Área Temática: Empreendedorismo e Inovação

Obtenção de Conhecimento Necessário a Inovações: Benefícios e Malefícios de Processos de Gestão da Segurança da Informação

AUTORES
JOSE GERALDO PEREIRA BARBOSA
Universidade Estacio de Sá
jose.geraldo@estacio.br

FABIO DA SILVA EIRAS
UNIVERSIDADE ESTÁCIO DE SÁ - UNESA
fabiosee@hotmail.com

Resumo:
A pesquisa teve como objetivo descrever como os processos de segurança da informação da empresa INPA influenciaram a obtenção de conhecimento para duas inovações em processo fabril decorrentes da incorporação da prensa *Speed Size* no processo fabril e da obtenção da certificação FSC - *Forest Stewardship Council*. O estudo foi conduzido por meio de uma pesquisa de campo de finalidade descritiva com utilização de entrevistas, narrativas, observação direta e análise temática para tratamento e analise dos resultados. Verificou-se a presença de 5 instrumentos de segurança física e lógica: “Confidencialidade”, “Controle geral de proteção”, “Antivírus”, “Backups” e “Instrumentos de segurança para instalações”. Os resultados da análise temática das narrativas do desenvolvimento das inovações sugerem que os instrumentos acima mencionados não interferiram de forma negativa na obtenção de conhecimento. Verificou-se também que os formatos de obtenção de conhecimento que contribuíram para as inovações foram: “Tecnologias embutidas em máquinas, equipamentos e softwares”, “Consultorias especializadas” e “Programas de qualidade, treinamento de recursos humanos e aprendizado organizacional cumulativo”. Como bloqueio à obtenção de conhecimento foi identificado apenas a “falta de capacidade de absorção”, que se caracteriza como um bloqueio genérico à transferência de conhecimento e não ligado à gestão de segurança de informação propriamente dita.

Abstract:
The research aimed to describe how the processes of information security of the company INPA influenced the acquisition of knowledge for two innovations in the manufacturing process resulting from the incorporation of the machine Speed Size in the manufacturing process and attainment of the certification seal by FSC - Forest Stewardship Council. The study was conducted through a field survey for descriptive purposes with the use of interviews, narratives, direct observation and thematic analysis for treatment and analysis of results. It was observed the presence of five instruments of physical and logical security: "Confidentiality", "General Protection Control", "Antivirus", "Backups" and "Instrument for Facilities Security" The results of the thematic analysis of narratives of the development of innovations suggest that the instruments mentioned above did not interfere negatively in obtaining knowledge. It was also noted that the formats of obtaining knowledge that contributed to the innovations were "Embedded Technology in Machinery, Equipment and Software", "Specialized Consultancies" and "Quality Programs, Training of Human Resources and Cumulative Organizational Learning". As a blockage to the acquisition of knowledge was only identified the "Lack of Absorptive Capacity," which is characterized as a

generic blockage to the transfer of knowledge and not connected to the management of information security itself.

Palavras-chave:
Inovação. Segurança da Informação. Conhecimento.

1. INTRODUÇÃO

Ao enfatizarem importância do conhecimento para o processo de inovação, Tidd, Bessant e Pavit (2001) apontam para a necessidade das empresas focarem na questão da obtenção e transferência de conhecimento que possa alimentar o processo de inovação. Segundo alguns estudiosos do tema (LASTRES e CASSIOLATO, 2005; TIDD et al. 2001; TIGRE, 2006), qualquer tentativa de promover a inovação em uma organização passa pela necessidade de fomentar a interação entre as pessoas e gerir o conhecimento na empresa.

Com a crescente evolução dos sistemas de informação, cada vez mais as empresas tem investido em sofisticados *softwares* de gestão, como tecnologias de *EDI* (*Electronic Data Interchange*), sistemas em ambiente web (rede mundial) e sofisticados bancos de dados demandando equipamentos de alta capacidade e tecnologia. Com isso, se faz necessária a adoção de normas de Segurança da Informação como uma das formas de garantir a continuidade do negócio e integridade de todas as informações armazenadas em seus bancos de dados, nos seus aspectos físicos, lógicos e humanos, bem como a regulação dos acessos às informações, definindo quem irá acessar, onde e quando.

A informação deve ser considerada um ativo da empresa e seu correto gerenciamento é fundamental para o sucesso de qualquer organização. Devido à sua importância nos negócios, a informação precisa ser protegida, de forma que acessos não autorizados, alterações indevidas e indisponibilidades sejam evitadas (CACIATO, 2004).

Mas como obter e transferir conhecimento necessário ao desenvolvimento de inovação em ambientes onde operam processos de gestão da segurança da informação? A questão se justifica porque apesar de necessários para assegurar a integridade e disponibilidade das informações, os procedimento de segurança da informação podem em certa medida restringir ou dificultar o acesso a conhecimento necessário a inovações.

Assim, este estudo teve como objetivo descrever, na empresa INPA - Indústria de Embalagens Santana S/A, como a gestão de segurança da informação interfere no processo de obtenção e transferência de conhecimento necessário às inovações. Para essa finalidade, foram identificadas: as inovações desenvolvidas pela empresa nos últimos 5 anos; as fontes e formas de obtenção e transferência de conhecimento para o desenvolvimento dessas inovações; e os procedimentos e instrumentos de gestão de segurança da informação utilizados pela empresa pesquisada.

2. REFERENCIAL TEÓRICO

2.1. O CONHECIMENTO COMO PRINCIPAL INSUMO DE INOVAÇÕES

Quando as organizações inovam, elas não só processam informações, de fora para dentro, com o intuito de resolver os problemas existentes e se adaptar ao ambiente em transformação, mas criam novos conhecimentos e informações, de dentro para fora, a fim de redefinir tanto os problemas quanto as soluções e, assim recriar seu meio. (NONAKA e TAKEUCHI 1997) Conforme Machado et al. (p. 2, 2008), o progresso econômico acontece principalmente dirigido pelos avanços do conhecimento e aplicação da inovação, influenciando diretamente no desenvolvimento de nações.

Para Tsujiguchi e Camara (p. 3, 2008), as possibilidades de conhecimento não só aumentam a eficiência produtiva, mas colaboram para a ampliação da variedade de novos produtos, processos e serviços e até a geração de novos setores e demandas. Nonaka e Takeuchi (1997) argumentam que a criação do conhecimento organizacional é a chave para as formas características com que as empresas japonesas inovam.

Sobre conhecimento, Davenport e Prusak (1998) afirmam que a única vantagem competitiva sustentável de uma empresa é aquilo que ela coletivamente sabe, aliado à eficiência com que ela usa esse conhecimento e a prontidão com que ela o adquire. Anand et

al. (2002, p.58), definem conhecimento organizacional como qualquer informação, crença ou habilidade que a organização possa aplicar às suas atividades.

