ignorado, o que não poderia acontecer já que os usuários-finais são os principais responsáveis pela informação e para que esta realmente cumpra o seu papel: informar.

Portanto, ao falar de informação deve-se identificar se este recurso encontra-se realmente disponível e acessível ao usuário-final. Desta forma, é indispensável que o conceito de informação esteja claramente definido e para que isto ocorra é possível tomar por base alguns conceitos apresentados a seguir:

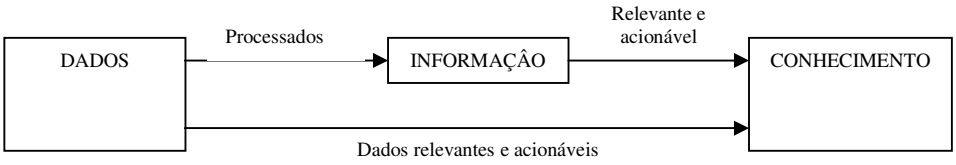
---

[2] Conforme BEAL (2005, p. 8), tecnologia da informação é a "solução ou conjunto de soluções sistematizadas baseadas no uso de métodos, recursos de informática, de comunicação e de multimídia que visam a resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados, e a subsidiar processos que convertem dados em informação".

Para DAVENPORT (2001, p. 18), a informação é difícil de ser definida, tendo em vista que envolve uma conhecida distinção entre dados, informação e conhecimento, sendo que, estes termos fazem conexões uns com os outros. No entanto o autor apresenta as seguintes definições: dados – observações sobre um determinado estado; informação – dados dotados de relevância que visa um uso; conhecimento – esta baseado na mente humana.

Segundo TURBAN et al. (2004, p. 326), "informação são dados organizados ou processados, precisos e fornecidos no momento oportuno". Sendo que, para ilustrar a definição sobre dado, informação e conhecimento no contexto da tecnologia da informação, convém mostrar a Figura 1 que esclarece a definição do autor.

FIGURA 1 – DADOS, INFORMAÇÃO E CONHECIMENTO.



FONTE: TURBAN, E. et al. **Tecnologia da informação para gestão**. 3. ed. São Paulo: Boolkmam, 2004.

MCGARRY (1999, pg. 1), avalia que a informação pode ser "a matéria-prima da qual se extrai o conhecimento" e entre outras avaliações também aponta que a informação é algo que reduz as incertezas em determinado momento e que realiza uma troca com o mundo exterior não sendo passivamente recebido.

Conforme SHAPIRO; VARIAN (2000, p. 15), "qualquer coisa que puder ser digitalizada – codificada como um fluxo de bits – é informação".

Com base nestas definições identifica-se que há uma complementação em cada um dos conceitos apresentados, desta forma, apesar da complexidade do tema é possível traçar uma distinção entre dado, informação e conhecimento, porém é importante destacar que em determinados momentos estas distinções podem ser confundidas.

Atualmente utilizar a informação como um recurso estratégico faz parte da

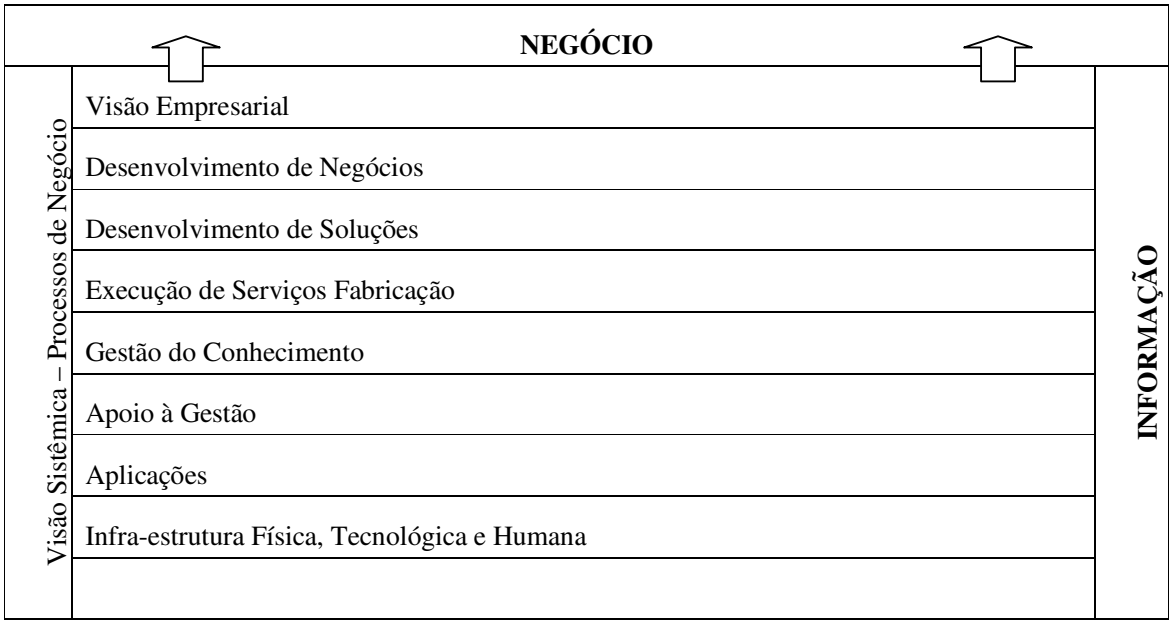
gestão de negócios e é o diferencial no ambiente empresarial, tendo em vista que, a informação é um ativo presente em todos os departamentos e setores. Seja qual for o ramo de atividade e o interesse das organizações, estas tomam sua decisão baseando-se nas informações. No entanto, ao discutirmos o papel estratégico que a informação assume dentro de uma organização é preciso observar que a informação recebe ênfases diferentes de acordo com o ramo de atividade e o segmento econômico em que atuam, assumindo diferentes níveis de importância e valor entre as organizações (MCGEE; PRUSAK, 1994, p. 26).

Como nos últimos anos temos os computadores e as redes de comunicação que disponibilizam um acesso maior as informações facilitando também o crescimento, armazenagem e as modificações destas. Concomitantemente a esta situação as mudanças também acontecem com mais facilidade e com mais agilidade, sendo que quando os negócios se modificam quer seja internamente ou externamente o ambiente informacional também se modifica. Desta forma, o uso estratégico da informação é o diferencial que possibilita que problemas como, a sobrecarga de informações, sejam amenizadas.

Conforme SÊMOLA (2003, p. 2), "segredos de negócios, análise de mercado e da concorrência, dados operacionais históricos e pesquisas, são informações fundamentais e se revelam como um importante diferencial competitivo ligado ao crescimento e a continuidade do negócio".

A Figura 2 a ser observada na próxima página, de SÊMOLA (2003, p. 2) mostra esta onipresença da informação que o autor aborda nos processos de negócios das empresas.

FIGURA 2 – ONIPRESENÇA DA INFORMAÇÃO NOS PRINCIPAIS PROCESSOS DE NEGÓCIO.



FONTE: SÊMOLA, M. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Campus, 2003.

Para TEIXEIRA (1997, p. 223), como em todos os momentos são utilizadas informações para o gerenciamento de negócios pode-se dizer que um bom negócio é determinado pela troca eficiente de informações. São as informações que permitirão o diagnóstico, análise, planejamento, implementação e controle de todos os setores da organização.

Neste contexto identifica-se que além da informação, a organização precisa saber utilizar este recurso estrategicamente caso contrário a ineficiência na administração informacional pode trazer malefícios a organização. Portanto, entender o que é a informação, reconhecer a sua importância e definir a forma de uso estratégico chega a ser vital para as organizações.

4.1.1 Característica da Informação

Ao reconhecer a importância da informação também é necessário dar atenção as características que a informação precisa atender, conforme STAIR (1998), menciona no Quadro 1, apresentado abaixo.

