Obtenção de Conhecimento para Inovação: Benefícios e Malefícios de Processos de Gestão da Segurança da Informação

Obtaining Knowledge for Innovation: Benefits and Harms of Procedures for Managing Information Security

José Geraldo Pereira Barbosa
Doutor em Administração – COPPEAD/UFRJ
Coordenador e Professor do Mestrado em Administração e Desenvolvimento Empresarial (MADE/UNESA).
Av. Pres. Vargas 642 22º andar, Centro, Rio de Janeiro, RJ, 20071-001
jose.geraldo@estacio.br.

Fábio da Silva Eiras
Mestre em Administração – MADE/UNESA
Professor do Curso de Administração da Fundação Educacional de Além Paraíba
Rua Izabel Herdy Alves, 305 - São José, Além Paraíba - MG, 36660-000.
fabiosee@hotmail.com

Antonio Augusto Gonçalves
Doutor em Engenharia de Produção – COPPE/UFRJ
Professor do Mestrado em Administração e Desenvolvimento Empresarial (MADE/UNESA).
Av. Pres. Vargas 642 22º andar, Centro, Rio de Janeiro, RJ, 20071-001
augusto@inca.br.

Elaine Maria Tavares Rodrigues
Doutora em Administração – EBAPE/FGV-RJ
Pós-Doutorado em Administração - CERGAM), Université Aix-Marseille III
Professora do Instituto COPPEAD de Administração da UFRJ
Rua Pascoal Lemme, 355 – Ilha do Fundão – Rio de Janeiro, RJ – 21941-918
elainetavares@unb.br

Resumo

A pesquisa relatada neste artigo teve como objetivo descrever como os processos de segurança da informação utilizados numa empresa de fabricação de papel e embalagens influenciaram a obtenção de conhecimento em duas inovações. O estudo foi conduzido por meio de uma pesquisa de campo, com utilização de entrevistas, narrativas, observação direta e análise temática, para coleta e tratamento dos dados. 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, prejudicariam o processo de obtenção e transferência de conhecimento necessário às inovações. Verificou-se a presença de cinco instrumentos de segurança física e lógica: "confidencialidade", "controle geral de proteção", "antivírus", "backups" e "instrumentos de segurança para instalações", que não interferiram de forma negativa na obtenção de conhecimento. O único bloqueio identificado no caso para a transferência de conhecimento residiu na falta de capacidade de absorção do conhecimento dos funcionários. O caso

Artigo publicado anteriormente nos Anais do XIII SEMEAD em 2010.
Artigo submetido em 22 de maio de 2012 e aceito em 30 de junho de 2012 pelo Editor Marcelo Alvaro da Silva Macedo, após *double blind review*.

apresentado relata assim uma situação onde uma política de segurança da informação clara e coerente possibilitou o processo de obtenção e transferência de conhecimentos necessários a inovação. Em outras palavras, a partir dos resultados da pesquisa foi possível rejeitar a suposição da pesquisa.
Palavras-chave: Inovação. Segurança da Informação. Conhecimento.

Abstract

The research reported in this article aims to describe how the processes of information security used in a manufacturing and packaging paper company influenced the attainment of knowledge on two innovations. The study was conducted through field research, using interviews, narratives, direct observation and thematic analysis for data collection and data processing. The research started from the assumption that even considering the importance of managing information security and its benefits to an organization, the processes of logical security, and physical access controls, would undermine the process of obtaining and transference of knowledge required by innovations. It was observed the presence of five instruments of physical and logical security: "confidentiality", "general control of protection", "antivirus", "backups" and "facility security procedures" which did not interfere negatively in obtaining knowledge. The single barrier identified for the transfer of knowledge was the lack of absorptive capacity of knowledge workers. Therefore, the case describes a situation where a clearly and consistent information security policy allowed the obtaining and transferring of knowledge necessary for innovation. In other words, the assumption of the research was rejected by the findings.
Keywords: Innovation. Information security. Knowledge.

1. Introdução

A obtenção e transferência de conhecimento é um insumo fundamental para os processos de inovação (TIDD et al., 2001) . 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 (LASTRES e CASSIOLATO, 2005; TIDD et al. 2001; TIGRE, 2006).

Com a crescente evolução dos sistemas de informação, as empresas têm investido em sofisticados *softwares* de gestão, como tecnologias de *EDI* (*Electronic Data Interchange*), sistemas em ambiente web e sofisticados bancos de dados, demandando uma ampla infra-estrutura de Tecnologia da Informação (TI).