Por criação de conhecimento organizacional Nonaka e Takeuchi (1997, p. 1) entendem a capacidade de uma empresa de criar novo conhecimento, difundi-lo na organização como um todo e incorporá-lo a produtos, serviços e sistemas. Rosiri e Palmirano (2003) mencionam que o conhecimento, nas organizações, se encontra não apenas nos documentos, bases de dados e sistemas de informação, mas também nos processos de negócios, nas práticas dos grupos e na experiência acumulada pelas pessoas. Segundo Tigre (2006), as empresas inovadoras geralmente recorrem a uma combinação de diferentes fontes de tecnologia, informação e conhecimento tanto de origem interna quanto externa.

2.2. FONTES DE OBTENÇÃO DE CONHECIMENTO

No atual contexto sócio-econômico, as organizações se deparam com o fato de que o conhecimento evolui constantemente, sendo assim necessária a busca por novas fontes de obtenção de conhecimento, inclusive para além das fronteiras organizacionais. Conseqüentemente, grandes quantidades de conhecimento são adquiridas de fontes externas, quando as organizações estendem seus vínculos a organizações e indivíduos de fora (ANAND et al. 2002). Seguindo o mesmo pensamento acima, Tsujiguchi e Camara (2008), afirmam que o processo inovativo não acontece isoladamente, ou seja, na busca por inovações as firmas procuram estabelecer relações e interagir com outras organizações, pois podem utilizar informações e conhecimentos que se localizam também fora de seu ambiente interno.

Imbuzeiro e Marsíglia (2009), afirmam que a obtenção de conhecimento refere-se às informações e dados adquiridos do ambiente interno e externo por meio das pessoas, e que resultam em conhecimento. O processo de inovação é, portanto, um processo interativo realizado com a participação de variados agentes sócio-econômicos que possuem diferentes tipos de informações e conhecimentos que acabam sendo incorporados em produtos, processos. É o caso por exemplo das informações aos quais as organizações podem ter acesso, utilizando seus funcionários, seus vínculos formais e informais com agentes externos, tais como clientes, organizações parceiras e funcionários de outras organizações. (LEMOS, 2001).

Sobre as fontes de obtenção de conhecimento necessárias a inovação, Tigre (2006) destaca que, as empresas inovadoras geralmente recorrem a uma combinação de diferentes fontes de tecnologia, informação e conhecimento tanto de origem interna quanto externa. Segundo o autor, as fontes internas de inovação envolvem tanto as atividades explicitamente voltadas para o desenvolvimento de produtos e processos quanto à obtenção de melhorias incrementais por meio de programas de qualidade, treinamento de recursos humanos e aprendizado organizacional. As fontes externas, por sua vez, envolvem: a aquisição de informações codificadas, a exemplo de livros e revistas técnicas, manuais, software, vídeos etc.; consultorias especializadas; obtenção de licenças de fabricação de produtos; tecnologias embutidas em máquinas e equipamentos. (TIGRE, 2006).

Para Nonaka e Takeuchi (1997), existem dois tipos de conhecimento: o explícito, contido nos manuais e normas de praxe, e o tácito, que só se obtém pela experiência, e que só se comunica indiretamente por meio de aprendizado e com o auxílio de metáforas e analogias. O conhecimento codificado é apresentado sob a forma de informação, através de manuais, livros, revistas técnicas, *software*, fórmulas matemáticas, documentos de patentes, bancos de dados etc. (TIGRE, 2006) Já o conhecimento tácito, envolve habilidades e experiências pessoais ou de grupo, apresentando um caráter mais subjetivo, sendo de difícil mensuração e transmissão, o que dificulta a transformação do mesmo em informação. (TIGRE, 2006). Para Anand et al. (2002), os formatos mais adequados à obtenção de conhecimento dependem de

sua natureza, ou seja – explícito versus tácito – e do volume de conhecimento que se está buscando

2.3. FORMAS DE TRANSFERÊNCIA DE CONHECIMENTO

Para Davenport e Prusak (1998), a transferência do conhecimento ocorre de maneira permanente e espontânea nas organizações. Porém, para Simões (2008), a transferência espontânea ocorre de maneira fragmentada e localizada. O autor ainda enfatiza que um dos principais objetivos da gestão do conhecimento é atribuir certo nível de formalização à transferência de conhecimento e, dessa forma, desenvolver estratégias específicas para incentivar a transferência de forma espontânea. Ainda de acordo com Simões (2008), muitos autores continuam direcionando a transferência do conhecimento para a área da informática e dos sistemas de informação. Embora tal comportamento não seja totalmente incorreto, pois existem diversas tecnologias de informação que podem ajudar a transferência do conhecimento, existem outras variáveis que podem influenciar, de forma positiva ou negativa, essa mesma transferência.

"As organizações contratam freqüentemente pessoas inteligentes e então as isolam ou as sobrecarregam com tarefas que as deixam com pouco tempo para pensar e nenhum para conversar" (DAVENPORT e PRUSAK, 1998, p. 88). Dessa forma, o sucesso da transferência do conhecimento, segundo Silva e Neves (2003, p. 193) apud Simões (2008, p. 2), é determinado pelos "valores, normas e padrões de comportamento que incorporam a cultura organizacional mais do que pelas ferramentas proporcionadas pela tecnologia, embora estas sejam essenciais, em particular no caso de organizações grandes e complexas".

A transferência de conhecimento, segundo Davenport e Prusak (1998) envolve duas ações, transmissão (enviando ou apresentando o conhecimento a um potencial receptor) e absorção pelo receptor. Se o conhecimento não for absorvido, não pode ser considerado como transferido. Tornar o conhecimento meramente disponível, não é sinônimo de transferência. O acesso é necessário, mas não é nenhum meio suficiente para assegurar que aquele conhecimento será usado. O objetivo da transferência de conhecimento é melhorar a habilidade de uma organização para fazer coisas e então aumentar o seu valor. Segundo o autor, a transferência do conhecimento pode ser feita por meio dos mecanismos por ele denominados de transferência por informação e transferência por tradição. No Quadro 1 apresenta-se uma comparação entre esses mecanismos.

Ainda hoje a transferência por tradição parece continuar sendo a melhor forma de transferência de conhecimento. O aprendizado prático é a melhor maneira de se aprender no ambiente de trabalho. Pessoas aprendem principalmente seguindo os exemplos de outras, praticando e conversando. Elas não gostam de ler e interpretar instruções. "Portanto, a competência é transferida com mais eficácia quando o receptor participa do processo" (SVEIBY, 1998, p.52).

