

## Como as Empresas de Base Tecnológica protegem suas Informações e Conhecimentos?

Ernani Elias de Souza<sup>1</sup>  
Maria Celeste Reis Lobo de Vasconcelos<sup>2</sup>  
George Leal Jamil<sup>3</sup>

### RESUMO

Este artigo tem por objetivo principal analisar como as empresas de base tecnológica gerenciam e protegem suas informações e seus conhecimentos estratégicos. Para isso, utilizou-se de conceitos essenciais como dado, informação, conhecimento, gestão, gestão da informação e do conhecimento, proteção da informação e do conhecimento, além de vetores de vazamentos de informações e conhecimentos. Com a base conceitual consolidada, foi feito um estudo de caso com três empresas de base tecnológica. Para viabilizar a pesquisa, foi construído um questionário, sendo este respondido por pessoas diretamente ligadas aos processos de informações e conhecimentos organizacionais das empresas pesquisadas. Os resultados obtidos revelaram que as empresas pesquisadas não possuíam qualquer processo estruturado de gestão e proteção de suas informações e conhecimentos, apesar de todas possuírem uma clara consciência sobre a importância vital que é lidar com tais questões. Em suma, as empresas pesquisadas ainda terão que percorrer um longo caminho até viabilizarem a estruturação de seus processos de gestão da informação e do conhecimento, e também proverem a proteção de suas informações e conhecimentos. Isso abre um campo para atuação de consultores na área.

**PALAVRAS-CHAVE:** Gestão do Conhecimento, Gestão da Informação, Proteção do Conhecimento, Proteção da Informação. Empresas de Base Tecnológica

### ABSTRACT

The main objective of this article is to analyze how technology-based companies manage and protect their information and their strategic knowledge. To achieve that goal, essential concepts were used such as data, information, knowledge, management and protection of information and knowledge. A case study was carried out with three technology-based companies. A questionnaire was elaborated which was answered by people directly linked to the information and organizational knowledge processes of the companies researched. The results revealed that the companies did not have any structured process to manage or protect their information and knowledge, though all companies had a clear conscience of the importance of working with such issues. It could be concluded that the investigated companies still have a long way to go in order to structure the processes to manage and protect their information and knowledge.

**KEY-WORDS:** Knowledge Management; Information Management; Knowledge Protection; Information Protection; Technological Base Companies

---

<sup>1</sup> TESE Empreendimentos Ltda., Diretor de Tecnologia e Negócios, Mestre em Administração, [ernanielias@gmail.com](mailto:ernanielias@gmail.com)

<sup>2</sup> Fundação Pedro Leopoldo, Professora do Mestrado em Administração, Doutora em Ciência da Informação, [celestevasconcelos@gmail.com](mailto:celestevasconcelos@gmail.com)

<sup>3</sup> Universidade Fumec, professor do Mestrado em Administração, Doutor em Ciência da Informação, [gljamil@gmail.com](mailto:gljamil@gmail.com)

## 1 INTRODUÇÃO

Nas últimas três décadas, a sociedade industrial vem se deparando com uma transição para uma sociedade da informação e do conhecimento. Esta parece ser uma transição sem volta. A informação e o conhecimento serão a força motriz para todo o tipo de desenvolvimento, seja ele econômico e/ou social. Nesse tipo de contexto, o sucesso será obtido através do que se sabe, assim como o diferencial entre empresas e também entre pessoas se dará pela quantidade e qualidade de informações e conhecimentos que se tem. McGee e Prusak (1994, p. 3) dizem que nesta realidade “a concorrência entre as organizações baseia-se em sua capacidade de adquirir, tratar, interpretar e utilizar a informação de forma eficaz”.

Choo (2006) e Jamil (2006) afirmam que, na concepção atual da administração, o uso da informação para criação do conhecimento e também o armazenamento e a disseminação do conhecimento desempenham um papel imprescindível no crescimento e na capacidade de resposta às mudanças ambientais a que as organizações são submetidas, com a necessidade de reações rápidas às mudanças de um mercado dinâmico e incerto.

As organizações necessitam de informações oportunas e conhecimentos personalizados, para efetivamente auxiliar os seus processos decisórios e a sua gestão empresarial, principalmente por estarem enfrentando um mercado altamente competitivo, globalizante e turbulento. De forma permanente, elas buscam adequação e ajustes entre suas funções e operações cotidianas com as reais efetivas necessidades do meio ambiente interno e/ou externo em que estão inseridas, por meio de decisões e ações de seus gestores (JAMIL, 2006, p. 77).