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 dos dados armazenados, nos seus aspectos físicos, lógicos e humanos, bem como a regulação dos acessos às informações, definindo quem irá acessar o quê e sobre quais condições.

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 para os negócios, a informação precisa ser protegida, de forma que acessos não autorizados, alterações indevidas e indisponibilidades sejam evitadas (CACIATO, 2004).

Apesar de necessários para assegurar a integridade e disponibilidade das informações, os procedimento de segurança da informação podem em certa medida restringir ou dificultar a obtenção e transferência do conhecimento necessário a inovação.

Este artigo apresenta um estudo de caso que teve como objetivo descrever como a gestão de segurança da informação interfere no processo de obtenção e transferência de

conhecimento necessário à inovação na empresa INPA - Indústria de Embalagens Santana S/A,.

Para essa finalidade, foram identificadas as inovações desenvolvidas pela empresa nos últimos cinco 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.

Foram selecionadas as duas inovações, denominadas Speed Size e Selo FSC (*Forest Stewardship Council*), e verificados: a natureza e grau de novidade da inovação, suas vantagens e desvantagens para a organização, 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.

Além de entrevistas e narrativas, foram utilizados documentos e observação direta na coleta de dados. A técnica de análise temática foi utilizada para tratamento e análise dos resultados.

Na próxima seção, são apresentadas as teorias de referência utilizadas na pesquisa. Inicia-se pela visão do conhecimento como principal insumo de inovações e discute-se suas fontes de obtenção e formas de transferência. O tema da segurança da informação é tratado a seguir, onde é apresentada a idéia de política de segurança da informação e sua importância e são introduzidos os mecanismos de gestão da segurança da informação. Os procedimentos metodológicos utilizados são então explicados. Na análise dos dados, é elucidada a utilização da TI na empresa em análise e, para cada inovação objeto do estudo, são discutidos como os processos de segurança da informação utilizados influenciaram a obtenção de conhecimento. As considerações finais discutem os resultados encontrados e a contribuição da pesquisa.

2. Referencial Teórico

2.1. O Conhecimento como Principal Insumo de Inovações

As inovações podem ocorrer em produtos e processos. No caso de uma inovação em processo, trata-se de uma mudança 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. (TIDD et al., 2001)

As inovações surgem de iniciativas internas ou externas e podem ser motivadas por fatores de natureza mercadológica (*market pull*) ou tecnológica (*technology push*). Um exemplo de *market pull* são as idéias que surgem na área de vendas e a identificação de novas demandas de mercado (*demand pull)* e de *technology push* são as idéias que surgem nas áreas técnicas. TIGRE (2006)

Rothwell (1992) sugere que os processos de inovação podem ser classificados em cinco gerações:

a) Inovação empurrada pela tecnologia (*technology push*) – é o modelo adotado nas décadas de 1950 e 1960. Nesse período a demanda era usualmente maior do que a capacidade de produção e a maioria das inovações, empurrada pela tecnologia, era bem aceita pelos mercados.
b) Inovação puxada pelo mercado (*market pull*) – esse modelo é considerado a segunda geração de inovação. Entre os anos 1960 e 1970, o mercado começou a ficar mais competitivo, de modo que as empresas passaram a se certificar das necessidades dos consumidores antes de desenvolverem soluções tecnológicas para satisfazê-los.

c) Modelo composto (*coupling model of innovation*) – já nos anos 1970 e 1980, o processo de inovação se caracteriza pela comunicação interligando os agentes internos e externos para conquistar acesso a conhecimentos externos na comunidade científica e no mercado. O autor definiu a terceira geração como uma combinação entre os dois modelos anteriores, com base em uma forte ligação entre as áreas de *marketing* e de P&D.
d) Modelo integrado (*integrated innovation process*) – a quarta geração é representada pelo modelo integrado, baseado nas características de inovação em companhias japonesas nos anos 1980 e 1990. O modelo é caracterizado pela integração e desenvolvimento paralelo (engenharia concorrente), onde as companhias integram os fornecedores ao processo de desenvolvimento de novo produto, ao mesmo tempo em que integram as atividades dos diferentes departamentos.
e) Modelo de Redes – a última geração é caracterizada pela integração de sistemas, extensivo *networking*, resposta flexível e customizada e inovação continua. Ele decorre do aumento das alianças estratégicas, do P&D colaborativo, da maior atenção à gestão da cadeia de suprimento, do crescimento de redes entre pequenas e médias empresas com empresas grandes e do crescimento das redes entre pequenas empresas.