QUADRO 1 – AS CARACTERÍSTICAS DA BOA INFORMAÇÃO.

CARACTERÍSTICAS	**DEFINIÇÕES**
Precisa	A informação *precisa* não conter erros. Em alguns casos, a informação imprecisa é gerada pela entrada de dados incorretos no processo de transformação. Isto é comumente chamado de **entra lixo, sai lixo (ELSL).**
Completa	A informação *completa* contém todos os fatos importantes. Por exemplo, um relatório de investimentos que não inclui todos os custos importantes não está completo.
Econômica	A informação também deve ser de produção relativamente *econômica*. Os tomadores de decisão devem sempre fazer um balanço do valor da informação com o custo de sua produção.
Flexível	A informação *flexível* pode ser usada para diversas finalidades. Por exemplo, a informação de quanto se tem de estoque disponível de uma determinada peça pode ser usada pelos representantes de vendas no fechamento de uma venda, por um gerente de produção para determinar se mais estoque é necessário, e por um diretor financeiro para determinar o valor total que a empresa tem investido em estoques.
Confiável	A informação *confiável* pode ser dependente. Em muitos casos, a confiabilidade do método de coleta dos dados. Quer dizer, a confiabilidade depende da fonte de informação. Um boato vindo de fonte desconhecida que os preços do petróleo devem subir pode não ser confiável.
Relevante	A informação *relevante* é importante para o tomador de decisões. A informação de que os preços da madeira de construção deve cair pode não ser relevante para um fabricante de chips de computador.
Simples	A informação também deve ser *simples*, não deve ser exageradamente complexa. A informação sofisticada e detalhada pode não ser necessária. Na realidade, informação em excesso pode causar **sobrecarga de informação**, quando um tomador de decisões tem informação demais e não consegue determinar o que é realmente importante.
Em tempo	A informação em *tempo* é enviada quando necessário. Saber as condições do tempo da semana passada não ajudará a decidir qual agasalho vestir hoje.
Verificável	Finalmente, a informação deve ser *verificável*, isto significa que pode-se checá-la para saber se está correta, talvez checando várias fontes da mesma informação.

FONTE: STAIR, R. H. **Princípios de sistemas de informação**: uma abordagem gerencial. 2. ed. Rio de Janeiro: LTC, 1998.

Estas características fazem com que a informação tenha mais valor para a organização, pois quando a informação não é precisa e/ou confiável podem ser

tomadas decisões não satisfatórias ou que não trarão o resultado esperado. Se a informação não é relevante à situação, não é transmitida aos tomadores de decisão no tempo adequado e não é simples então esta pode ter pouco valor para a organização.

4.1.2 Ciclo de vida da Informação

Pelo sumo valor que cada vez mais é atribuído à informação, além de saber utilizar estrategicamente, garantir a segurança deste recurso tem sido visto como um critério que tem recebido mais cuidado das organizações. Sendo que, assegurar que as informações sejam preservadas e estejam sobre controle considerando todos os momentos que fazem parte do seu ciclo de vida, é primordial. O ciclo de vida da informação pode ser identificado pelos momentos vividos por esta e que a colocam em risco. Estes momentos existem quando são realizadas ações para manter a operação da empresa. Segundo BEAL (2005, p. 5) o ciclo de vida da informação compreende as seguintes etapas:

a) identificação das necessidades e dos requisitos: afim de desenvolver serviços e produtos de informação para a necessidade interna e externa dos usuários, sendo fundamental identificar a necessidade de informação destes indivíduos;
b) obtenção: esta etapa compreende obter as informações para suprir as necessidades identificadas na etapa anterior. Nesta etapa não pode-se esquecer da integridade dos dados, ou seja, que a informação é autêntica e de uma fonte confiável;
c) tratamento: esta etapa é o processo de organização, formatação, estruturação, análise, síntese, apresentação e reprodução, com a finalidade de deixar esta mais acessível aos usuários;
d) distribuição: a distribuição da informação possibilita que esta seja disseminada a quem precisa dela;

e) uso: esta é uma das mais importantes etapas pois não é a existência da informação que garante melhor resultado e sim o uso que é feito;
f) armazenamento: o armazenamento permite o uso e o reuso da informação, sendo necessário assegurar a conservação da informação, incluindo também o cuidado com as mídias utilizadas;
g) descarte: obedecendo as normas da empresa de política de descarte quando uma informação se torna obsoleta ou perde a sua utilidade ele deve ser descartada. A exclusão de informações inúteis proporciona economia no armazenamento o que aumenta a eficiência na localização de informações, no entanto, este processo precisa ser realizado dentro das condições de segurança.

4.2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um conjunto de medidas que se constituem basicamente de controles e política de segurança, tendo como objetivo a proteção das informações dos clientes/usuários da instituição, controlando o risco de revelação ou alteração por pessoas não autorizadas.

Para conceituar Segurança da Informação será utilizado como base as definições a seguir:

Conforme SÊMOLA (2003, p. 43), Segurança da Informação é “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

FERREIRA (2003, p.1), define que “segurança da informação protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios, minimizando os danos e maximizando retorno dos investimentos e das oportunidades”.

Para SÊMOLA (2003, p. 43) e BEAL (2005, p. 1), a Segurança da Informação precisa considerar o processo de proteção das ameaças à

confidencialidade, integridade e disponibilidade da informação. Para entender este processo será detalhado cada um destes objetivos fundamentais da Segurança da Informação a seguir:

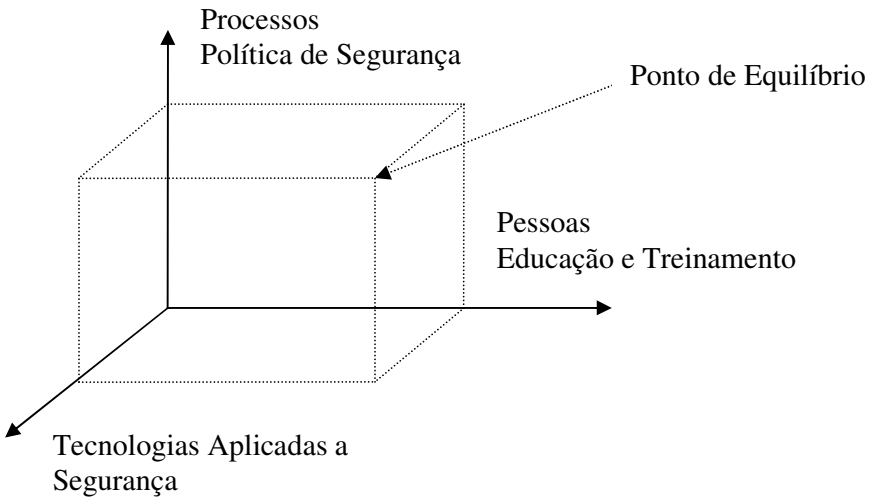
a) confidencialidade: proteger as informações de acessos a pessoas não autorizadas;
b) integridade: garantia da criação legítima, protegendo a informação contra alterações indevidas quer sejam acidentais ou intencionais;
c) disponibilidade: garantir que a informação esteja disponível aos usuários no momento em que for necessária.

DIAS (2000, p. 42-44), também aponta mais quatro objetivos da Segurança da Informação que são:

d) consistência: garantir que o sistema atue conforme as expectativas do usuário;
e) uso legítimo: garantir que o acesso aos recursos informacionais não sejam realizados por pessoas não autorizadas ou de forma não autorizada;
f) confiabilidade: proteção para que mesmo em condições desfavoráveis o sistema atue como o esperado;
g) auditoria: proteger os recursos informacionais contra erros e ações danosas de usuários autorizados.

Somando a essas definições, OLIVEIRA (2005) apresenta o que chama de "tríplice PPT" – Pessoas, Processos e Tecnologias. Segundo o autor, a segurança da informação jamais será alcançada se esses três aspectos não estiverem envolvidos na estratégia de segurança, a Figura 3 na página seguinte, ilustra a proposta do autor.