Sêmola (2003) corrobora os estudos dos autores McGee e Prusak (1994) e Choo (2006) no que se refere às mudanças e novidades que surgem no mercado e obrigam as empresas a se adaptarem e reagirem de forma ágil, e para isso os aliados são a informação e o conhecimento. Tal fato gera a necessidade do compartilhamento da informação, conforme a prática moderna de gestão, para que as empresas consigam a velocidade necessária em suas ações. Diante desse cenário, se torna evidente a necessidade de proteção da informação e do conhecimento, de caráter estratégico, uma vez que desses objetos nascem os diferenciais competitivos, bem como sua manutenção. Neste processo, as organizações precisam adotar controles de segurança, que abrangem uma grande diversidade de iniciativas, indo dos cuidados com os processos de comunicação entre organizações e intraempresarial à segurança de pessoas, mídias e componentes de Tecnologia da Informação. Sendo assim, as empresas se tornam cada vez mais dependentes das informações e de seus conhecimentos estratégicos para conseguirem se manter em seus mercados, por isso a necessidade da proteção da informação e do conhecimento. É nesse meio que se desenvolve este trabalho, abordando as nuances desse contexto.

Os fatos e estudos citados anteriormente geram uma inquietação traduzida pela seguinte questão: como as empresas de base tecnológica gerenciam e protegem suas informações e seus conhecimentos estratégicos?

Norteados por essa indagação, este artigo visa analisar como as empresas de base tecnológica gerenciam e protegem suas informações e seus conhecimentos estratégicos. Para isso, algumas etapas serão contempladas:

- a) analisar o processo de gestão do conhecimento em empresas de base tecnológica, segundo o modelo proposto por De Sordi (2003);

- b) analisar os vetores de vazamento dos conhecimentos das organizações, em especial as de base tecnológica, segundo proposto por Vasconcelos (2007);
- c) verificar o processo de proteção das informações e dos conhecimentos nas organizações de base tecnológica, segundo modelo proposto por Sêmola (2003);
- d) analisar o enquadramento das empresas de base tecnológica de acordo com os quatro níveis de proteção da informação e do conhecimento segundo Beal (2008).

Estas etapas se tornam importantes em uma realidade em que se evidencia dependência crescente de informações e conhecimentos por parte das empresas e pessoas para desempenharem seus papéis na sociedade. Busca-se aqui compreender o processo de contextualização e relacionamento de informações e conhecimentos no que se refere aos processos estratégicos de manutenção de competitividade e, até mesmo, de sobrevivência dos agentes envolvidos.

...estamos nos movendo em direção de uma sociedade em rede onde a oportunidade e capacidade de ter acesso e participar de redes intensivas em conhecimento – e aprendizagem – determinam a posição socioeconômica dos indivíduos e das firmas. A economia está se transformando numa hierarquia de redes com algumas redes globais no topo e uma crescente proporção de excluídos sociais na base da pirâmide. (LUNDVALL, 1992, p. 34)

Avaliando-se que organizações se tornam cada vez mais dependentes de informações e conhecimentos para conseguirem se manter em seus mercados, torna-se oportuno analisar a necessidade de segurança para a proteção destes acervos. O presente estudo tem, portanto, como objetivo a análise de processos de gestão e proteção do conhecimento e da informação, visando criar e manter diferenciais competitivos em um mercado dinâmico em que, ao lado da competição, há também a necessidade de cooperação entre as organizações para que todas consigam alcançar seus objetivos e metas.

A pesquisa ocorreu em empresas de base tecnológica, sediadas em Belo Horizonte, escolhidas em virtude de serem potenciais criadoras de conhecimentos e gestoras de informações, sendo que sua sobrevivência depende da manutenção desse processo.

O artigo está estruturado em cinco seções, incluindo esta introdução. A seção 2 apresenta o referencial teórico do estudo, envolvendo a descrição de conceitos relativos à gestão da informação e do conhecimento e a importância da proteção destes ativos intangíveis na sociedade atual. A seção 3 apresenta a metodologia utilizada na pesquisa, ressaltando-se a pesquisa de campo, com aplicação de questionários. A seção 4 resalta os principais resultados obtidos na pesquisa e é seguida pelas conclusões (seção 5).

## **2 REFERENCIAL TEÓRICO**

Este artigo tem como fundamentação um relacionamento entre diversos conceitos que proporcionam um aprendizado sobre o tema, cujos resultados somente serão entendidos se houver uma clara exposição dessas bases. Para isso, se faz essencial o conhecimento do conceito de dado, informação, conhecimento e gestão, que são bases para que em momento adequado seus entrelaçamentos possam gerar os resultados esperados, além da compreensão dos mesmos.

### **2.1 Dado, informação e conhecimento**

Para iniciar o entendimento do tema, é necessário discorrer sobre a base de uma informação, que se dá através de dados, sendo que estes representam o ponto de partida para o entendimento e a construção de uma “escada do saber”, na qual eles representam o primeiro degrau. (JAMIL, 2006)

Segundo Ferreira (1977), dados são elementos que servem de base para a formação de juízos ou para a resolução de problemas, desde que estes sejam estruturados, contextualizados, relacionados e processados. Chiavenato (1997, p. 108) diz que um dado “é apenas um índice, um registro, uma manifestação objetiva, passível de análise subjetiva”. Quando classificados, relacionados e armazenados, são bases para a criação da informação. O dado por si só, sem relacionamento, não tem valor.