Quando as organizações inovam, elas não só adquirem informações externas, com o intuito de resolver os problemas existentes e se adaptar ao ambiente em transformação, mas criam novos conhecimentos e informações que muitas vezes são transmitidos além de suas fronteiras, a fim de redefinir problemas e soluções e, assim, recriar seu meio (NONAKA e TAKEUCHI 1997). O progresso econômico acontece principalmente dirigido pelos avanços do conhecimento e aplicação da inovação, influenciando diretamente o desenvolvimento de nações (MACHADO et al., 2008, p. 2),.

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. A criação do conhecimento organizacional é um fator chave para explicar, por exemplo, o sucesso das empresas japonesas em inovação (NONAKA e TAKEUCHI, 1997).

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. Entende-se por conhecimento organizacional qualquer informação, crença ou habilidade que a organização possa aplicar às suas atividades (ANAND et al., 2002, p.58). Este conhecimento, nas organizações, se encontra não apenas nos documentos, bases de dados e sistemas de informação, mas também nos processos de negócios, nas práticas grupais e na experiência acumulada pelas pessoas (ROSIRI e PALMIRANO, 2003).

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 em produtos, serviços e sistemas. As empresas inovadoras geralmente recorrem a uma combinação de diferentes fontes de tecnologia, informação e conhecimento, tanto de origem interna quanto externa (TIGRE, 2006).

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 necessária a busca por novas fontes de obtenção de conhecimento, inclusive para além das fronteiras organizacionais. Quando as organizações estendem seus vínculos com organizações e indivíduos de fora, ocorre a aquisição de conhecimento de fontes externas (ANAND et al. 2002). Desta forma, o processo inovativo não acontece isoladamente. Na busca por inovações, as firmas procuram estabelecer relações e interagir com outras organizações e indivíduos, pois podem utilizar informações e

conhecimentos que se localizam também fora de seu ambiente interno (TSUJIGUCHI e CAMARA, 2008). É o caso, por exemplo, das informações as 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).

A obtenção de conhecimento refere-se, assim, às informações e dados adquiridos do ambiente interno e externo por meio das pessoas, e que resultam em conhecimento (IMBUZEIRO e MARSÍGLIA, 2009). 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 e processos.

Tigre (2006) explica que as fontes internas de inovação envolvem tanto as atividades explicitamente voltadas para o desenvolvimento de novos produtos e processos, quanto aquelas que colaboram para implementação de melhorias incrementais em produtos e processos já existentes, como é o caso de programas de qualidade, treinamento de recursos humanos e aprendizado organizacional. Sobre as fontes externas, o autor acrescenta que elas envolvem também: 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 e tecnologias embutidas em máquinas e equipamentos (TIGRE, 2006).

Nonaka e Takeuchi (1997) ressaltam ainda que 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, por meio de manuais, livros, revistas, *software*, fórmulas, , 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 (TIGRE, 2006). 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 (ANAND et al., 2002).

2.3. Formas de Transferência de Conhecimento

A transferência do conhecimento ocorre de maneira permanente e espontânea nas organizações (DAVENPORT e PRUSAK, 1998). Este tipo de transferência é vital para o sucesso de uma empresa (DAVENPORT, 1998, p. 108). Porém, a transferência espontânea ocorre de maneira fragmentada e localizada. Assim, 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 (SIMÕES, 2008).

Muitos autores enfatizam em demasia o papel da área da informática e dos sistemas de informação na transferência do conhecimento. Embora tal postura não seja totalmente incorreta, pois existem diversas TIs que podem ajudar a transferência do conhecimento, existem outras variáveis que podem influenciar, de forma positiva ou negativa, essa mesma transferência (SIMÕES, 2008).

O sucesso da transferência do conhecimento, segundo Silva e Neves (2003, p. 193), 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". Um contra exemplo disto ocorre quando as organizações contratam 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).