FIGURA 3 - TRÍPLICE PPT: PESSOAS, PROCESSOS E TECNOLOGIAS



FONTE: OLIVEIRA, S. de. **As tríplices da segurança da informação**, 14 mar. 2005. Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=2&objid=432&> Acesso em: 15 jun. 2006.

OLIVEIRA (2005) considera que as **pessoas** são o elo mais fraco da segurança, sendo que basta que uma pessoa não esteja preparada para que o risco de incidente aumente. No que se refere a **processos** estes precisam ser flexíveis desde que não afetem a segurança por isto é necessário um ponto de equilíbrio, que irá variar de uma organização para outra. Sobre **tecnologia** esta só deve ser aplicada aonde a Política de segurança da informação sejam suportadas.

4.2.1 Política de Segurança da Informação

Devido ao caráter dinâmico das atividades que envolvem o processo de informação a política de Segurança da Informação precisa ser o mais simples e ampla possível.

Conforme DIAS (2000, p. 40), a segurança de informações devido a grande importância para a sociedade atual, deu origem a grupos de pesquisa aonde os

trabalhos muitas vezes são traduzidos em padrões de segurança e projetos legislativos que visam tratar do assunto sob o aspecto legal, protegendo os direitos da sociedade em relação as informações e prevendo sanções legais aos infratores.

Na proposta de CARUSO; STEFFEEN (1999, p. 24), "por política de segurança entende-se política elaborada, implantada e em contínuo processo de revisão, válida para toda a organização, com regras mais claras e simples possível e estrutura gerencial e material de suporte a essa política, claramente sustentada pela alta hierarquia".

A política de segurança em informação é a forma de comunicar aos usuários como tomar as decisões sobre a segurança. Para isto VAITSMAN (2001, p. 108) aborda o que uma política precisa conter. Para o autor a política de segurança necessita especificar o que deve ser feito precisando ser explícita e compreensível para que os usuários compreendam a sua importância. Portanto, a linguagem precisa ser simples e comum, e a responsabilidade precisa ser coletiva entre os usuários, todos precisam se preocupar e sentirem co-responsáveis pela segurança.

Ainda conforme VAITSMAN, a política precisa especificar quem tomará as decisões caso a mesma não seja seguida para que hajam as correções e indicar quais penalidades serão aplicadas. Como as necessidades mudam freqüentemente a política de segurança precisa prever mudanças e ser regularmente revisada.

SILVA (2004) diz que para implementar políticas de segurança de informação deve-se utilizar os seguintes passos:

a) identificar o que se está interessado em proteger;
b) de quem está preocupado em proteger;
c) determinar quais as principais ameaças;
d) implementar as medidas que protegerão os recursos com uma boa relação custo-benefício;
e) rever este processo continuamente aperfeiçoando e eliminando possíveis falhas.

Retomando a proposta de CARUSO; STEFFEN (1999, p.49), estes apontam

as conseqüências de uma política de segurança implementada e corretamente seguida, possuindo os seguintes aspectos:

a) redução da probabilidade de ocorrência, já que as medidas de política de segurança devem ser preventivas;
b) redução dos danos provocados por eventuais ocorrências, se mesmo após as medidas preventivas acontecer algum acontecimento danoso à segurança;
c) recuperação de dados provocados por ocorrências, se mesmo depois que todas as medidas tomadas ainda houver ocorrência danosa, há necessidade de se ter um plano para recuperar os danos.

Essas políticas são tão importantes no que se refere a segurança das informações que conforme FERREIRA (2003, p.17), não é aconselhável que uma organização implemente procedimentos de segurança sem uma política formalmente definida.

FERREIRA (2003, p. 49) também aponta as conseqüências de uma política de segurança implementada e corretamente adotada sendo resumidas nos aspectos a seguir:

a) redução da probabilidade de ocorrências: as medidas precisam ser de cunho preventivo, sendo que riscos eventuais precisam ser previstos e eliminados antes que se manifestem;
b) redução dos danos provocados por eventuais ocorrências: se mesmo com as medidas preventivas houver ocorrências danosas, estas precisam ser reduzidas ao mínimo;
c) criação de procedimentos para se recuperar de eventuais danos: caso aconteçam danos é necessário que existam planos para a recuperação do que foi danificado pela ocorrência.

4.2.2 Classificação das Informações

Diferentes tipos de informações precisam ser protegidos de formas distintas. Para que isto seja possível a informação precisa ser classificada. Sendo que, a classificação é um dos primeiros passos para o estabelecimento de uma política de segurança da informação. Ao classificar a informação a política pode definir como tratá-la de acordo com sua classe, escolhendo os mecanismos de segurança mais adequados.

As autoras DIAS (2000, p. 52-53) e BEAL (2005, p.63-64), identificam que a informação é classificada nos níveis descritos a seguir:

a) informações públicas: estas informações podem ser divulgadas a qualquer pessoa sem que a organização seja prejudicada. Por exemplo, informações divulgadas na imprensa;
b) informações internas: são informações que não devem sair da organização, porém se isto ocorrer não trará conseqüências danosas a organização. Por exemplo, documentos que só interessam aos funcionários, como a divulgação de uma vaga interna;
c) informações confidenciais: o acesso a estas informações é realizado somente conforme a sua necessidade, sendo que somente será permitido o acesso se as informações forem fundamentais para o desempenho satisfatório do trabalho. Exemplo: informações sobre dados pessoais de clientes;
d) informações secretas: para este tipo de informação o controle sobre o uso das informações precisa ser total sendo que o acesso não autorizado é crítico para a organização. Exemplo: senhas de funcionário, dados bancários;
e) informações ultra-secretas: neste tipo de informação o controle também precisa ser total, pois o acesso não autorizado é extremamente crítico a organização. Exemplo: informações de segurança nacional.

Estas classificações são mutáveis, tendo em vista que, as informações consideradas sigilosas em determinada época podem ser de domínio público futuramente, pode-se exemplificar esta situação quando uma empresa esta trabalhando no desenvolvimento de um novo produto, no momento do desenvolvimento as informações são secretas, tendo em vista que não devem chegar ao conhecimento do concorrente, no entanto após o lançamento do produto, estas informações serão de domínio público.

4.2.3 A base da Segurança da Informação

Com o propósito de garantir a Segurança da Informação em uma organização precisa-se identificar a existência de informações não informatizadas, ou seja, que não estão em meios eletrônicos e as que estão armazenadas em computadores e que, portanto se baseiam na tecnologia da informação (TI), tal informação está presente em base de dados, arquivos informatizados e outras mídias que exigem soluções de informática para ser acessada.

Como a maior parte das informações esta baseada na TI muitas vezes as organizações se esquecem que é preciso zelar também pelas informações que estão em suporte físico (por exemplo, papel) garantindo também a sua proteção. No entanto, as pessoas desempenham um papel crucial para a segurança da informação, portanto, aspectos humanos não podem ser descartados, desta forma, aspectos físicos, lógicos e humanos precisam constar em uma política de informações.

4.2.3.1 Segurança em Aspectos Humanos

Como visto no início desta seção as pessoas são consideradas o “elo frágil” da corrente pela segurança da informação e esta preocupação é entendida quando uma única pessoa abusa de seus privilégios de acesso e destrói um esquema de segurança,

por mais sofisticado que seja. Devido a esta problemática BEAL (2005, p. 71) aponta que:

> "A melhor política de segurança em relação a qualquer pessoa com acesso aos recursos de informação corporativos continua sendo a descrita pela conhecida expressão *trust, but verify* (confie, mas verifique). Apesar da maior atenção concedida pela mídia aos ataques causados por *hackers*[3], estudos demonstram que grande parte dos incidentes de segurança é provocada por integrantes da própria organização, sejam eles acidentais (decorrentes de ignorância, erro, negligência ou distração) ou intencionais (por motivo de fraude, vingança, descontentamento etc.)".