Os dados têm um relacionamento com informação em uma contextualização direta, sendo que os mesmos serão agrupados e processados resultando em informação. (JAMIL, 2006) De modo geral os dados servirão de matéria-prima para a construção da informação.

O conceito, a noção e o juízo que se tem de informação é bem vago e intuitivo. (SIMON, 1999) Ferreira (1977) define a informação como sendo o “ato de informar”, o que não conceitua objetivamente, não obstante consegue-se identificar o que é informação de forma intuitiva. Jamil (2006, p. 17) relata que pode se considerar a “informação como um elemento composto a partir de um conjunto de dados relevantes para uma análise, contextualizados”.

De acordo com McGee e Prusak (1994), a informação é utilizada como matéria-prima para a construção do planejamento voltado à construção da competitividade nas organizações; se essa postura não for adotada pela organização, se arriscará a ficar em uma posição desfavorável e até mesmo ultrapassada perante seus concorrentes mais capacitados no que se refere à busca e ao processamento da informação. Segundo Rezende e Abreu (2006), a informação tem inestimável valor quando é usada para conhecer situações e características de pessoas, processos, sistemas, recursos financeiros, tecnologias, entre outros. Isso pode gerar poder para quem possuir tais informações, seja pessoa física ou organização.

McGee e Prusak (1994) afirmam que a informação é um dos principais recursos para a confecção da estratégia de uma empresa, não sendo o único, mas é este que deve ser bem desenvolvido em termos de sua construção e forma de captação para que não haja falha na formação da estratégia, pois, se uma pequena informação incorreta for adicionada às variáveis utilizadas, o resultado do plano estratégico da empresa pode possuir grandes erros em termos de seu direcionamento, podendo ocasionar falha de competitividade em seu mercado de atuação ou até mesmo a falência da empresa. McGee e Prusak (1994) também afirmam que o uso efetivo da informação é muito importante para a construção da estratégia competitiva. A própria estratégia competitiva é um “mapa de informações” que responderá às perguntas sobre de que maneira a empresa deverá se portar, em um mundo onde a informação desempenha um papel preponderante. (MINTZBERG *et al.*, 2006) Além disso, esse “mapa” direcionará quais informações são mais relevantes para a manutenção e o aprimoramento de sua sustentabilidade e competitividade da organização. Isso é essencial no processo de desenvolvimento do conhecimento organizacional.

Segundo Wielinga (2000), conhecimento é resultado da interpretação da informação e de sua utilização para algum fim, especificamente para gerar novas ideias, resolver problemas ou tomar decisões. O processo de geração do conhecimento é através da captação, interpretação, assimilação e absorção de informações. Para Davenport e Prusak (1998, p. 19), o “conhecimento é a informação mais valiosa (...) é valiosa precisamente porque alguém deu à informação um contexto, um significado, uma interpretação; alguém refletiu sobre o conhecimento, acrescentou a ele sua sabedoria”.

Vasconcelos (2000, p. 29) afirma:

O conhecimento é identificado como a crença produzida (ou sustentada) pela informação. Assim a informação é um fluxo de mensagens, enquanto o conhecimento é criado por este mesmo fluxo de informação ancorado nas crenças e compromissos do seu detentor.

Albrecht (1999, p. 109) relata que conhecimento é:

Conteúdo de valor agregado do pensamento humano, derivado da percepção e manipulação inteligente das informações. Os conhecimentos são transcendentais. Existem apenas na mente do pensador. São a base de ações inteligentes.

Na sociedade contemporânea a informação e o conhecimento são os fatores mais importantes para a construção dos diferenciais competitivos, planejamentos e gestão das organizações. Para isso é citado o conhecimento prático nos processos organizacionais, não seu sentido abstrato ou teórico. Este conhecimento relacionado às organizações é referente ao seu mercado, aos seus processos e atividades, seus clientes, sua tecnologia, seus concorrentes, entre outros. (TEIXEIRA FILHO, 2000)

## **2.2 Gestão da informação e do conhecimento**

De Sordi (2003) define gestão como sendo planejar, organizar, liderar e controlar as pessoas que constituem uma organização, bem como tarefas, processos e atividades por elas desempenhadas. Para Chiavenato (1997), gestão é o processo que envolve o planejamento, o desenvolvimento, o controle e a ação dentro de uma organização, seja em termos de recursos físicos, procedimentos ou pessoas.

Houaiss (1981) descreve gestão como sendo um conjunto de normas e funções elaboradas para organizar componentes de produção, para alcançar resultados esperados de forma eficaz e prover todas as expectativas de retorno. Mendes (2002) relata que a gestão moderna é composta de vários componentes que devem interagir em harmonia. O autor descreve a interdisciplinaridade, complexidade, exiguidade, multiculturalidade, inovação e competitividade como sendo processos que devem ser abordados pela gestão para que haja a possibilidade de alcançar os objetivos organizacionais. Uma vez descrito o conceito de gestão, deve-se fazer uma ligação deste com a informação e o conhecimento.