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 há que haver um meio para assegurar a transmissão do conhecimento. Segundo Sveiby (1998), a transferência do conhecimento pode ser feita por meio de mecanismos direcionados à 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 "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

Fonte: Sveiby (1998, p. 53

O termo gestão do conhecimento implica a transferência formalizada, embora um de seus elementos essenciais seja o desenvolvimento de estratégias específicas estimuladoras de 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	Estabelecer um consenso através de educação, discussão, publicação, trabalho em equipe e rodízio de funções
Falta de tempo e de locais de encontro, idéia estreita de trabalho produtivo	Criar tempos 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 o aprendizado, basear as constatações na abertura a idéias
Crença de que o conhecimento é uma 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 nem sempre é tratada de maneira adequada pelos gestores, principalmente em pequenas empresas (BARBAES et al., 2007). Entretanto, a informação deve ser considerada um ativo da empresa e seu correto gerenciamento é fundamental para o sucesso de qualquer organização (CACIATO, 2004). Devido à sua importância nos negócios, a informação precisa ser protegida, de forma que acessos não autorizados, alterações indevidas e indisponibilidades sejam evitadas.

A implementação da segurança da informação é norteada por três princípios básicos (SÊMOLA, 2003):

- 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.

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 (CARVALHO, 2008). Um 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, e comportamento dos funcionários. Ou seja, deve abranger os ativos tangíveis e intangíveis de uma organização (PELTIER, 2001).

Para Gil (2008), a informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Confidencialidade, integridade e disponibilidade da informação podem ser essenciais para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado.

Semola (2003), ressalta quer os modelos de segurança têm limites teóricos e práticos. Nem sempre é possível satisfazer a todos os requisitos de segurança desejados. O emprego de um modelo de segurança não implica em segurança total, pois constantemente novas técnicas são criadas para fazer alterações indevida de sistemas e produtos.

Segundo Comer (2004) os requisitos de segurança são identificados através de uma avaliação sistemática dos riscos de segurança. Os gastos com os controles necessitam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança. As técnicas de avaliação de risco podem ser aplicadas em toda a organização ou apenas em parte dela, assim como em um sistema de informação individual, componentes de um sistema específico ou serviços, quando for viável, prático e útil.

Para Turban (2004) uma vez tendo sido identificados os requisitos de segurança, convém que os controles sejam selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável. Os controles podem ser selecionados a partir da norma ISO 17799:2005 ou de outro conjunto de controles, ou novos controles podem ser desenvolvidos para atender às necessidades específicas, quando apropriado.

2.4.1. Política de Segurança da Informação (SI)

Para que todos os esforços e investimentos em tecnologia sejam bem sucedidos, é essencial que as empresas assimilem 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)

Segundo Gonçalves (2002 apud Moraes et al. 2007), as políticas de 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.

De acordo com a norma NBR ISO/IEC 17799 (ABNT, 2005), o conjunto de políticas de SI de qualquer organização deve 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.

Segundo a norma acima mencionada, 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 O principal objetivo da política de SI é proteger as informações e os recursos computacionais que as apóiam (MORAES et al., 2007).

2.4.2. Gestão da Segurança da Informação

Segundo Turban et al. (2004), os controles de proteção são divididos em duas categorias principais: controles gerais e controles de aplicativos. Os controles gerais são implantados para proteger o sistema. As principais categorias deste tipo de controle são (Turban et al., 2004):

- controles físicos: referem-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. 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 e etc.
- controle de acesso: restrição imposta a usuários não autorizados de acessar uma parte ou toda informação. Tal controle pode *utilizar s*istemas de identificação biométrica, como por exemplo, impressões digitais, geometria da mão, leitura da íris, voz e etc. Também pode utilizar controles de web (internet), como por exemplo, autenticação, podendo essa ser biométrica, criptografia, testadores de cabos, *firewalls* e proteção contra vírus. 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.

- 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.
- controles administrativos: lidam com a definição de diretrizes e o monitoramento de seu cumprimento.

Em relação aos controles de aplicativos, Turban et al. (2004) 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. 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. Os controles de processamento garantem que os dados sejam completamente processados, sendo válidos e precisos e que os programas sejam executados corretamente. Com relação aos controles de saída, eles garantem que os resultados do processamento sejam precisos, válidos, completos e consistentes (TURBAN et al., 2004)

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 . Para manutenção da segurança no tráfego de informações na rede, a criptografia de dados é um dos principais recursos (SILVA et al. 2003). 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.

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 decisão da melhor maneira para prover segurança aos dados, seja local ou remotamente, é um grande desafio, principalmente se não forem estabelecidos objetivos estratégicos para esta finalidade (Moraes et al., 2007).