BEAL (2005, p. 73) também aborda as principais medidas a ser adotada para reduzir os riscos que a informação está sujeita sendo provocadas pelo elemento humano que são:

a) processo de seleção do pessoal, incluindo a investigação de antecedentes de funcionários, contratados temporários e terceirizados;

b) documentação das responsabilidades de segurança nos contratos de trabalho de funcionários e terceiros;

c) assinatura de acordos de confidencialidade e definição de termos relativos à segurança da informação;

d) supervisão gerencial que permitam detectar e agir em situações de risco ou atitudes suspeitas;

e) nível adequado de segregação de funções, afim de evitar que uma única pessoa seja responsável por todas as etapas de um processo;

f) treinamento e conscientização dos funcionários;

g) expectativa de controle e punição para os casos de descumprimento da política de segurança da informação;

h) processos seguros de demissão, abrangendo a retirada dos privilégios de acesso físico e lógico a informação.

---

[3] Segundo VAITSMAN (2001, p. 93-94) o termo *hackers* poderia ser resumido em "piratas" ou pilhadores modernos do conhecimento. São especialistas de informática que fazem o uso do conhecimento para invadir e causar danos aos sistemas informacionais este termo é comumente divulgado, no entanto o termo correto quando se trata de crimes virtuais é: *cracker,* em geral *hackers* não causam danos.

4.2.3.2 Segurança física

Segundo a proposta de CARUSO; STEFFEN (1999, p. 30) o acesso de um ativo do ponto de vista físico é o uso que se faz de determinado recurso, sendo que o acesso físico é representado pelo acesso ao meio de registro ou suporte que abriga as informações. Desta forma, caso as informações estejam registradas em papel, não há possibilidade de separar o acesso físico do acesso lógico, já que não há como separar os dois tipos de acesso.

Ainda conforme CARUSO; STEFFEN, ainda que o acesso físico seja mais perceptível e sujeito a mais riscos do que o acesso lógico o controle é mais difícil, tendo em vista que depende muito mais da intervenção humana.

A segurança física compreende a segurança de acesso não autorizado e também a segurança ambiental que visa prevenir danos por causas naturais (como incêndios, inundações, umidade, ameaças biológicas como fungos, traças etc.). Por este aspecto DIAS (2000, p. 103) propõe uma "lista de verificações" primeiramente para a segurança de acesso físico que compreende: controles de identificação afim de distinguir um funcionário de um visitante; devolução de bens da organização quando o funcionário é desligado; controle da entrada e saída de equipamentos; vigilância 24 horas em todos os dias; não instalação em áreas públicas equipamentos que possam ser acessar a rede interna; incentivar o bloqueio do teclado, a guarda de documentos confidenciais, disquetes, *backup* e *laptops* em armários com chave; uso de controle de acesso físico como fechaduras, câmeras de vídeo e alarmes; proteção das linhas telefônicas contra "grampos"; restrição do acesso a informações que possam manipular dados confidenciais; instituir uma política de descartes de informações.

No que se refere aos controles ambientais alguns dos cuidados apresentados dizem respeito a: instituição de procedimentos que visem a prevenção contra incêndio conforme normas da Associação Brasileira de Normas Técnicas (ABNT); uso de materiais resistentes ao fogo na construção do prédio e instalação de pára-raios; proibir o consumo de comidas e bebidas próximos aos equipamentos; vistoriar regularmente

dispositivos de combate a incêndios; realizar manutenção periódica dos possíveis focos de problemas com água; instalação de dispositivos que minimizem os efeitos de cortes, picos e flutuações de energia; controlar temperatura, umidade e ventilação do ambiente computacional.

Através desta análise identifica-se que a sobrevivência de muitas organizações esta inteiramente atrelada à segurança física, sendo que esta indiretamente protege os recursos lógicos, como programas e dados.

4.2.3.3 Segurança lógica

Neste aspecto de controle de segurança tem-se um fator agravante que é que o conceito de acesso lógico estar mais voltado a informática, no entanto os conceitos a serem apresentados nesta seção podem ser aplicados aos demais ambientes conforme a proposta de CARUSO; STEFFEN (1999, p. 26) que faz o seguinte apontamento:

> "Ainda que o conceito de acesso lógico esteja mais associado à informática, ele é também aplicável a informações armazenadas em outros ambientes. Dentro de uma organização existem muitas informações sensíveis que não estão armazenadas em computadores; provavelmente, as informações mais sensíveis não são armazenadas lá. Elas normalmente estão relacionadas com as decisões estratégicas tomadas pela alta direção. Assim, mesmo que essas informações não estejam armazenadas em computadores, valem os mesmos conceitos de segurança de acesso lógico".

Dentro deste contexto como os computadores não são facilmente controlados, principalmente se estes estiverem conectados a redes locais ou de maior abrangência, faz-se necessário que medidas preventivas e procedimentos de acordo com cada ambiente sejam tomadas.

Para DIAS (2000, p. 84) os controles de acesso lógico são o conjunto de medidas e procedimentos que as organizações adotam ou que são intrínsecos aos *softwares* utilizados, com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizado realizado por usuários ou outros programas.

No que se refere aos controles de aspecto lógico as autoras DIAS (2000, p. 84-85) e BEAL (2005, p. 112-113) apresentam os recursos e informações

normalmente sujeitos a controles de acesso, sendo eles:

a) programas fonte e objeto: o acesso não autorizado ao código fonte dos aplicativos pode ser usado para alterar suas funções e a lógica do programa com a finalidade de fraude ou sabotagens;
b) arquivos de dados: bases de dados, arquivos ou transações de banco de dados precisam ser protegidos para evitar que dados sejam apagados ou alterados sem autorização;
c) sistema operacional e utilitários: o acesso a todos os componentes do sistema operacional e também editores, compiladores, *softwares* de manutenção, monitoração e diagnóstico necessitam ter seu acesso restrito, já que essas ferramentas podem ser usadas para alterar arquivos de dados, aplicativos e arquivos de configuração do sistema, sendo estes alvos muito visados, já que a configuração é o ponto chave de qualquer esquema de segurança;
d) arquivos de senha: a proteção inadequada aos arquivos que armazenam as senhas pode permitir o acesso de um usuário não autorizado a informações privilegiadas comprometendo todo o sistema;
e) arquivos de log: são fontes de informação para auditorias e análises de quebra de segurança por registrarem as ações dos usuários, incluindo o tipo de operação realizada e quem fez o acesso.

Com o intuito de garantir o correto funcionamento deste tipo de segurança o aspecto humano também é imprescindível, por isto conscientizar o usuário é fator crucial e fundamental para que este controle seja eficaz.

4.2.3.3.1 Controles de segurança baseados no aspecto lógico

Visando garantir um nível de risco adequado a segurança da informação, existem mecanismos de controle de segurança que são desenvolvidos com base na

análise de riscos ou através das recomendações das normas de segurança (como a NBR ISO/IEC[4] 17799 a ser abordada na próxima seção). Existem mecanismos aplicáveis a segurança física, humana e lógica.