De Sordi (2003, p. 117) destaca que “a política informacional define as diretrizes para o gerenciamento e uso das informações corporativas”. A maioria das empresas prefere ignorar a política informacional, embora esteja nela um modelo implícito de poder informacional. Este modelo de poder informacional é componente importante para a construção do processo de gestão da informação. O surgimento de um modelo informacional que gera poder requer que os executivos da empresa falem de forma direta e clara sobre a política informacional.

Componente importante também é a equipe informacional, que não deve ser limitada aos profissionais de Tecnologia da Informação. Ela deve abranger todas as pessoas que possam agregar valor à informação. A equipe informacional deve sempre se preocupar em adicionar valor à informação, contextualização, condensação, adequação à política informacional e escolha dos melhores meios para a construção do fluxo da informação. (DE SORDI, 2003)

E, por último, mas não menos importante, a infraestrutura informacional, que compreende os recursos utilizados para atender às necessidades específicas da empresa em relação à informação. A essa arquitetura estão ligados os software utilizados, as garantias de confidencialidade de

determinadas informações, mapas, documentos, diretórios e pessoal especializado. A arquitetura informacional faz a ligação entre comportamento, processos e pessoal especializado com a estrutura da organização, espaço físico e métodos administrativos. Ela deve prover uma facilidade de acesso a informações, evitar redundâncias e problemas de integridade pela sua reutilização, e gastos desnecessários na compra ou geração de informações irrelevantes ou já existentes. (DE SORDI, 2003; STAIR; REYNOLDS, 2008)

O alinhamento desses componentes vai gerar a construção de um modelo de gestão da informação que seja eficaz, propiciando à empresa a utilização das melhores práticas em relação ao uso, à retenção, ao refinamento, à distribuição e à utilização da informação. (STAIR; REYNOLDS, 2008) Aliado a isso, McGee e Prusak (1994) afirmam que deve haver gerência ativa com responsáveis bem identificados para os processos, com o reconhecimento da importância para a organização dessa gerência.

Segundo Davenport e Prusak (1998), o processo de gerenciamento da informação pode ser único e gerar resultados diferentes: depende do tratamento dos detalhes que envolvem a informação, da organização financeira ou de marketing, e do estilo do gestor. De forma geral, Davenport e Prusak (1998) propõem um modelo genérico de gerenciamento da informação apresentado pela Figura 1:

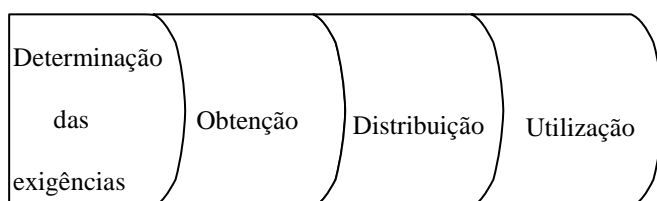


FIGURA 1 – O processo de gerenciamento da informação

Fonte: DAVENPORT; PRUSAK, 1998, p. 175.

Mesmo que seja proposto um modelo de gestão da informação bem definido, não há garantia de sucesso. Trata-se de estruturação necessária, pois será a base para a construção do conhecimento organizacional. E este sim deve gerar resultados esperados, mas também depende de uma gestão eficaz. (DAVENPORT; PRUSAK, 1998)

De Sordi (2003) propõe um ciclo de gestão do conhecimento com nove passos: identificar necessidades, obter, distribuir, utilizar, aprender com conhecimentos gerados, contribuir com a geração, avaliar os conhecimentos da organização, construir e sustentar a infraestrutura de conhecimento organizacional e descartar conhecimentos não relevantes para a organização.

A Figura 2 mostra graficamente a relação entre os passos da gestão do conhecimento:

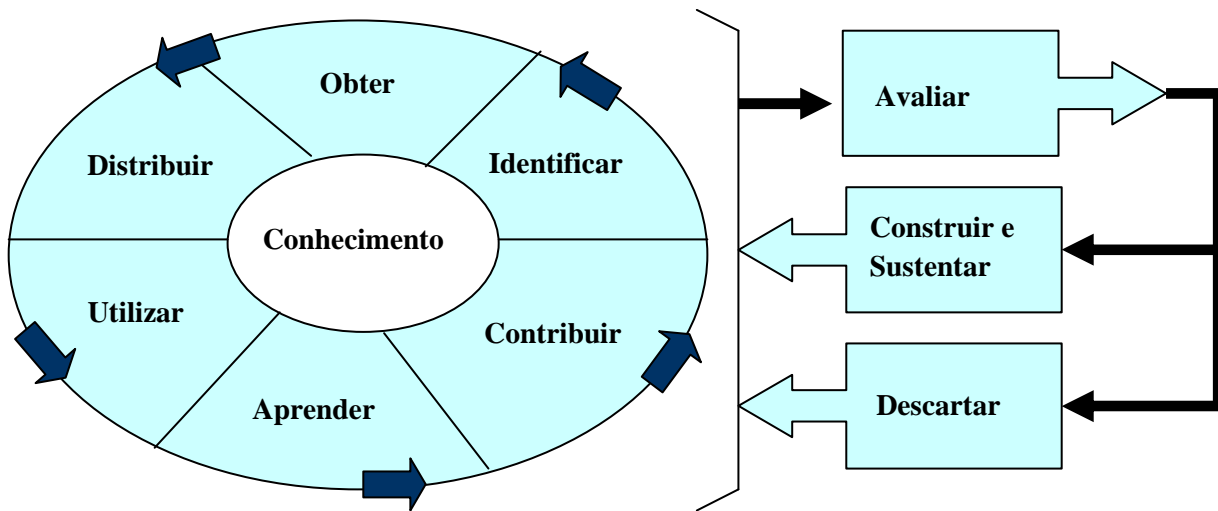


FIGURA 2 – Passos que compõem o ciclo para o gerenciamento do conhecimento (KM)

Fonte: DE SORDI, 2003, p. 113.

As empresas que adotam práticas de gestão do conhecimento, geralmente, são aquelas que se destacam em seus setores de atuação, tendo uma postura sempre inovadora e sólida, ao mesmo tempo, perante seu mercado. Essas empresas estão sempre aprimorando seu potencial inventivo, por meio de novos conhecimentos e ideias que, possivelmente, agregarão valor aos seus produtos e serviços. Tal postura manterá seu diferencial competitivo que é a base para a manutenção de sua posição de destaque. Por isso, além de cuidarem de seus processos de gestão da informação e do conhecimento, elas precisam proteger tais ativos. (DE SORDI, 2003)

### 2.3 Proteção da informação e do conhecimento

Segundo Sêmola (2003), é inegável que todas as empresas, independente de seu *core business* ou segmento de mercado, necessitam de proteger suas informações operacionais, táticas e estratégicas, seja para manter sua produtividade, reduzir custo, aumentar sua fatia de mercado, conseguir otimização de processos, competitividade ou apoio à tomada de decisão. Cada vez mais as empresas se tornam dependentes da informação, e por isso elegem sua proteção como fator importante.

Sêmola (2003) define segurança da informação – proteção da informação – como sendo uma área de conhecimento que se dedica a ações de proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Stewart (2002) afirma que hoje existe uma possibilidade muito maior de haver vazamento de conhecimentos e informações de uma empresa do que no passado, devido aos novos processos que trabalham os fluxos de conhecimentos e informações nas organizações. Além disso, o autor relata que o risco de fazer o vazamento desses conhecimentos de forma anônima é muito menor do que dois anos atrás, mas ainda é maior do que se fazia na década de 70. Essa possibilidade de anonimato incentiva ações que promovam tal vazamento. Com tudo isso, as empresas se veem na necessidade de criarem medidas mais eficazes para a proteção do conhecimento contra os novos riscos. A empresa tem que tomar atitudes que vão desde cobrar posicionamentos éticos de seus colaboradores até medidas de punição tanto administrativas quanto policiais, de acordo com leis vigentes.

Vasconcelos (2007) disserta sobre as políticas de proteção ao conhecimento que são cada vez mais complexas devido aos ambientes internos e externos referentes à organização. O tema se tornou muito importante despertando interesse em pesquisadores, que de forma constante buscam criar melhores formatos para os processos da cadeia produtiva, fazendo com que os mesmos aconteçam visando à competitividade. Tais processos buscam também que as empresas possam mitigar a fuga

de seus conhecimentos estratégicos. Essa preocupação se dá devido ao grande fluxo de conhecimento intra e interorganizacional inerentes ao processo de relacionamento na atual cadeia produtiva. Todo esse processo produz impactos que podem ser positivos ou negativos para a vida organizacional.

Tanto a proteção da informação quanto a proteção do conhecimento estão sob uma mesma ótica. Para lidar com processos estruturados de proteção da informação e do conhecimento, Sêmola (2003) afirma que há necessidade de uma análise do risco, que deve ser feita atentando para o estudo e a compreensão de algumas variáveis que o compõem. Estas variáveis são:

- a) Ameaças: são, por características de formação, externas às informações e seu processo de construção. Podem ser consideradas ameaças os agentes ou condições que causam incidentes que comprometem os ativos da informação por meio de exploração de vulnerabilidades, provocando perda em confidencialidade, integridade e disponibilidade e, conseqüentemente, causando impactos aos negócios de uma empresa.
- b) Vulnerabilidades: essencialmente são fragilidades presentes ou associadas aos ativos informacionais, que, exploradas pelas ameaças, causam incidentes de segurança. As vulnerabilidades por si só não geram problemas aos ativos da informação, por sua característica passiva.
- c) Impactos: trazem a abrangência das conseqüências causadas por um incidente de segurança sobre processos de negócio.
- d) Medidas de segurança: representam as práticas, os procedimentos e os mecanismos para a construção de processos de proteção. O principal papel das medidas de segurança é impedir que as ameaças explorem as vulnerabilidades, gerando impactos.