Quadro 1 - A transferência de conhecimento pela informação e pela tradição

INFORMAÇÃO	TRADIÇÃO
Transfere informações articuladas	Transfere capacidades articuladas e não articuladas
Independente do indivíduo	Dependente e independente
Estática	Dinâmica
Rápida	Lenta
Codificada	Não codificada
Fácil distribuição em massa	Difícil distribuição em massa

Davenport (1998, p. 108) assegura que "[...] a transferência espontânea e não estruturada do conhecimento é vital para o sucesso de uma empresa". O termo gestão do

conhecimento implica a transferência formalizada, embora um de seus elementos essenciais seja o desenvolvimento de estratégias específicas estimuladoras das trocas espontâneas. O Quadro 2 apresenta alguns fatores culturais que inibem a transferência do conhecimento. Pela análise desse quadro, percebem-se os elementos de atrito, geralmente originados em diferenças culturais e de *status* entre indivíduos e também algumas sugestões para superação desses obstáculos, com a finalidade de se criar uma cultura que favoreça a transferência e crescimento do conhecimento dentro da organização.

Quadro 2 - Fatores culturais inibidores da transferência do conhecimento

ATRITO	SOLUÇÕES POSSÍVEIS
Falta de confiança mútua	Construir relacionamentos e confiança mútua através de reuniões face a face
Diferentes culturas, vocabulários e quadros de referência.	Estabelece um consenso através de educação, discussão, publicação, trabalha em equipe e rodízio de funções.
Falta de tempo e de locais e encontro; idéia estreita de trabalho produtivo.	Criar tempo e locais para a transferência de conhecimento: feiras, salas de bate-papo, relatos de conferências.
Status e recompensas vão para os possuidores de conhecimento	Avaliar o desempenho e oferecer incentivos baseados no compartilhamento
Falta de capacidade de absorção pelos recipientes	Educar funcionários para a flexibilidade; propiciar tempo para aprendizado; basear as contratações na abertura a idéias.
Crença de que o conhecimento é prerrogativa de determinados grupos, "síndrome do não inventado aqui".	Estimular a aproximação não hierárquica do conhecimento; a qualidade das idéias é mais importante do que o cargo da fonte.
Intolerância com erros ou necessidade de ajuda	Aceitar e recompensar erros criativos e colaboração; não há perda de *status* por não se saber tudo.

Fonte: Davenport (1998)

2.4. SEGURANÇA DA INFORMAÇÃO

A informação, de acordo com Barbaes et al. (2007), nem sempre é tratada de maneira adequada pelos gestores, principalmente em pequenas empresas que geralmente ocupam todo seu tempo procurando sobreviver no mercado. De acordo com Sêmola (2003), a implementação da segurança da informação é norteada por três princípios básicos. São eles:

- Confidencialidade – toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas;
- Integridade – toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais;
- Disponibilidade – toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

As medidas de segurança que visam preservar esses três princípios podem ser classificadas, em função da maneira como abordam as ameaças, em duas grandes categorias definidas por Silva et al. (2003) como:

- Prevenção: é o conjunto das medidas que visam reduzir a probabilidade de concretização das ameaças existentes;
- Proteção: é o conjunto das medidas que visa dotar os sistemas de informação com capacidade de inspeção, detecção, reação e reflexo, permitindo reduzir e limitar o impacto das ameaças quando estas se concretizam.

Para Caciato (2004), a informação deve ser considerada um ativo da empresa e seu correto gerenciamento é fundamental para o sucesso de qualquer organização. Devido à sua importância nos negócios, a informação precisa ser protegida, de forma que acessos não autorizados, alterações indevidas e indisponibilidades sejam evitadas.

Carvalho (2008) afirma que uma vez identificados os riscos a que as informações estão expostas deve-se imediatamente iniciar a implementação de processos de segurança física e lógica, com o intuito de alcançar um nível aceitável de segurança. O sistema de proteção da informação deve considerar aspectos ligados a: segurança física da informação, segurança lógica, segurança das relações financeiras, garantia da reputação e imagem da organização, aspectos legais, comportamento dos funcionários, ou seja, deve abranger os ativos tangíveis e intangíveis de uma organização. (PELTIER, 2001).

2.4.1. Política de Segurança da Informação

Para que todos os esforços e investimentos em tecnologia sejam bem sucedidos, é essencial que as empresas assimilem novas regras de segurança, transformando-as em parte integrante da sua cultura, incorporando-as às atividades de seu cotidiano com naturalidade.

> Neste sentido, algumas instituições costumam desenvolver uma política de segurança corporativa bastante rígida, com controles e processos rigorosos, diretrizes e orientações claras, objetivas e adequadas que ajudam a minimizar os riscos e reduzir o impacto sobre o negócio (SÊMOLA,2003, p. 22)

Conforme Gonçalves (2002 apud Moraes et al. 2007), as Políticas de SI (Segurança da Informação) são um conjunto de diretrizes, regras bem determinadas e práticas, que regulam como uma organização deve gerenciar, proteger e distribuir suas informações e recursos. Para Moraes et. al. (2007, p. 3), a Política de SI e outros controles de segurança tem a finalidade de procurar garantir que a SI seja mantida, e que os dados armazenados nos computadores sejam confiáveis e disponíveis.

Ainda segundo Moraes et al. (2007, p. 3), o objetivo da criação de Políticas de SI é o de prover uma orientação e uma base de práticas para a SI. Assim, o conjunto de Políticas de SI de qualquer organização deverá incluir:

- Definição de SI, resumo de metas e escopo e a importância da segurança, como um mecanismo que capacita o compartilhamento da informação;
- Declaração do comprometimento da alta direção, apoiando as metas e princípios da SI;
- Estrutura para estabelecer os objetivos de controles, incluindo a estrutura de análise, avaliação e gerenciamento de risco;
- Explicação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização, por exemplo:
    - Conformidade com a legislação e cláusulas contratuais;
    - Requisitos de conscientização e treinamento de segurança;
    - Gestão de continuidade de negócios;
    - Conseqüências das violações na política de SI;
- Definição das responsabilidades gerais e específicas na gestão da SI, incluindo o registro dos incidentes de segurança;
- Referências à documentação que possam apoiar a política.

De acordo com a NBR ISO/IEC 17799 (ABNT, 2005), a política de SI deve ser aprovada pela direção, publicada e comunicada através de toda a organização para os usuários na forma que seja relevante, acessível e compreensível para o leitor interessado. Para Moraes et al. (2007, p. 4), o principal objetivo da Política de SI é proteger as informações e os

recursos computacionais que as apóiam, sendo essencial que ela estabeleça normas para *backup* de dados.

2.4.2. Gestão da Segurança da Informação

2.4.2.1 Tipos de Controles de Proteção

Segundo Turban et al. (2004, p.546), os controles de proteção são divididos em duas categorias principais: controles gerais e controles de aplicativos. Para Turban et al. (2004, p. 546), os controles gerais são implantados para proteger o sistema, independentemente do aplicativo específico.