Devido, atualmente a maior parte das informações ser digitalizada, o aspecto lógico receberá uma atenção especial. No entanto, como já comentado, os demais aspectos da segurança não são de menor importância. No que se refere aos controles lógicos os mecanismos mais comumente utilizados são:

a) assinatura digital: a assinatura digital é uma modalidade da assinatura eletrônica que tem como principal propósito garantir o sigilo, integridade e autenticidade dos documentos eletrônicos e documentos envolvidos em transações eletrônicas. É constituído de um procedimento de assinatura propriamente dita e outra de verificação da assinatura, o que permite a proteção das partes na comunicação quanto a violação da autenticidade e a integridade da mensagem. (DIAS, 2000, p. 74);
b) sistemas de detecção de intruso (IDS[5]): este sistema analisa os pacotes que trafegam na rede e faz a comparação com assinaturas já prontas de ataques, identificando qualquer tipo de anomalia ou ataque que possa vir a ocorrer na rede/ computador. (CAFFARO, 2001);
c) criptografia: através do uso de algoritmos (seqüência de passos para o embaralhamento), dos dados a serem protegidos e de uma chave (conjunto de bits), transforma-se textos ou dados abertos em códigos ilegíveis. A chave existe para embaralhar o texto e, através do conhecimento dela, conseguir recuperar o texto original (FLEURY, 2001);

---

[4] IEC – (*International Electrotechnical Commission*): organização que trabalha desenvolvendo, sugerindo e definindo padrões para protocolos de rede em conjunto com a ISO.

ISO – (*International Organization for Standardization*): organização internacional que trabalha desenvolvendo, sugerindo e definindo padrões.

NBR – Norma Brasileira.

[5] IDS - *Intrusion Detection System*.

d) *firewall*: analisa o fluxo de pacotes de dados, filtragens e registros dentro da rede, representa uma parede de fogo que faz a execução de comandos de filtros que foram especificados com base no compartilhamento, acesso e proteção exigidos pela rede e pelas informações disponíveis através dela. (SÊMOLA, 2003, p.120);

e) *backup*: trata-se de uma cópia da informação contida em um banco de dados local ou remoto, sendo, na prática, uma réplica dos dados originais atuais, guardados em um outro local seguro. As cópias de segurança são fundamentais em qualquer sistema. No caso de uma pane mais séria no sistema, somente estas podem devolver os arquivos do usuário de volta, através da sua recuperação (*recovery*), desta forma os backup's permitem à organização ou usuário, a segurança de que, se uma falha grave ocorrer nos computadores ou nos servidores, esta não implicará a perda total da informação contida no sistema (PINHEIRO, 2004);

f) certificado digital: o certificado digital é um documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular. A função principal do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública (de uso compartilhado) (ITI, 2006);

g) antivírus: os antivírus são programas que procuram detectar e, então, anular ou remover os vírus de computador, para que estes cumpram seu papel precisam ser executados e atualizados regularmente. (FONTES, 2006, p. 67).

4.3 NORMAS TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO

As normas e padrões técnicos são um referencial importante para estabelecer a qualidade de determinado processo, quando estes são desenvolvidos em

conformidade com padrões e normas asseguram-se garantias maiores de eficiência e confiabilidade. No que se refere à segurança da informação existem várias referências internacionais, entre as quais são citadas as normas mais utilizadas nas organizações, no entanto, a ênfase maior ocorre na norma brasileira NBR ISO/IEC 17799 que é advinda da norma internacional BS 7799 (*British Standart* 7799) a ser analisada na próxima seção.

Entre as normas mais conhecidas e utilizadas dentro das organizações temos (BEAL, 2005, p.30-36):

a) ITIL (*It infrastructure library*): conjunto de documentos desenvolvido pelo gobverno do Reino Unido visando o registro das melhores práticas na área de gestão de serviços de TI;
b) COBIT (*Control objetives for information and related technology*): conjunto de diretrizes para a gestão e auditoria de processos de controles de TI, desenvolvido pela *Information System Audit and Control Association* (ISAC) e pelo *IT Governance Institute*;
c) ISO Guide 73: (*Risk management – vocabulary – guidelines for use in standards*), publicada em 2002, define 29 termos da Gestão de Riscos[6];
d) ISO/ IEC 13335: (*Guidelines for the management of IT security*) é um conjunto de diretrizes de gestão de segurança voltadas especificamente para a tecnologia da informação.

4.3.1 Norma BS 7799 e NBR ISO/IEC 17799

Devido ao crescente número de variáveis envolvidas com a segurança da informação a comunidade britânica desenvolveu a Norma BS 7799, que teve a sua

[6] Segundo MANFIO (2003), "gestão de risco significa avaliar o risco envolvido em cada operação".

primeira publicação em 2000. Esta norma reúne as melhores práticas para o gerenciamento da segurança da informação. Conforme DRAGO (2004, p. 25), "o objetivo principal desta norma é assegurar a continuidade e diminuir o dano empresarial, prevenindo e minimizando o impacto de incidentes relacionados à segurança". O padrão BS 7799 divide-se em duas partes, sendo que a primeira parte (BS 7799-1) corresponde um código de práticas para a gestão da segurança da informação e a segunda parte (BS 7799-2) é voltada para a definição de um sistema de gestão de segurança.

Em conseqüência da criação da norma a ISO desenvolveu uma versão do padrão chamado ISO 17799:2000. Desta forma, a ABNT operando juntamente com a ISO disponibilizou um projeto na versão brasileira surgindo então a NBR ISO/IEC 17799 (Tecnologia da Informação – Códigos de prática para a gestão da segurança da informação).

A norma nacional de segurança de informações ISO/IEC 17799 teve a sua primeira versão publicada no Brasil em 2001 e esta se divide-se em dez áreas de controle. Desta forma, é de vasta abrangência conforme é identificado nos aspectos abordados pela norma conforme consta a seguir (NBR ISO/IEC 17799, p. 2-51):

a) política de segurança: orientações e apoio para a implementação e manutenção de uma política de segurança;
b) segurança organizacional: recomendações para prover o estabelecimento de uma infra-estrutura para planejar e controlar a segurança da informação na organização;
c) classificação e controle dos ativos de informação: orientações sobre a realização de inventários dos ativos informacionais e atribuição de responsabilidades para manter a proteção adequada;
d) segurança em pessoas: orientações para a redução de riscos de erro humano, roubo fraude e uso indevido de instalações;
e) segurança física e do ambiente: orientações para prevenir acesso não autorizado, dano ou interferência dos recursos e instalações de

processamento de informações;

f) gerenciamento das operações e comunicações: orientações com vistas a garantir a operação correta e segura dos recursos de processamento da informação;
g) controle de acesso: orientações para o monitoramento e o controle de acesso à informação;
h) desenvolvimento e manutenção de sistemas: orientações para o uso de controles de segurança em todas as etapas do processo;
i) gestão da continuidade do negócio: orientações para que a organização neutralize as interrupções as atividades do negócio e proteção dos processos críticos contra falhas ou desastres;
h) conformidade: orientações para assegurar a conformidade dos sistemas com leis, regulamentações, políticas e normas internas de segurança.

É importante destacar que as normas sofrem uma evolução natural visando a adequação a novos aspectos, CAUBI (2006), aborda as evoluções que ocorreram da norma nos últimos anos, como visto a seguir.

No ano de 2002 foi publicada a revisão da segunda parte da norma BS 7799 (BS 7799-2:2002), assim sendo em agosto de 2005 houve a publicação da segunda versão da norma brasileira ISO/IEC 17799 (NBR ISO/IEC 17799:2005).

Em conseqüência destas adequações das normas em outubro de 2005 a ISO publicou a norma ISO 27001 (ISO/IEC 27001:2005 – Tecnologia da Informação – Técnicas de segurança – Sistema de gestão da Segurança da Informação – Requisitos).

Segundo CAUBI, as mudanças mais relevantes foram a inclusão da seção de Gestão de Incidentes de Segurança da Informação contemplando os seguintes aspectos:

a) política de segurança da informação;
b) organizando a segurança da informação;
c) gestão de ativos;
d) segurança em recursos humanos;

e) segurança física e do ambiente;

f) gerenciamento das operações e comunicações;

g) controle de acessos;

h) aquisição, desenvolvimento e manutenção de sistemas de informação;

i) gestão da continuidade do negócio;

j) conformidade.

Assim como, as normas necessitam se adequar às alterações ao longo do tempo as organizações também precisam estar constantemente revisando seus sistemas de segurança, com vistas a manter o objetivo de assegurar a proteção da informação. Este é um recurso que a cada dia é mais valorizado independente da área de atuação e conseqüentemente um ativo cada vez mais visado. Portanto, adequar-se as modificações e as normas é primordial para garantir a boa "saúde organizacional".