No caso de um desastre de grandes proporções, muitas vezes é necessário transferir a instalação central de computação para um local de *backup* remoto. 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 (TURBAN et al., 2004).

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, os mesmos têm como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos (PINOCHET et al., 2007). 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 sejam 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

A pesquisa, de natureza qualitativa e finalidade descritiva, foi baseada em um estudo de caso realizado na empresa INPA - Indústria de Embalagens Santana S/A, localizada na cidade de Pirapetinga – MG.

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, 9.000 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.

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 houvessem 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, denominadas Speed Size e Selo FSC (*Forest Stewardship Council*).

Foi solicitado então a cada um dos colaboradores que acompanharam de perto o desenvolvimento dessas inovações, que narrasse da forma livre o 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 coleta de dados, além das entrevistas e narrativas, foram utilizados documentos e observação direta (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). Esta técnica foi empregada para avaliar a partir de material transcrito das narrativas a ocorrência de forma manifesta ou latente de temas previamente retirados da teoria. Esses temas foram 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 desses temas, em termos de freqüência e profundidade, foi possível avaliar como a gestão de segurança da informação da empresa interferiu em seu processo de obtenção e transferência de conhecimento necessário às inovações.

4. Análise dos Resultados

4.1 A Tecnologia da Informação na INPA

Para compreender o contexto tecnológico, foi necessário analisar a situação da empresa em relação a TI, além de avaliar como esta lida com a segurança da informação.

O Departamento de Tecnologia da INPA Embalagens trabalha constantemente para melhoria de toda a empresa, com serviços de manutenção de hardware, software e gestão da tecnologia da informação.

A INPA está investindo para ampliar a integração de seu sistema de gestão empresarial (*software* de gestão), com o objetivo de integrar e aperfeiçoar seus processos e elevar sua produtividade.

O principal sistema de gestão é o *ERP - enterprise resource planning* - fornecido pela Microsiga - TOTVS, utilizado para o processamento e integração de transações das áreas funcionais da empresa. A INPA utiliza também os softwares *Trimbox* e *Trimpapel*, fornecidos pela empresa Simula. O primeiro tem como objetivo o processamento das informações técnicas referentes à produção e o segundo processa informações sobre as características do papel produzido, esses dois últimos se comunicam entre si.

Em 2008, a empresa adquiriu novos servidores de última geração para otimizar a performance de sua base de dados integrada. Além disso, em parceria com a empresa Indicca Tecnologia, novas melhorias foram desenvolvidas no recebimento e envio de correio eletrônico (*e-mail*) através de políticas de segurança que garantiram mais integridade nas mensagens, através de um filtro *anti-spam* e anti-vírus corporativo da empresa *Symantec*.

Com estas melhorias a produtividade da TI teve crescimento de cerca de 30%, além de consideráveis ganhos em agilidade na comunicação externa através do correio eletrônico. Em parceria com a Embratel, a INPA dobrou a capacidade de seu *link* com a Internet, tornando mais rápida a comunicação com suas filiais, escritórios, parceiros de negócio e clientes.

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* 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.

Embora os sistemas *ERP, Trimbox e Trimpapel* armazenem informações relevantes para a operação e gestão estratégica da empresa, não existe nenhum sistema específico para a gestão do conhecimento, ou seja, não há nenhum modelo de repositório do conhecimento associado às tecnologias utilizadas pela INPA.

4.2. 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 que 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. Na Size Press, no lugar do filme de amido, utilizava-se um chuveiro aspersor na fase inicial da fabricação do papel.

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 havia dificuldade na etapa de pró-secagem, para fazer com que o papel chegasse 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, o que 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 do aumento da vantagem competitiva que ela possibilitou.

Cabe ressaltar que as inovações em processo levam também a inovações em produtos e vice e versa. Percebeu-se então que a introdução da Speed Size 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. Pelo fato de ter sido a primeira empresa fabricante de embalagem de papelão no Brasil a utilizar a prensa Speed Size, a INPA obteve 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.*

Sobre o desenvolvimento dessa inovação, ele ocorreu da seguinte forma (i) identificação de uma demanda efetiva e crescente, (ii) busca de conhecimento externo à empresa, em 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 permitir a obtenção de um diferencial competitivo, (iii) comercialização das embalagens produzidas com o novo equipamento.