Para efetivar a proteção da informação, Sêmola (2003) propõe que seja criado um comitê corporativo de segurança da informação como sendo a espinha dorsal do processo. Este comitê tem o objetivo de representar os interesses da empresa diante dos desafios que a sociedade da informação e do conhecimento impõem ao negócio. Tal comitê tem a responsabilidade de criar processos e procedimentos que vão mitigar o risco em relação aos ativos informacionais. É parte de seu papel, também, estudar vazamento da informação e do conhecimento.

## **2.4 Vazamento da informação e do conhecimento**

Existe proximidade da informação com o conhecimento de forma que, em determinados momentos, somente uma análise mais profunda da contextualização pode desvendar se é conhecimento ou informação. Essa constatação se dá através da verificação do tipo de conhecimento com que se está lidando, pois alguns autores não reconhecem o conhecimento explícito como conhecimento, mas sim como informação. Nessa conjuntura, o assunto vazamento da informação e do conhecimento ora pode fazer uma análise do ponto de vista da informação, ora do conhecimento, mas todas as colocações são pertinentes aos dois objetos. (DAVENPORT; PRUSAK, 1998; CHOO, 2006)

As organizações devem, cada vez mais, aprimorar seus processos de proteção da informação e do conhecimento diante da amplitude e complexidade de seus papéis dentro da empresa. A fase ou camada desse processo que deve ter uma ênfase maior é a descoberta do vazamento de informações e conhecimentos, abordando suas rotas, envolvidos e suas conseqüências, para que sejam norteadores de ações para a proteção dos ativos informacionais. (SÊMOLA, 2003)



Uma parcela cada vez maior do vazamento de conhecimentos se dá através de variáveis incontrolláveis pela organização que fazem parte dos principais processos em seu dia a dia, como por exemplo pessoas, parceiros e o próprio ambiente. (STEWART, 2002)

A definição de vazamento do conhecimento é a possibilidade de haver perda ou escoamento indevido de conhecimento e informações, que são críticas para a organização; tais conhecimentos e informações são críticos para o bem-estar da empresa em seu mercado, e podem vir a parar sob o domínio de seus concorrentes ou pessoas não autorizadas. (VASCONCELOS, 2007) Tal escoamento pode ser de forma intencional ou acidental, segundo Mohamed *et al.* (2006).

Kaplinsky *et al.* (2006 *apud* VASCONCELOS, 2007) salientam que o vazamento de conhecimento deve ser avaliado segundo um relacionamento ponderado entre perdas e ganhos no contato de ações estratégicas. Isso revela que existem consequências positivas e negativas no processo de vazamento de informações e conhecimentos. Os autores falam que a bibliografia disponível é falha quanto à abordagem de consequências positivas em algumas situações de vazamento de conhecimento. Outras visões falhas, segundo os autores, são o fato de não haver discussão sobre o grau de intencionalidade do vazamento do conhecimento, além das técnicas para construção de uma política e estratégia de proteção do conhecimento organizacional.

## **2.5 Vetores do vazamento de conhecimento**

Kaplinsky *et al.* (2006 *apud* VASCONCELOS, 2007) dizem que existem seis pontos-chaves que são vetores de vazamento do conhecimento, a saber: fornecedores, clientes, concorrentes, colaboradores, relacionamento da empresa com o sistema de inovação e ações relacionadas à propriedade intelectual. Os processos do dia a dia organizacional levarão a múltiplas interações referentes a cada um dos pontos citados acima com outras empresas. Esse dia a dia organizacional pode levar a ações intencionais como, por exemplo, entrega de uma fórmula para criação de um produto industrializado que será componente de outro produto, ou não intencionais, como, por exemplo, o pedido de demissão de um gerente de pesquisa e desenvolvimento, o que resultará no vazamento de conhecimento, que poderá gerar consequências positivas ou negativas.

Sobre o vazamento do conhecimento e seus vetores, Mohamed *et al.* (2006) afirmam que estes objetos são conceitos crescentemente estratégicos. As empresas devem construir uma forma de análise do vazamento de conhecimento de forma explícita e intencional, e não de forma implícita e não intencional, como normalmente as organizações fazem. Nos processos de gestão do vazamento de conhecimento devem ser criadas rotinas que maximizem os impactos positivos e mitiguem os impactos negativos, em todos os níveis organizacionais. As empresas devem ser conscientes de que há vazamento de conhecimento tanto nas empresas grandes quanto nas pequenas e médias. Deve ser uma máxima o fato de que as empresas trabalham em diferentes redes com variado grau de confiança entre os membros.

Seguindo as argumentações dos autores, faz-se necessária uma classificação das empresas, segundo suas ações para garantir que haja gestão e proteção de suas informações e conhecimentos. Essa classificação serve para que as organizações tomem ciência de sua real postura em relação ao tema, bem como instrui passos no sentido de evoluir para o próximo nível de maturidade.