5 METODOLOGIA

Consiste basicamente numa pesquisa de cunho exploratório, pois há poucos estudos anteriores que abordam o tema sob a ótica da Gestão da Informação, ou seja sob o foco da administração não apenas em sistemas de informações mais em qualquer ambiente que a informação esteja. Com base no levantamento da literatura pertinente gerou-se a análise de uma empresa que atua na área informacional, pretendendo assim contribuir para ampliar o conhecimento da temática tanto no âmbito de pequenas empresas que buscam informações sobre a segurança da informação, como da própria Gestão da Informação, enquanto área envolvida.

Primeiramente foi realizado um levantamento da literatura através de leituras de textos/ artigos/ livros e pesquisas na internet, nas áreas relacionadas à informação especificamente a segurança da informação e as políticas para melhor aprofundamento e conhecimento do tema em questão possibilitando assim uma análise minuciosa sobre os aspectos da segurança da informação e sobre as políticas que visam assegurar este objetivo.

Posteriormente, foi realizado estudo de caso, que, conforme FACHIN (2002, p. 42-43), é estudo intensivo que leva em consideração, principalmente, a compreensão, como um todo, do assunto investigado, e que pode ser auxiliado pela aplicação de questionários, formulários ou entrevistas. Sua principal função é a explicação sistemática dos fatos que ocorrem no contexto social e que geralmente se relacionam com multiplicidade de variáveis. Neste momento do trabalho sendo analisados aspectos da informação e da sua segurança e a importância que organização atribui a este ativo em uma empresa que basicamente desenvolve sistemas de informações geográficos, sendo escolhido este ambiente em virtude da informação propriamente dita, ser o produto final desenvolvido pela organização. Portanto, identifica-se como este tipo de organização é rico para o aprofundamento e detalhamento do tema proposto.

Para sistematizar a forma de realização deste trabalho foram seguidas as

seguintes etapas:

a) levantamento da literatura pertinente existente sobre o assunto: onde foram revisados, livros, artigos, trabalhos acadêmicos e internet;
b) realização do estudo de caso.

Os passos para realização do estudo de caso foram:

a) a escolha da empresa que presta serviços de informações;
b) identificação da empresa observando a forma de trabalho principalmente em relação a informação e o cuidado com a proteção dos recursos informacionais;
c) aplicação de entrevista semi-estruturada. Para realização da entrevista foram estabelecidos os seguintes passos:

   - elaboração do roteiro de entrevista (apêndice);

   - escolha do entrevistado; sendo escolhida para a realização da pesquisa uma pessoa em cargo gerencial e responsável pela segurança da informação dentro da organização;

   - realização da entrevista: agendado horário para realizar a pesquisa com o diretor técnico da TI.

6 ESTUDO DE CASO

Nesta seção do trabalho apresenta-se as informações obtidas durante a aplicação do instrumento de pesquisa realizado na empresa GeoPlus. Primeiro faz-se um breve relato do histórico, da estrutura e da área de negócio da organização, posteriormente descreve-se a forma que a mesma trabalha com a informação, a importância que é atribuída a esta, e os cuidados que a empresa possui com a segurança da informação e mecanismos utilizados.

6.1 A GEOPLUS GEOTECNOLOGIA E INFORMÁTICA LTDA.

A GeoPlus Geotecnologia e Informática Ltda com três anos no mercado (inaugurada em 11 junho de 2003) é uma empresa especializada em soluções de informática, especialmente para Sistemas de Informações Geográficas. Com experiência no desenvolvimento de redes, softwares, bancos de dados e aplicações WEB – internet e intranet, atende empresas ou órgãos públicos em campos diversos, tais como agronegócio, logística, saneamento, meio ambiente, gestão municipal e setor florestal.

A empresa realiza análise de soluções necessárias para as organizações, desenvolve sistemas e treinamento técnico. Valoriza a infra-estrutura e sistemas já existentes no cliente, com o objetivo de projetar soluções que atinjam os objetivos, mas que respeitem os recursos disponíveis.

Quanto à estrutura a empresa possui escritório localizado na Av. República Argentina, 50, cj 52, em Curitiba-PR. A sua equipe é formada por engenheiros cartógrafos, analistas de sistema, administradores, técnicos em cartografia, programadores e estagiários. Ao todo a empresa conta com sete colaboradores e estagiários e três diretores, totalizando dez funcionários.

Especializada em desenvolvimento de sistemas para WEB, a empresa possui servidores destinados a hospedar aplicações dos clientes, cujo principal objetivo é

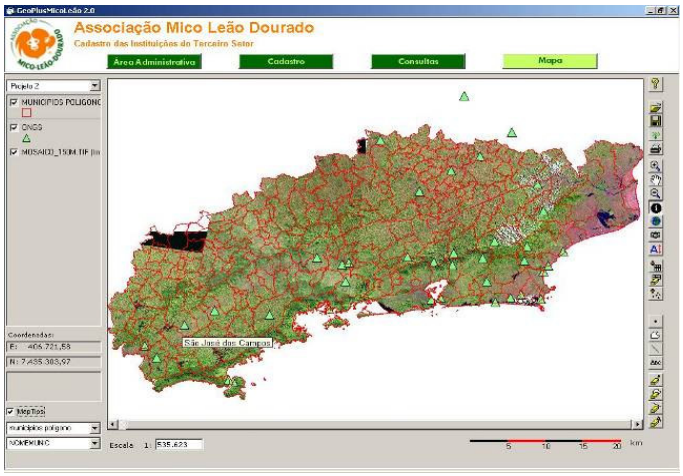
primar pela segurança, confiabilidade, disponibilidade e velocidade de acesso às informações.

Alguns clientes da empresa e respectivos projetos:

a) Fundação ABC para Assistência e Divulgação Técnica Agropecuária (desde nov/03): consultoria na elaboração do projeto da versão WEB do Banco de Dados Agronômicos e do Sistema de Informações Geográficas para o LIG, fornecendo subsídio para definição da tecnologia, softwares e linguagens de programação;

b) Associação Mico Leão Dourado/RJ (jun/03 e abr/04): desenvolvimento de sistema para cadastro institucional de ONGS na área de atuação da associação e divulgação de dados espaciais (Figura 4);

FIGURA 4 - CADASTRO INSTITUCIONAL DE ORGANIZAÇÕES NÃO GOVERNAMENTAIS (ONGS) NA ÁREA DE ATUAÇÃO DA ASSOCIAÇÃO MICO LEÃO DOURADO E DIVULGAÇÃO DE DADOS ESPACIAIS.

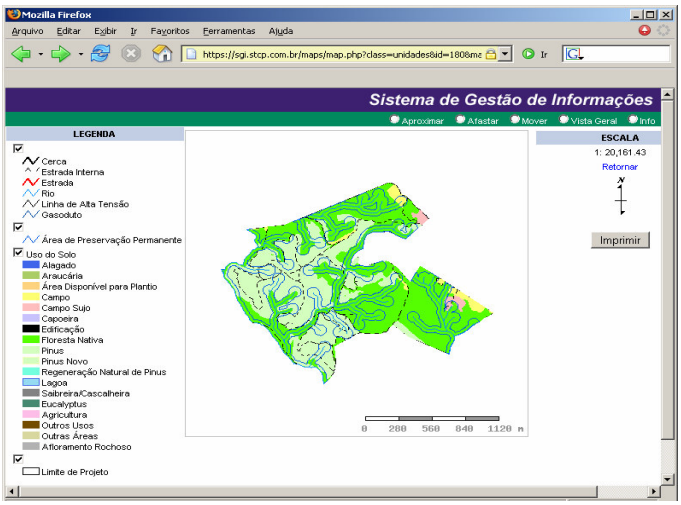


FONTE: Geoplus Geotecnologia e Informática Ltda (26 maio 2006).

c) Masisa (desde fev/06): desenvolvimento de sistema de controle das operações florestais integrado ao cadastro da base florestal existente e do sistema de informações geográficas, possibilitando aos usuários visualizar todas as informações em ambiente WEB.

d) STCP Engenharia de Projetos Ltda (desde nov/03): desenvolvimento de sistema de gestão de informações composto por documentos e mapas, desenvolvido com tecnologia WebMapping (Figura 5);

FIGURA 5 – SISTEMA DE GESTÃO DE INFORMAÇÕES.