As principais categorias de controles gerais são: controles físicos, controle de acesso, controle de segurança de dados, controles de comunicação (redes) e controle administrativos. (TURBAN et al. 2004, p.546). Sobre controles físicos Turban et al. (2004, p. 546), destacam que:

> "a segurança física refere-se à proteção das instalações e dos recursos computacionais. Isso inclui proteger a propriedade física, bem como os computadores, os centros de dados, *software*, manuais e redes. A segurança física é a primeira linha de defesa e normalmente a mais fácil de construir. Fornece proteção contra a maioria dos perigos naturais, bem contra riscos humanos. Uma segurança física adequada poderá incluir diversos controles, tais como: Desenho adequado do centro de dados, escudo contra campos eletromagnéticos, sistema de desligamento emergencial de energia elétrica, detecção e extinção de incêndios, bombas de água, entre outros."

Sobre controle de acesso, Turban et al. (2004, p. 546), o define como a restrição imposta a usuários não autorizados de acessar uma parte ou toda informação. Tais controles podem utilizar sistemas de identificação biométrica, como por exemplo, fotografia do rosto, impressões digitais, geometria da mão, leitura da íris, voz, assinatura entre outros. Também podem utilizar controles de web (internet), como por exemplo, autenticação, podendo essa ser biométrica, criptografia, testadores de cabos, *firewalls* e proteção contra vírus.

A respeito de controles de segurança de dados Turban et al. (2004, p. 548), relatam que:

> "o controle de acesso se preocupa com a proteção dos dados contra sua revelação acidental ou intencional para pessoas não autorizadas, ou com modificações ou destruição não autorizada. As funções de segurança de dados são implementadas através de sistemas operacionais, programas de controles de acesso de segurança, produtos de bancos de dados/comunicação de dados, procedimentos recomendados de *backup*/recuperação, programas de aplicativos e procedimentos de controle externo. A segurança dos dados deve tratar dos seguintes aspectos: confidencialidade, disponibilidade e integridade dos dados."

Sobre controles de comunicação, a proteção às redes é algo cada vez mais importante à medida que cresce o uso da internet, de intranets e do comércio eletrônico. (TURBAN et al. 2004, p.548) E sobre controles administrativos, enquanto os controles gerais discutidos anteriormente eram de natureza técnica, estes lidam com a definição de diretrizes e o monitoramento de seu cumprimento. (TURBAN et al. 2004, p.548). A respeito de outros controles gerais, Turban et al. (2004, p. 548), citam os controles de programação, controles de documentação e controles de desenvolvimento de sistemas.

Em relação aos controles de aplicativos, Turban et al. (2004, p. 548) relatam que os mesmos procuram proteger as instalações de computação e prover segurança para *hardware*, *software*, dados e redes. No entanto, os controles gerais não protegem o conteúdo de cada aplicativo específico. Por isso, freqüentemente são embutidos controles dentro dos aplicativos, ou seja, eles fazem parte do *software*, e normalmente são escritos sob formas de

regras de validação. Eles podem ser classificados em três categorias principais: controles de entrada, controles de processamento e controles de saídas.

Para Turban et al. (2004, p. 548), controles de entrada são desenhados para impedir a alteração ou a perda de dados. Os dados são verificados quanto a sua precisão, inteireza e consistência. Sobre controles de processamento, os autores afirmam que eles garantem que os dados sejam completamente processados, sendo válidos e precisos e que os programas sejam executados corretamente. Com relação aos controles de saída, para Turban et al. (2004, p. 549), eles garantem que os resultados do processamento sejam precisos, válidos, completos e consistentes.

2.4.2.2. Processos de Segurança Lógica

Para manter seus sistemas de informações seguros, a organização deve primeiramente definir o que proteger. Sem a existência de medidas de segurança lógica, a informação encontra-se exposta a ataques. (SILVA et al. 2003, p.79). Os autores relatam que para manutenção da segurança no tráfego de informações na rede, a criptografia de dados é um dos principais recursos.

Outro importante método de controle é o *firewall* de rede que consiste em um sistema de computador "guardião" que protege as intranets e demais redes de computadores da empresa contra ataques, funcionando como um filtro e ponto seguro de transferência para acesso à Internet e demais redes. Segundo Silva et al. (2003), o *firewall* é essencial para organizações que dependem da Internet ainda muito insegura e vulnerável. Programas antivírus são *softwares* que devidamente atualizados, protegem micro computadores contra os ataques de vírus.

2.4.2.3. Segurança quanto à integridade física das informações (*backup*)

Segundo Moraes et al. (2007, p. 2), no passado o *backup* simplesmente significava cópia de segurança. Entretanto, no presente ambiente de Tecnologia da Informação, o *backup* e a proteção dos dados são utilizados para prover continuidade ao negócio, replicação de dados, recuperação de desastres e redução nos custos de infra-estrutura. Porém a melhor maneira para assegurar os dados, seja local ou remotamente, pode ser um desafio desanimador, se não forem estabelecidas normas estratégicas para este fim.

Turban et al. (2004, p. 554) relatam que no caso de um desastre de grandes proporções, muitas vezes é necessário transferir a instalação central de computação para um local de *backup* remoto. Segundo esses autores esse procedimento é chamado de *hot site*. Outra opção de menor custo seria o procedimento *cold site*, onde fornecedores externos fornecem espaço livre de escritório com piso, ventilação e fiação especiais. Em uma situação de grande emergência, a empresa com problemas transfere seus próprios computadores, ou computadores alugados para aquele local.

2.4.2.4. Processos de Segurança Física

Sobre segurança física Caruso e Steffen (1999 apud Pinochet et al. 2007, p.1) observam que:

> "segurança física relaciona-se diretamente com os aspectos associados ao acesso físico a locais e a recursos de informações, tais como disponibilidade física ou o próprio acesso físico, sejam esses recursos às próprias informações, seus meios de suporte e armazenamento ou os mecanismos de controle de acesso às informações. Além disso, está também relacionada com as técnicas de preservação e recuperação das informações e seus meios de suporte e armazenamento."

No que concerne aos controles de acesso físico Pinochet et al. (2007) afirmam que os mesmos têm como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. Apenas as pessoas expressamente autorizadas pela gerência podem ter acesso físico aos sistemas de computadores. O controle de quem entra e de quem sai das instalações é um aspecto particularmente importante da segurança física. Não basta ter um guarda à entrada e obrigar todos os visitantes a se registrarem. É fundamental ter a certeza, por exemplo, de que os visitantes não levam material da Empresa sem autorização expressa do responsável por esse equipamento. (SILVA et al. 2003, p. 67)

Adicionalmente, são necessárias medidas adicionais para garantir que as soluções de controle não são ultrapassadas, evitando situações em que, por comodismo, uma porta seja deixada aberta, por exemplo. Mas o controle de acessos não se resume a uma portaria com guardas e, eventualmente, um sistema de vídeo em circuito fechado. Tal controle deve ser estendido a todas as áreas sensíveis, principalmente aos centros de dados e aos arquivos centrais.