## **2.6 Nível de maturidade da proteção à informação e ao conhecimento**

Beal (2008) propõe a questão da proteção em quatro níveis: inicial, reativo, proativo e adição de valor.

- a) No nível inicial, que é o Nível 1, os problemas são tratados de forma isolada e dependem de iniciativas individuais dos envolvidos. Nele a documentação do processo é incompleta ou

inexistente, e a organização não possui uma forma estruturada e formalizada para as ações e responsabilidades referentes aos ativos informacionais.

b) No Nível 2, que é reativo, já existe uma política de segurança corporativa e desenvolvem-se planos de proteção. Já existem algumas documentações referentes ao processo de proteção, mas os problemas são trabalhados à medida que são identificados, não havendo processo sistêmico de monitoração do ambiente, avaliação dos controles implementados e correção de falhas.

c) O nível proativo, que é o Nível 3, os processos de proteção são implementados de maneira consistente e integrada, além de serem reforçados por ações de treinamento e conscientização. As informações e os conhecimentos passam por um processo de classificação de criticidade e probabilidade de acontecimento de quebra de segurança para a construção dos processos de sua proteção. Testes frequentes são executados para a avaliação dos processos construídos e seus resultados analisados. Há uma monitoração do ambiente externo para avaliação de novas ameaças; este ambiente é externo à organização, mas pode ser interno à rede de sua participação.

d) Já no nível de adição de valor, que é o Nível 4, a proteção do conhecimento e da informação é vista como parte integrante dos processos estratégicos da organização. A aquisição ou o desenvolvimento de conhecimentos leva em consideração os princípios para sua proteção. Existe todo um trabalho de análise e gestão do risco no contexto no qual a organização está inserida. Este nível propõe uma monitoração constante das agitações do ambiente para haver uma reação imediata a problemas de proteção relacionados a mudanças organizacionais, estratégicas ou tecnológicas, além de promover os ajustes necessários.

Beal (2008) afirma que nem todas as empresas conseguirão trabalhar em todos os processos de proteção no nível ideal que, segundo ela, é o quatro. Cada empresa terá, segundo suas possibilidades de investimentos financeiros e também segundo sua visão em relação à proteção do conhecimento e das informações, um formato que se encaixará em um dos níveis propostos.

Esses níveis servem para as organizações identificarem seu posicionamento e, diante disso, tomarem ações para lidarem de forma efetiva com suas informações e seus conhecimentos. Todos os conceitos apresentados formam a base para a análise da pesquisa realizada que será descrita a seguir.

### **3 METODOLOGIA**

Com base no que afirma Michel (2005, p. 36), dando ênfase às principais características de uma pesquisa, “os fatos e os fenômenos devem ser extraídos do ambiente natural, da vida real, onde ocorrem, e analisados à luz das influências que o ambiente exerce sobre eles”; por esse motivo uma pesquisa de campo deve ser orientada segundo princípios da pesquisa descritiva e exploratória.

O tipo de estratégia adotado nesta pesquisa foi o estudo de casos, com propósito exploratório. Conforme Yin (2005), a preferência pelo uso de estudo de casos deve ser utilizada quando o estudo suporta eventos em que é possível se fazerem observações diretas, aplicação de questionários e entrevistas sistemáticas. O autor diz que o estudo de casos é comumente um método de pesquisa específico para estudos exploratórios, mas que há possibilidade de seu uso em estudos descritivos e causais. O que proporciona essa flexibilidade é a forma de coleta de dados, que deve adaptar-se aos objetivos e às especificidades de cada estudo.

Para apoiar o estudo de caso foi realizada uma pesquisa bibliográfica. Essa busca conceitual foi para balizar a contextualização, a análise dos resultados, e para a construção de proposições das quais as organizações podem se utilizar.

Para objeto da pesquisa, foram selecionadas três empresas de base tecnológica, situadas em Belo Horizonte. Foi delimitado que respondessem aos questionários gerentes e diretores, ligados diretamente ao nível estratégico das empresas, e que lidam com informações e conhecimentos das mesmas. Para a coleta de dados, foi elaborado um questionário com 11 perguntas de caráter subjetivo, abordando pontos específicos pertinentes ao estudo.

O método apresentado se limita pelo pequeno número de empresas estudadas e pela ausência de um contato pessoal com os respondentes.

## **4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS**

Foram pesquisadas três empresas de base tecnológica, sendo que a Empresa 1 é de grande porte e atua com desenvolvimento de softwares, que é a atividade da Empresa 2, mas esta segunda é de pequeno porte. A Empresa 3 também é de pequeno porte e trabalha especificamente com treinamento de uso do software SAP.