FONTE: Geoplus Geotecnologia e Informática Ltda (26 maio 2006).

Nas próximas seções será abordado o estudo realizado na empresa através da ferramenta de pesquisa utilizada, neste caso a entrevista realizada com um dos diretores da empresa: Roberto Oliveira Santos (licenciado em matemática pela UFPR e mestrando em informática, atua na área de desenvolvimento de Sistemas Informações Geográficas e suporte a bancos de dados).

6.2 A IMPORTÂNCIA DA INFORMAÇÃO E DA SUA PROTEÇÃO

A GeoPlus é uma empresa focada fundamentalmente no uso da informação como ferramenta para desenvolvimento de suas atividades. Esta característica pode ser constatada nos projetos de consultoria, desenvolvimento e treinamento da qual a organização participa, onde a informação e/ ou a capacidade de transferência e/ ou a capacidade de armazenar a informação são utilizadas amplamente. Muitos dos

produtos entregues são compostos de documentos (mapas, memoriais descritivos, apostilas, etc) ou programas (código fonte, instaladores, etc).

Como os produtos que são desenvolvidos não possuem grande custo material, em geral é o custo dos cds e papel, o valor está ligado a informação que estas mídias contém. Portanto, a disponibilidade destas informações, sua segurança, o controle de acesso e a privacidade são fundamentais. Além disto, a empresa é contratada por diversas organizações para armazenar seus dados cartográficos e /ou seus sistemas de informação. Neste caso existe uma obrigação contratual de garantir a segurança das informações que estão sob a guarda da GeoPlus.

6.3 SEGURANÇA DAS INFORMAÇÕES

A Segurança da Informação dentro da organização é aplicada nos ambientes físico, lógico e nos aspectos humanos. No que se refere ao ambiente físico a empresa está localizada em um prédio com portaria e câmeras de segurança 24 horas nos ambientes que dão acesso ao escritório.

Referente aos aspectos humanos os funcionários recebem orientações verbais de utilização de senhas de acesso ao servidor e de e-mails para que estas sejam de difícil adivinhação, mas de fácil retenção na memória, para evitar a necessidade do registro em papel e da importância da troca periódica da senha (porém, o sistema não solicita automaticamente a troca em intervalos regulares). Os funcionários também são orientados a utilizarem antivírus e evitarem o acesso a arquivos suspeitos, mas não existe um procedimento de verificação que permita acompanhar se estas orientações estão sendo atendidas. Sendo que os acidentes com vírus e perda de arquivos são tratados de forma pontual e os usuários são alertados das melhores práticas a serem observadas no uso dos computadores e do acesso as informações da empresa.

Convém acrescentar que a empresa não possui uma norma de segurança ou política de segurança clara e formal e também não segue nenhuma norma técnica de

segurança da informação.

Sobre os aspectos lógicos a empresa possui um servidor para uso interno que está conectado a internet e um servidor de desenvolvimento fornecido por um cliente para uso exclusivo de seus sistemas. O acesso ao servidor é controlado e existem contas individuais para cada usuário. As permissões de acesso as pastas também são controlados e informações da empresa, dos projetos e dados de clientes são separados e controlados individualmente. Na próxima seção comentaremos mais sobre o aspecto lógico.

6.3.1 Mecanismos de Segurança voltados ao Aspecto Lógico

Como 95% das informações da empresa estão disponíveis digitalmente o foco maior da empresa para garantir a proteção das informações é no ambiente lógico, aonde são utilizados os seguintes mecanismos: antivírus, controle de acesso (citado anteriormente), criptografia, *backups*, certificados digitais e *firewall*, que será apresentado seu funcionamento.

O acesso remoto[7] ao servidor só pode ser feito através de uma conexão SSH[8], que utiliza a tecnologia de criptografia para garantir a segurança e privacidade das senhas e dados trafegados na rede.

Os sistemas hospedados no servidor em ambiente WEB utilizam certificados digitais SSL[9] para garantir a autenticidade e privacidade da informação. Estes certificados são adquiridos por uma empresa que segundo o entrevistado é uma representante da maior empresa de certificação digital do mundo atualmente, a Verisign. Este tipo de certificado SSL é utilizado em praticamente todos os bancos e sítios[10] de comércio eletrônico.

---

[7] Acesso a um computador através da rede, em que não é necessário estar fisicamente próximo a este.

[8] SSH - *Secure Shell*, programa que permite a execução de comandos em uma máquina remota.

[9] SSL - *Secure Socket Layer*

[10] *sites* de Internet.

Para garantir a segurança das informações armazenadas no servidor, diariamente é feito um *backup* incremental[11], que é composto por todos os arquivos que foram alterados nas últimas 24 horas. Sendo que nos finais de semana é realizado um *backup* completo do servidor para garantir uma forma rápida de retornar os dados em caso de falha do sistema e equipamentos ou falha humana.

O servidor da GeoPlus utiliza um mecanismo de *firewall* nativo do Linux chamado *iptables*. Este mecanismo permite que seja controlado o acesso do servidor tanto do lado externo (internet) quanto do lado interno (rede local). Este mecanismo é baseado em filtros e tentativas de quebrar ou contornar estas regras são armazenadas no servidor para posterior auditoria.

O acesso ao servidor é controlado e senha do *root* (administrador do sistema) é alterado a cada 2 ou 3 semanas.

A maior parte dos serviços que são executados no servidor só estão disponíveis para a rede local, ou quando estão abertos para a internet, é feita uma filtragem de quais endereços de origem podem acessar o servidor.

Os *backups* diários são salvos em DVD e guardados dentro de um armário na empresa e ficam disponíveis para todos que precisem recuperar dados dentro de um determinado período e o *backup* semanal é feito em um outro disco rígido externo ao servidor.

O serviço de *firewall* é iniciado no momento em que o servidor é ligado, garantindo desta forma que o sistema estará protegido neste aspecto. Os usuários que não estão mais ligados a empresa ou os serviços que não estão sendo mais utilizados são desativados para evitar falhas na segurança dos dados.

Atualmente não existe um sistema ou processo de verificação rotineiro destes mecanismos, ou seja, os *backups* não são testados para verificar sua consistência e os arquivos de log não são lidos diariamente. No entanto, a empresa identifica que esta é

[11] Conforme PINHEIRO (2004) este tipo de *backup* necessita que seja realizado o *backup* normal, que consiste em armazenar tudo que foi solicitado, visando o incremento da informação após a criação do *backup* normal.

uma prioridade nas atividades internas área de informática da empresa e que, portanto serão providenciados os testes destes mecanismos o mais breve possível.

7 CONSIDERAÇÕES FINAIS

No aspecto geral identificou-se através deste estudo na empresa GeoPlus a existência de uma preocupação com a segurança da informação, entretanto persiste muitas etapas a serem postas em prática. Como por exemplo, o cuidado maior com informações não digitalizadas, o cuidado mais intensivo com os aspectos humanos e também com a própria segurança física. Sendo que, algumas das melhorias na segurança envolvem um aporte financeiro maior e neste caso a empresa precisa avaliar de acordo com a disponibilidade. No caso das soluções que não envolvem grandes investimentos como aquisição de discos rígidos de *backup* e mídias de DVD são aprovadas sem maiores dificuldades. Existe uma consciência de que o valor das informações armazenadas no servidor é muito maior que o custo de soluções que aumentem a segurança do sistema.