3. METODOLOGIA

Entendeu-se que a melhor opção metodológica para o desenvolvimento desta pesquisa, seria a pesquisa de campo, de natureza qualitativa e finalidade descritiva. (VERGARA, 2005) A pesquisa foi realizada na empresa INPA - Indústria de Embalagens Santana S/A, localizada na cidade de Pirapetinga – MG Inicialmente foram entrevistadas quatro pessoas da alta gerência (os responsáveis pelas áreas de operações, comercial/suprimentos, desenvolvimento e qualidade/marketing) da empresa para: (i) identificar os procedimentos utilizados para gerenciar a segurança da informação da empresa; (ii) identificar as fontes e formas de obtenção e transferência de conhecimento para o desenvolvimento de inovações na empresa selecionada; e (iii) identificar as inovações - em natureza, grau de novidade, fonte de conhecimento – desenvolvidas pela empresa nos últimos 5 anos.

Solicitou-se a cada entrevistado que indicasse duas inovações (em processo ou produto) que tivessem contribuído de forma relevante para vantagem competitiva da empresa. A eles também foi requerido que informassem o nome do colaborador da empresa que acompanhou de perto o desenvolvimento (em especial a fase de obtenção de conhecimento) de cada uma das inovações citadas. A partir das indicações, foram selecionadas as duas inovações que receberam o maior número de indicações.

Foi solicitado então a cada um dos colaboradores que acompanharam de perto o desenvolvimento dessas inovações, que narrasse da forma mais livre possível as estórias do desenvolvimento das mesmas. Durante as narrativas, procurou-se verificar se os narradores mencionavam a natureza e grau de novidade da inovação, as vantagens e desvantagens para a organização, decorrentes da inovação, as fontes e as formas de obtenção de conhecimento utilizadas e principalmente os fatores que tenham facilitado e bloqueado o processo de obtenção de conhecimento utilizado na inovação.

Como meios de investigação e coleta de dados, foram utilizados documentos, observação direta, entrevistas e narrativas. (GIL, 2008) A técnica de análise temática, uma forma de análise de conteúdo, foi utilizada para tratamento e análise dos resultados (BOYATZIS, 1998, ROESCH, 1999). No caso da presente pesquisa, a analise temática foi empregada para avaliar a partir de material transcrito das narrativas a ocorrência (presença) de forma manifesta ou latente de temas previamente retirados da teoria. Esses temas são aqueles relacionados às fontes de conhecimento e as formas de obtenção e transferência de conhecimento a ser utilizado no desenvolvimento de inovações na empresa pesquisada e aos processos de gestão de segurança da informação implementados pela empresa**.** A partir do levantamento da ocorrência (presença), em termos de freqüência e profundidade, desses temas, foi possível

avaliar como a gestão de segurança da informação da empresa interfere no processo de obtenção e transferência de conhecimento necessário às inovações.

4. ANÁLISE DOS RESULTADOS

A presente seção procurou confrontar o que os autores visitados no referencial teórico afirmam sobre a influência da gestão de segurança da informação sobre o processo de obtenção e transferência de conhecimento necessário às inovações, com os resultados da pesquisa realizada na empresa INPA. Ou seja, o referencial teórico foi confrontado com as respostas obtidas nas entrevistas com a alta gerência da empresa e com os resultados da análise temática efetuada sobre as narrativas dos colaboradores acerca do desenvolvimento de duas inovações denominadas: Speed Size e Selo FSC (*Forest Stewardship Council*).

4.1 A EMPRESA PESQUISADA

Pirapetinga é uma cidade típica do interior mineiro, com pouco mais de 10 mil habitantes. Nesta cidade, em 1961, foi fundada a INPA, Indústria de Embalagens Santana SA, que é a maior fonte de arrecadação de impostos do município e emprega mais de 800 funcionários. Produzir papel e embalagens de papelão ondulado é o negócio da empresa que fabrica, atualmente, 9000 toneladas mensais de vários tipos de papéis para embalagens como papel miolo, capa e papel branco. São 15 milhões de m² em embalagens de papelão ondulado usando, como matéria-prima, 90% de aparas de papelão ondulado e 10% de celulose. A empresa tem clientes de vários segmentos como os de produtos alimentícios, frigoríficos, laticínios, cerâmica, limpeza, eletrodomésticos, bebidas, química, siderurgia, confecções, vidros, enlatados e petrolíferos.

4.1 A INOVAÇÃO SPEED SIZE

Trata-se de uma prensa de fabricação alemã fornecida pela empresa Voith, sendo utilizada na fabricação de chapas de papelão e tem como principal característica a adição de um filme de amido no papel que aumenta a impermeabilidade e a resistência do mesmo. O equipamento foi adquirido há cerca de três anos e substituiu uma máquina conhecida como Size Press, que era uma prensa de forma que utilizava um processo muito parecido, só que de maneira bem mais simples, no lugar do filme de amido ela utilizava um chuveiro aspersor na fase inicial da fabricação do papel, ao contrário da Speed Size que utiliza o amido na fase final do processo de fabricação do papelão.

A presente inovação proporcionou melhoria no processo produtivo e nos produtos da INPA, pois o amido aplicado provê alta consistência ao papel produzido, o que não ocorria no antigo processo em que o papel ficava muito molhado. Consequentemente a consistência era baixa e a produção tinha dificuldade na pró-secagem para fazer o papel chegar ao final do processo com um percentual de apenas 8% de umidade. No processo anterior para se conseguir uma secagem satisfatória os operadores acabavam tendo que diminuir a velocidade da máquina para conseguir alcançar uma secagem ideal, isso resultava em perda de produtividade e conseqüente perda de vantagem competitiva.

Conclui-se, portanto que a introdução da speed size no processo de fabricação do papelão pode ser considerada uma - “inovação incremental” – em processo e produto. Ou seja, sua implementação representou uma melhoria na versão anterior do processo, sem alterar de forma radical a linha evolutiva do mesmo. Deve-se atentar, entretanto que a percepção do grau de novidade depende da percepção do usuário. No caso da INPA, eles percebem tal melhoria como uma inovação de médio a alto incremento, principalmente em função da vantagem competitiva decorrente.

Cabe ressaltar que as inovações em processo levam também a inovações em produtos e vice e versa. No caso de uma inovação em processo, trata-se de mudanças no processo de produção do produto ou serviço. Gera impacto no produto final e produz benefícios no processo de produção, geralmente com aumentos de produtividade e redução de custos. Sobre as inovações em produtos, elas consistem em modificações nos atributos do produto, com mudança na forma como ele é percebido pelos consumidores. Na maior parte das vezes isso produz também necessidade de melhorias em processo. Percebeu-se então que a introdução da Speed no processo fabril da INPA não só levou a ganhos em produtividade, mas também a melhorias na qualidade de seus produtos em função da adição do filme de amido realizado pela Speed. Tendo sido a INPA a primeira empresa fabricante de embalagem de papelão no Brasil a utilizar a prensa Speed Size, em certa medida, ela obteve uma vantagem competitiva no seu setor.