Conclui-se, portanto que o processo de inovação da Speed Size passa pela segunda geração de processos de inovação, o modelo linear "puxado pelo mercado" (*market pull*), e também contém características da quarta geração, modelo "paralelo" em que a inovação ocorre por meio de parcerias com clientes e fornecedores. De acordo com os entrevistados, os clientes da empresa são os maiores responsáveis pelo direcionamento de suas atividades.

A introdução da Speed Size 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.

Também relacionado à introdução da Speed Size, ocorreu a 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.

Observou-se também a transferência para a INPA, de tecnologias incorporadas na Speed Size por meio de treinamentos ministrados pela empresa fornecedora do equipamento. Isso representa também uma conversão de conhecimento do tipo internalização, ou seja,

conhecimento explícito sendo convertido em conhecimento tácito por meio do "aprender fazendo".

Verificou-se que o acesso aos parâmetros de desempenho e utilização da Speed Size 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". 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 impedir o acesso às informações restritas sobre o equipamento, visando reduzir o risco de pessoas não autorizadas utilizarem o equipamento, bem como essas informações serem acessadas por concorrentes.

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, sob o ponto de vista ambiental. O certificado estabelece que todas as fibras processadas pela INPA são 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 obtenção do selo FSC, popularmente chamado de "selo verde", foi gerada pela necessidade de atender aos clientes que, assim como a INPA, também estão preocupados com a questão ambiental. A referida certificação foi fundamental para a INPA se projetar como uma empresa ambientalmente responsável, pois ela percebeu que reduções dos impactos de suas atividades no meio ambiente são exigidas pela grande maioria de seus clientes. Em outras palavras, a implantação desse selo conferiu à 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. 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 relacionadas a procedimentos e processos de controle de matéria prima é restrito aos funcionários envolvidos com essa etapa do processo e seus gerentes imediatos. Tal restrição evidencia um bloqueio relacionado à transferência de conhecimento relacionado especificamente à segurança da informação, o que a teoria denomina de confidencialidade.

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 a ver 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, por meio de um estudo de caso, como a gestão de segurança da informação influencia o processo utilizado para obtenção e transferência de conhecimento necessário ao desenvolvimento de inovação. 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*, 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 originam--se de fontes externas e a terceira de 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, pois 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 e está diretamente relacionada a níveis não adequados de capacitação profissional e de instrução de funcionários da empresa. Em certa medida, o bloqueio identificado justifica a presença da terceira forma de obtenção de conhecimento mencionada. Isto porque, para implementação das inovações citadas, a INPA precisou desenvolver vários programas de treinamento e 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", "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 prejudicariam 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.

A não verificação da suposição acima pode ser parcialmente atribuída ao fato de que a empresa pesquisada não utiliza sistemas de gestão de conhecimento, ou seja, não existe um modelo de repositório do conhecimento associado às tecnologias da empresa. Os sistemas de informação da empresa, *ERP*, *Trimbox (Produção) e* Trimpapel (características do papel), são de natureza transacional e, portanto não tem por fim alimentar plenamente os processos de obtenção de conhecimento necessário a inovações. Em outras palavras, a presença de sistemas de conhecimento poderia ter mudado os rumos da pesquisa de campo, levando eventualmente à confirmação da suposição inicial da pesquisa.

Foi possível constatar que o processo de obtenção e transferência de conhecimentos necessários a inovações requer uma política de segurança da informação clara e coerente. Ou seja, é importante uma exata identificação de quem irá acessar as informações, onde e quando e a definição de instrumentos de segurança compatíveis com as suas necessidades, de forma que os acessos a informações vitais a determinados colaboradores não sejam equivocadamente restringidos. É justamente essa correta escolha de instrumentos de segurança da informação, bem como a definição clara de acessos, que garante uma influencia positiva nos processos de obtenção e transferência de conhecimentos necessários a inovações da empresa pesquisada.

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.

COMER, D. Segurança na Internet, Rio de Janeiro: Campos, 2004.

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.

ROTHWELL, R. **Successful industrial innovation: critical success factors for the 1990s**. R & D Management, v. 22, n. 3, p. 221-239, 1992.

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

SILVA, P.T., CARVALHO, H. e TORRES, C.B.. **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.

SILVA, R.V; Neves, A. **Gestão de Empresas na Era do Conhecimento**. Lisboa: Edições Sílabo, 2003.

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.