O presente trabalho preocupou-se em mostrar a necessidade de prover segurança da informação e sistemas de informações nas organizações, identificando fatores básicos para preservar as informações e os sistemas, sem esquecer que ao se tratar de informações disponibilizadas em ambientes informatizados o cuidado com a segurança das informações precisa ser ainda maior para não comprometer a organização.

Identificou-se que as informações são vistas como algo crucial as organizações por permitirem a aquisição de conhecimento e estas são trocadas entre os mais variados sistemas. Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual. Inúmeras decisões e ações são tomadas com base nas informações manipuladas nestes sistemas automatizados. Neste contexto, toda e qualquer informação necessita ser correta, precisa e estar disponível, a fim de ser armazenada, recuperada, manipulada ou processada, além de poder ser trocada de forma segura e confiável. No entanto, ao falar de segurança da informação é preciso observar que não apenas as soluções técnicas são suficientes, os mecanismos de segurança precisa considerar além da aquisição de ferramentas de segurança, mas

também considerar o componente humano de um sistema de segurança da informação a fim de minimizar a vulnerabilidade destes.

Neste trabalho foi possível comprovar os apontamentos levantados por autores da área onde muitas empresas estão conscientes do valor da informação para a organização. No entanto, quando se fala em preservar a segurança, muito precisa ser realizado, pois apesar de terem conhecimento da necessidade da proteção, os mecanismos utilizados não são os mais adequados, pois o objetivo maior são as informações digitalizadas e as informações em papel são praticamente esquecidas, identificando-se assim o problema da "cegueira tecnológica" que atinge a maior parte das organizações atualmente.

Pode-se também traçar através do levantamento bibliográfico e do estudo de caso realizado, a necessidade da organização adotar uma política sobre a segurança e/ou norma técnica para uma gestão da segurança informacional ser mais efetiva. No entanto, este aspecto acaba não sendo priorizado na organização, onde se observa a adoção de medidas paliativas, colocando as informações em risco por desconhecimentos da política de segurança da informação por parte dos funcionários, que conforme visto anteriormente é o maior problema relacionado a segurança lógica, sendo assim, a organização acaba correndo riscos que poderia ser resolvido em curto tempo e com baixo investimento.

O problema de segurança da informação também permanece quanto abordamos o aspecto físico na organização que precisa haver um cuidado maior, tendo em vista que os armários que a empresa utiliza não possuem chaves ou cadeados, desta forma, qualquer funcionário pode ter acesso aos documentos não havendo um controle confiável de entrada e saída de documentos.

Conclui-se desta forma que as organizações ainda tem muito a se desenvolver na área de segurança informacional para redução dos riscos a um nível desejado. Em geral estas compreendem a importância deste tipo de procedimento, no entanto, estão despertando somente agora para este tipo de apontamento, o que se deve em parte a cultura ou forma equivocada de enxergar o problema, o que pode ser vital

para a organização pois a demora para investir em áreas que não consideram primordiais, mas que são a base do negócio da empresa pode levar a perda ou o comprometimento da segurança das informações. Desta forma, identifica-se a importância de despertar a conscientização do problema para que sejam tomadas medidas preventivas.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

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

CAFFARO, M. L. **Sistemas de detecção de intrusos**. 06 maio 2001. Disponível em: <http://www.securenet.com.br/artigo.php?artigo=95> Acesso em: 01 maio 2006.

CAUBIT, R. **O que é a ISO27001, afinal?**, 19 jan. 2006. Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=2&objid=432&> Acesso em: 20 abr. 2006.

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

DAVENPORT, T. H. **Ecologia da informação**: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 2001.

DIAS, C. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel, 2000.

DRAGO, I. **Segurança da informação:** estudo exploratório em organizações de grande porte do município de Curitiba. Curitiba, 2004. 71 f. Monografia (Graduação em Gestão da Informação) – Setor de Ciências Sociais Aplicadas,Universidade Federal do Paraná.

FACHIN, O. **Fundamentos de metodologia**. 3. ed. São Paulo: Saraiva, 2002.

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

FLEURY, A. **Criptografia: uma questão de segurança nacional**. 18 set. 2001. Disponível em: <http://www.securenet.com.br/artigo.php?artigo=101> Acesso em 01 maio. 2006.

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

GEOPLUS: Geotecnologia e informática Ltda. Disponível em:<http://www.geoplus.com.br> Acesso em 14 maio 2006.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO – ITI. **Certificado digital**. Disponível em: <http://www.iti.br/twiki/bin/view/Main/Principal> Acesso em 01 maio 2006.

MANFIO, F. **A prática atual de gerenciamento de riscos**. 2003. Disponível em: <http://www.equifax.com.br/cmn_mat.asp?MAT_COD=64&MAT_ANO=2003> Acesso em: 17 jun. 2006.

MCGARRY, K. **O contexto dinâmico da informação.** Brasília: Briquet de Lemos, 1999.

MCGEE, J. V.; PRUSAK, L. **Gerenciamento estratégico da informação**: aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. 12. ed. Rio de Janeiro: Campus, 1994. (Série Gerenciamento da Informação).

OLIVEIRA, S. de. **As tríplices da segurança da informação,** 14 mar. 2005. Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=2&objid=432&> Acesso em: 15 jun. 2006.

PINHEIRO, J. M. S. **Backup e Recovery. 07 jul. 2004.** Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_backup_e_recovery.php> Acesso em: 04 maio 2006.

SÊMOLA, M. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Campus, 2003.

SHAPIRO, C. VARIAN, H. R. **A economia da informação**: como os princípios economicos se aplicam à era da Internet. 4. ed. Rio de Janeiro: Campus, 2000.

SILVA. A. F. da. **O impacto político, financeiro, de desempenho da implantação de políticas e métodos de segurança**. 2004. Disponível em:<http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=84> Acesso em: 07 jun. 2005.

STAIR, R. H. **Principios de sistemas de informação**: uma abordagem gerencial. 2. ed. Rio de Janeiro: LTC, 1998.

TEXEIRA, H. de A. Pesquisa de mercado. **Pespect. cienc. inf.**, Belo Horizonte, v. 2, n. 1, p. 223 – 234, jul./dez. 1997.

TURBAN, E. et al. **Tecnologia da informação para gestão**. 3. ed. São Paulo: Boolkmam, 2004.

VAITSMAN, H. S. **Inteligência empresarial**: atacando e defendendo. Rio de Janeiro: Interciência, 2001.

APÊNDICE

APÊNDICE – ROTEIRO DE ENTREVISTA (QUESTÕES)

a) Qual o papel que a informação representa para a organização? Esta é vista como um ativo importante para a área de negócio em que atua?
b) Existe uma preocupação em proteger a informação?
c) É adotada alguma norma de segurança da informação ou uma diretriz interna?
d) Caso da existência da norma. Esta é do conhecimento de todos, houve um trabalho de conscientização ou mesmo de treinamento dos funcionários?
e) A segurança da informação dentro da organização contempla informações digitalizadas e no ambiente físico?
f) Existe cuidado que são adotados para garantir a segurança física, lógica e também com vistas nos aspectos humanos (por exemplo, proteger a informação contra erros cometidos por usuários autorizados)?
g) Quais mecanismos de segurança são utilizados pela organização (Exemplo: *firewall, backup's*, controles de acesso,...)?
h) Como estes mecanismos funcionam dentro da organização garantindo que as informações estão protegidas?
i) Como são avaliados (testados) os sistemas existentes? Identifica-se que os sistemas utilizados são os necessários para a garantia da segurança da informação?
j) Existe uma atenção da organização visando a manutenção dos sistemas de segurança com o objetivo de manter estes atualizados ou mesmo a uma preocupação em investir mais nesta área?