O principal fator motivador para implantação desse equipamento surgiu da oportunidade de atender a uma crescente demanda por embalagens mais leves, resistentes e de melhor qualidade. Essa inovação, portanto, está mais alinhada ao conceito de *market pull* ("puxado" pelo mercado) onde o desenvolvimento de inovações surge com base em uma necessidade do mercado, ao contrário do conceito de *Technology-push* ("empurrado" pela tecnologia) que se refere ao desenvolvimento de inovações direcionadas primordialmente por fatores de natureza tecnológica.

O processo de desenvolvimento dessa inovação ocorreu da seguinte forma (i) identificação de uma demanda efetiva e crescente, (ii) busca de conhecimento externo à empresa, com clientes e através de contatos e testes com a empresa Voith, com o objetivo de superar suas limitações tecnológicas e obter um equipamento capaz de atender seus clientes mais exigentes e lhe dar um diferencial competitivo e assim proporcionando vantagem sobre seus concorrentes, (iii) comercialização das embalagens produzidas com o novo equipamento. Conclui-se, portanto que o processo de inovação da Speed Size passa pela segunda geração do processo de inovação, o modelo linear "puxado" pelo mercado (*market pull*) e contém características da quarta geração, modelo paralelo em que a inovação ocorre por meio de parcerias com clientes e fornecedores. Este último modelo enfatiza o papel das alianças: pesquisa e desenvolvimento, produção e marketing, entre outras áreas que estejam simultaneamente engajadas no processo de inovação. De acordo com os entrevistados, os clientes da empresa são os maiores responsáveis pelo direcionamento de suas atividades.

A introdução da speed representou para a INPA a obtenção de conhecimento de fonte externa por meio da incorporação de "tecnologias embutidas em máquinas, equipamentos e softwares". Tal forma de obtenção de conhecimento é bastante utilizada por empresas brasileiras e a tecnologia assim obtida pela INPA pode ser considerada uma tecnologia chave para a empresa. Isso porque ela faz parte do núcleo dos atuais processos e produtos da organização e oferece um elevado impacto competitivo. Ela é importante estrategicamente para a organização e pode ser bem protegida, do acesso por concorrentes, por meio de procedimentos de segurança de informação como, processos de segurança física em instalações e segurança lógica, que compreendem a utilização de câmeras, catracas eletrônicas, definição de senhas e perfis de acesso ao equipamento.

Foi identificada uma forma de obtenção de conhecimento interno sob a forma "programas de qualidade, treinamento de recursos humanos e aprendizado organizacional." Tais atividades compreendem programas de qualidade, treinamento de recursos humanos e aprendizado organizacional. Na fase inicial de implantação a empresa Alemã Voith realizou testes (controle de qualidade) com o papel produzido pela INPA com o objetivo de verificar alguma possibilidade de incompatibilidade de medidas em relação ao papel utilizado. Além disso, o fornecedor desenvolveu treinamentos com os gerentes e colaboradores envolvidos com a utilização do equipamento.

Verifica-se que tais formas e fontes de obtenção e transferência de conhecimento identificados na pesquisa coincidem com aquelas apontadas em estudos já desenvolvidos por pesquisadores do tema “Inovação”, em especial por Anand (2002) e Tigre (2006).

Sobre as dificuldades relacionadas à transferência para a força de trabalho do conhecimento necessário à introdução do equipamento no processo fabril e sua operação, verificou-se que a falta de capacitação profissional e o baixo nível de escolaridade de seus colaboradores, características comuns na região, foram os principais. Tal situação configura o que a teoria denomina “falta de capacidade de absorção”, um dos bloqueios genéricos encontrados na transferência interna ou externa de conhecimento, usualmente manifestado como incapacidade de valorizar, assimilar e aplicar o novo conhecimento em finalidades comerciais. A empresa tem se esforçado para superar tais bloqueios, promovendo treinamentos, como por exemplo, o desenvolvimento de um programa de capacitação profissional em parceria com o SESI de Pirapetinga.

Foi verificado que a INPA implementa iniciativas como programas de treinamento, exercícios de simulação de processos e operações de equipamentos e rodízios entre funcionários de diferentes setores. Essas iniciativas envolvem basicamente, práticas de *learning-by-doing* (aprender fazendo), que são centrais na fase do processo de conversão de conhecimento conhecida como internalização do conhecimento explícito. Com auxílio de documentos, manuais, histórias orais e através de aprendizado e experimentação, o conhecimento explícito é incorporado em ações e práticas gerando aquilo que a teoria denomina conhecimento operacional.

Pode-se verificar que no caso da presente inovação, a empresa incorporou aos seus processos os conceitos e tecnologias adquiridas por meio de treinamentos ministrados pela empresa fornecedora da Speed Size. Isso representa uma conversão de conhecimento do tipo internalização, ou seja, conhecimento explícito foi convertido em conhecimento tácito por meio do “aprender fazendo”.

Verificou-se que o acesso à tecnologia incorporada na Speed Size (parâmetros de desempenho e utilização) é restrito aos funcionários envolvidos com essa etapa do processo e seus gerentes imediatos. Tal restrição ilustra um bloqueio à transferência de conhecimento relacionado especificamente à segurança da informação, que é denominado pela teoria de “restrição de acesso a equipamentos”. Tal restrição abrange os recursos de informações, tais como disponibilidade física ou o próprio acesso físico, sejam esses recursos às próprias informações, seus meios de suporte e armazenamento ou os mecanismos de controle de acesso às informações. No caso da INPA, seus funcionários não o percebem como um bloqueio referente à transferência de conhecimento, pois para eles isso se trata apenas de uma forma de assegurar o acesso as informações restritas sobre o equipamento, visando reduzir o risco de pessoas não autorizadas utilizarem o equipamento, bem como essas informações serem acessadas por concorrentes.

A empresa considera importante investir em segurança da informação e implementou diversas iniciativas relacionadas com esse tema. A INPA possui uma política de segurança bem definida e com regras claras e documentadas, e que coloca grande ênfase nos controles lógicos de proteção como: utilização de *backups* (cópias de segurança) de seus bancos de dados, perfis de acesso e utilização de senhas aos sistemas aplicativos de gestão e equipamentos. Percebe-se uma preocupação da empresa em assegurar suas informações em caso de algum sinistro e mantê-las em sigilo, limitando os acessos a pessoas autorizadas. Com isso, identifica-se na empresa a presença de dois princípios básicos em segurança da informação, a “confidencialidade” e “disponibilidade”, os quais são considerados bloqueios à transferência de conhecimento. O primeiro princípio afirma que toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando limitar seu acesso e uso apenas às pessoas para quem elas são destinadas. Quanto ao segundo princípio, toda

informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem.

Identificou-se também a utilização de processos de segurança física, como por exemplo, a utilização de catracas eletrônicas na portaria da empresa e utilização de câmeras em todo o parque industrial. Tais instrumentos configuram bloqueios à transferência de conhecimento, denominados "instrumentos de segurança para instalações", e se referem ao desenho adequado das instalações e centros de processamento de dados, bem como, proteção contra campos eletromagnéticos, sistema de desligamento emergencial de energia elétrica, detecção e extinção de incêndios, bombas de água, entre outros.

4.3 A INOVAÇÃO SELO FSC

A obtenção do selo FSC (*Forest Stewardship Council*) por uma empresa garante que seus produtos ou seus componentes são provenientes de matéria prima originária de uma floresta bem manejada. O certificado estabelece que todas as fibras processadas pela INPA devem ser provenientes de fontes controladas. Em novembro de 2008 a INPA recebeu os auditores do IMAFLORA (Instituto de Manejo e Certificação Florestal e Agrícola), órgão credenciado para as auditorias do FSC no Brasil, que realizaram as auditorias para a Certificação. Em abril de 2009 a empresa recebeu o Certificado registrado sob o código: SW-COC-004047 / SW-CW-004047, emitido pelo órgão Smartwood Aliance.

A certificação pelo FSC - *Forest Stewardship Council* (Conselho de Manejo Florestal), popularmente chamada de "selo verde", partiu da necessidade de atender aos clientes que assim como ela também estão preocupados com a questão ambiental. A referida certificação foi fundamental para a INPA se projetar como uma empresa ambientalmente responsável, pois presentemente a preocupação ambiental é uma questão de grande relevância para as empresas, tanto no que se refere às reduções dos impactos de suas atividades no meio ambiente as quais são exigidas pela grande maioria de seus clientes. Em outras palavras, a implantação desse selo confere a INPA um diferencial competitivo no mercado de embalagens de papelão.

Essa inovação pode ser considerada como uma "inovação incremental" – em "processo" e "produto". Ou seja, sua implementação representou uma melhoria na versão anterior do processo, sem alterar de forma radical a linha evolutiva do mesmo. O selo FSC também representou melhorias em produtos da INPA na medida em que os clientes passaram a associar a empresa a causas ecológicas, um resultado típico de estratégia de diferenciação de produtos em imagem.

Sobre as fontes e formas de obtenção e transferência de conhecimento, a empresa utilizou "consultorias especializadas" como fonte de obtenção de conhecimento externo para a referida inovação. Em outras palavras, a empresa contratou os serviços de uma consultoria para adequar o seu atual sistema de gestão da qualidade aos requisitos do FSC.

Entretanto, antes da certificação, a INPA já possuía um sistema de gestão da qualidade implantado e sendo utilizado. Isso facilitou muito no processo de certificação, pois já existiam controles de documentos, registros, ações corretivas e preventivas, planejamento periódico de auditorias e controle de produtos não conformes. Com isso, pode-se afirmar que boa parte do conhecimento necessário a essa inovação a empresa já o possuía internamente. Houve uma adaptação do sistema de gestão da qualidade já existente, tornando-se um sistema de gestão integrada de acordo com as exigências do FSC.

No que concerne à obtenção de conhecimento interno, identificou-se também a presença do formato "programas de qualidade, treinamento de recursos humanos e aprendizado organizacional". Tal presença é percebida devido ao fato de o setor de qualidade buscar aprimorar seus processos através de treinamentos internos, palestras e programas de

capacitação. Apesar de terem recebido treinamentos de consultorias eles também investem em programas de treinamentos para obterem melhorias em seus processos.

Durante a implementação da inovação, foi possível perceber a presença do processo de conversão do conhecimento conhecido como "combinação", que é definido como a combinação de conjuntos diferentes de conhecimento explícito a partir do banco de conhecimentos da empresa. Essa afirmação é possível devido à constatação de que os funcionários da INPA compartilharam conhecimento com a consultoria especializada, por meio de documentos, reuniões e palestras e posteriormente sistematizaram esse conhecimento em banco de conhecimento da empresa.

Em relação aos bloqueios genéricos à transferência de conhecimento interno e externo, foi identificado o que a teoria denomina de "falta de capacidade de absorção." Trata-se de uma incapacidade de valorizar, assimilar e aplicar o novo conhecimento em finalidades comerciais foi apontado para a referida inovação como um dos maiores bloqueios a obtenção e transferência de conhecimento. O baixo nível de instrução dos funcionários tornou mais lento o processo de implantação do selo FSC, principalmente na parte inicial.

Verificou-se que o acesso às informações técnicas como regras e processos é restrito aos funcionários envolvidos com essa etapa do processo de controle de matéria prima e seus gerentes imediatos. Tal restrição evidencia um bloqueio relacionado à transferência de conhecimento relacionada especificamente à segurança da informação, o que a teoria denomina de "confidencialidade". Por confidencialidade se entende que toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

No que concerne ao selo FSC, cada funcionário acessa apenas as informações que são relativas às suas funções, não visualizando dados de outros setores e outras funções que não tenham haver com suas tarefas. Tal bloqueio é relatado apenas como um procedimento de segurança contra acessos indevidos sobre informações do FSC. De fato tais limitações não são reconhecidas pelos funcionários como um bloqueio aos processos de obtenção e transferência de conhecimentos necessários as inovações.

A respeito dos controles de proteção, identifica-se o chamado "controle geral de proteção" que tem por finalidade proteger sistemas, independentemente do aplicativo específico. Assim, a INPA utiliza senhas de acesso geral ao sistema de gestão da empresa. Adicionalmente, cada funcionário possui um perfil com acessos específicos a determinados sistemas. A INPA não percebe controle como um bloqueio a transferência de conhecimento e sim apenas como um procedimento de segurança.

5 CONCLUSÕES

O objetivo dessa pesquisa foi descrever como a gestão de segurança da informação influencia o processo utilizado por empresas para obtenção e transferência de conhecimento necessário ao desenvolvimento de suas inovações. Através de entrevistas com gerentes sobre as inovações implementadas nos últimos 5 anos, foram identificadas duas inovações relevantes para a empresa pesquisada. A incorporação da prensa Speed Size no processo fabril e a alteração nesse mesmo processo fabril decorrente da obtenção da certificação FSC - *Forest Stewardship Council* (Conselho de Manejo Florestal), popularmente chamada de "selo verde".

Os resultados da pesquisa sugerem que as formas de obtenção e transferência de conhecimento que contribuíram para a implementação das inovações analisadas na INPA foram: "Tecnologias embutidas em máquinas, equipamentos e softwares", "Consultorias especializadas" e "Programas de qualidade, treinamento de recursos humanos e aprendizado organizacional cumulativo", as duas primeiras originando-se em fontes externas e a terceira em fonte interna. Sobre essa última forma, pode ser observada a alta freqüência com que ela

foi utilizada na INPA para o desenvolvimento das duas inovações analisadas. Em outras palavras, os resultados da pesquisa sugerem que a empresa investe intensamente em treinamentos e programas de qualidade, visando melhorar a capacitação de seus colaboradores.

Em relação aos bloqueios genéricos à transferência de conhecimento necessário, identificou-se apenas a "falta de capacidade de absorção". Tal bloqueio trata-se de uma incapacidade de valorizar, assimilar e aplicar o novo conhecimento está diretamente relacionado a níveis não adequados de capacitação profissional e o nível de instrução de funcionários da empresa. Em certa medida o bloqueio identificado está diretamente relacionado à terceira forma de obtenção de conhecimento mencionada no parágrafo anterior. Isto porque, para implementação das inovações citadas, a INPA precisou desenvolver vários programas de treinamentos e programas de qualidade para capacitar e melhorar os níveis de instrução de seus funcionários.

A respeito dos procedimentos e instrumentos de gestão da segurança da informação utilizados pela empresa pesquisada, verificou-se a presença de procedimentos de segurança física e lógica como: "Confidencialidade" – utilização de senhas e perfis de acesso, "Controle geral de proteção" – controles de proteção de sistemas (*hardware e software)*, "Antivírus", "Backups" (cópias de segurança), "Instrumentos de segurança para instalações" - catracas eletrônicas e câmeras.

A pesquisa partiu da suposição de que mesmo considerando a importância da gestão da segurança da informação e seus benefícios para uma organização, os processos de segurança lógica, física e os controles de acesso, prejudicam o processo de obtenção e transferência de conhecimento necessário às inovações. Tal suposição não foi verificada nas entrevistas e nos relatos dos colaboradores, pois ambos mencionaram como bloqueio à transferência de conhecimento apenas a "falta de capacidade de absorção", que se caracteriza como um bloqueio genérico à transferência de conhecimento e não ligado à gestão de segurança de informação propriamente dita.

Dessa forma, foi possível concluir que os instrumentos de segurança da informação não interferem de forma negativa no processo de inovação na empresa pesquisada. Tais instrumentos interferem de forma positiva no processo de obtenção e transferência de conhecimento necessário a inovações da INPA, uma vez que os mesmos têm por finalidade garantir o acesso e a disponibilidade das informações. Uma empresa que não possui os referidos instrumentos está vulnerável a desastres e acidentes, sejam eles intencionais ou não, o que acarretaria perda total ou parcial de suas informações ou até mesmo os acessos indevidos prejudicaria o processo de obtenção e transferência de conhecimento necessário a inovações.

REFERÊNCIAS

ABNT. **Tecnologia da informação – Código de prática para a gestão da Segurança da Informação (NBR ISO/IEC 17799).** Rio de Janeiro: 2005.

ANAND, V., GLICK, W. H., MANZ, C. C. Capital social: Explorando a rede de relações da empresa. **Revista de Administração de Empresas.** v. 16, n. 1, p. 87-101, 2002.

BOYATZIS, R. E. **Transforming qualitative information:** thematic analysis and code development. Thousand Oaks, CA: Sage, 1998.

CACIATO, Luciano Eduardo. **Gerenciamento da Segurança de Informação em Redes de Computadores e a Aplicação da Norma ISO/IEC 17799:2001.** Campinas, 2004. Disponível em: <http://www.rau-tu.unicamp.br/>. Acesso em: 25 Abr. 2008.

DAVENPORT, T. H., PRUSAK, L. **Conhecimento Empresarial: como as organizações gerenciam seu conhecimento.** 14 ed., Rio de Janeiro, Campus, 1998.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. Ed. São Paulo, editora Atlas, 2008.

IMBUZEIRO, P. E. A., MARSÍGLIA, D. C. **Rumo a um modelo de compartilhamento do conhecimento organizacional em um hospital público.** <http://www.ifbae.com.br/congresso5/pdf/B0109.pdf>. Acesso em 15 Out. 2009.

LASTRES, H. M. M.; CASSIOLATO, J. E.; ARROIO, A. (org.). **Conhecimento, sistemas de inovação e desenvolvimento.** Rio de Janeiro: UFRJ/Contraponto, 2005, p. 83-130.

LEMOS, C. **Rede de sistemas produtivos e inovativos locais: inovação em arranjos e sistemas de MPME.** Net, Rio de janeiro, outubro. 2001. Disponível em: <http://www.ie.ufrj.br/rede>. Universidade Federal do Rio de Janeiro Acesso em 06 de agosto de 2009.

MACHADO, D. D. P. N, GOMES, G., GIOTTO, O. T. O que se produz de conhecimento sobre inovação?: uma breve análise das características dos artigos de inovação publicados nos anais do enanpad (1997-2007). **Anais Simpoi.** São Paulo, 2008.

MORAES, E. M., FERREIRA, J. A. F., SANTOS, M. L. X. Normas de referência para backup de dados e segurança da informação. **Anais Contecsi.** São Paulo, 2007.

NONAKA, I.; TAKEUCHI, H. **Criação de conhecimento na empresa.** Campus: Rio de Janeiro, 2000.

PELTIER, T. **Information Security Policies, Procedures, and Standards**. Florida, Auerbach, 2001.

PINOCHET, L. H. C., BATISTA, M. C., RAUDELIUNAS, C. E. Análise comparativa do processo de implementação e solução em segurança para ambientes físicos. **Anais Contecsi.** São Paulo, 2007.

ROESCH, S. M. A. **Projetos de estágio e de pesquisa em administração: guia para estágios, trabalhos de conclusão, dissertações e estudos de caso.** São Paulo: Atlas, 1999.

ROSIRI, Alessandro Marco e PALMIRANO, Ângelo. **Administração de Sistemas de informação e a Gestão do Conhecimento.** 2ª Edição, São Paulo, Pioneira Thomson, 2003.

SILVA, Pedro Tavares, CARVALHO, Hugo e TORRES, Catarina Botelho. **Segurança dos sistemas de Informação – Gestão Estratégica da Segurança Empresarial.** S.1., s.n., 2003 Disponível em: <http://www.centroatl.pt/titulos/si/seguranca-si.php3/>. Acesso em 04 Abr. 2008.

SIMÕES J. M. M. Transferência do conhecimento no ensino superior público em Portugal. **Revista Universo Contábil.** v. 4, n. 1, p. 95-113, 2008.

SVEIBY, Karl Erik. **A Nova Riqueza das Organizações** – gerando e avaliando
patrimônios de conhecimento. Rio de Janeiro: Campus, 1998.

TIDD, J.; BESSANT, J.; PAVITT, K. **Managing innovation: integrating technological, market and organizational change**, 3.ed. Chichester, UK: Wiley, 2001.

TIGRE, P. B. **Gestão da inovação: a economia da tecnologia no Brasil.** Rio de Janeiro: Campus, 2006.

TURBAN, E. McLean, E., WETHERBE, J. **Tecnologia da informação para gestão. 3ª Edição**, Porto Alegre, Bookman, 2004.

TSUJIGUCHI, F. Y., CAMARA, M. R. G. Aprendizado e inovação na rede de micro e pequenas empresas de software de londrina. **Anais Simpoi.** São Paulo, 2008.

VERGARA, Sylvia Constant. **Projetos e Relatórios de Pesquisa em Administração.** Atlas, São Paulo, 2005.