Foram feitas perguntas sobre o conceito de informação e conhecimento, e as respostas sugeriram que elas não conhecem de forma clara tais conceitos. A Empresa 1 demonstrou uma percepção de que ambos são importantes para o sucesso da organização. Isso pode gerar ações futuras para a melhor compreensão deles. As Empresas 2 e 3 classificaram a informação como sendo igual a dado, sendo que a Empresa 3 faz referência a uma necessidade de organização desses dados para que haja uma valorização dos mesmos. As três empresas relacionam o conhecimento com experiência e com informações, mas mesmo assim, tanto em relação ao conceito de informação quanto ao de conhecimento, elas se mostram dispersas em relação ao descrito por Davenport e Prusak (1998). Feita a verificação dos conceitos de dado e informação, passam a ser analisados os módulos do modelo proposto por De Sordi (2003) referente à gestão do conhecimento, abordando o primeiro módulo, que é a captação do conhecimento.

### **4.1 A gestão do conhecimento nas empresas pesquisadas**

A Empresa 1 reconhece que não há uma estratégia definida para captação de conhecimento, mas descreveu pelo menos uma ação que serve de base para, possivelmente, captar ou criar algum conhecimento que será útil para a organização. Essa ação é direcionada ao compartilhamento de informações sobre concorrentes e suas ações no mercado, o que pode gerar conhecimento aos colaboradores, os quais se utilizaram disso para ações e/ou construção de planejamentos para a manutenção da competitividade organizacional.

A Empresa 2 descreveu algumas ações e situações que proporcionam a captação de informações e, possivelmente, de conhecimentos, mas a mesma não reconhece isso. Mesmo descrevendo processos que podem ser geradores de conhecimento, como propõe De Sordi (2003), ela disse que não há estratégia para a produção de conhecimento.

Já a Empresa 3 disse que existe uma estratégia referente à captação de conhecimento, mas descreve ações que sugerem a falta de um processo estruturado, possuindo apenas ações isoladas e de responsabilidade dos colaboradores. A análise dessa fase sugere que as empresas pesquisadas ainda não possuem um processo de gestão do conhecimento estruturado, ou não têm a percepção de sua existência.

### **4.2 Vetores de vazamento dos conhecimentos nas organizações**

Para a análise dos vetores de vazamento de informações e de conhecimentos, foi utilizado como base o que é referenciado por Vasconcelos (2007).

Foram realizados alguns questionamentos para a verificação da consciência sobre os vetores de vazamento dos conhecimentos nas organizações. Em primeira instância, foi perguntado às empresas sobre quais as principais rotas (processos) de vazamentos de informações e de conhecimento, como acontecem e quais os impactos negativos e positivos percebidos por elas.

Pôde-se inferir que a Empresa 1 ainda não distingue quais são vetores de vazamento dos seus conhecimentos. A Empresa 2 descreveu como principais vetores seus colaboradores e clientes, com uma ênfase nos clientes. A empresa tem uma visão de fatores positivos como, por exemplo, um processo de *benchmark* que mostra uma melhor performance de seu software, sendo que isso pode lhe render bons rendimentos. Mas sua maior preocupação é sobre os fatores negativos do vazamento do conhecimento, em que descreve o vazamento de códigos (linhas) de um programa (software) fonte (principal) como sendo um dos mais graves problemas gerados por um vazamento, pois neste código pode estar o diferencial de seu produto em relação ao concorrente. Com tais fatos, a Empresa 2 sugere que possa haver tanto ações intencionais quanto não intencionais nos processos descritos. A Empresa 3 tem uma percepção somente positiva do vazamento de seus conhecimentos e demonstra que todas as ações de vazamento são intencionais. Ela não faz nenhuma menção às formas não intencionais de vazamento de conhecimentos e nem mesmo a suas abordagens negativas.

Para analisar sobre o que as empresas têm de percepção em relação às consequências do vazamento de conhecimento, foi proposto a elas que relatassem seu entendimento sobre a afirmação de que o vazamento das informações e dos conhecimentos pode ter consequências positivas e negativas.

As declarações observadas revelam que a Empresa 1 só possui a visão de que o vazamento do conhecimento traz consequências negativas para a organização, mas relata um projeto para ações estruturadas em relação a isso. A Empresa 2 se declara em acordo com a afirmação, mas demonstra que construiu uma análise sobre um vazamento intencional em relação aos pontos positivos, e colocou como crítico as consequências negativas. A Empresa 3 declara que as consequências são mais positivas que negativas e ressalta as ações intencionais de vazamento de conhecimentos. Ante as afirmações efusivas sobre consequências negativas relacionadas ao vazamento do conhecimento e de informações, a proteção das informações e dos conhecimentos tem uma ênfase em meio ao ambiente organizacional. O ponto positivo fica por conta de uma visão sobre consequências positivas em um processo de vazamento de informações e conhecimentos.

### **4.3 O processo de proteção das informações e dos conhecimentos**

Para a construção do processo de proteção das informações e dos conhecimentos deve-se fazer uma análise de risco com foco nos ativos informacionais da organização, que contêm tanto suas informações quanto seus conhecimentos. Esta análise é proposta relacionando as variáveis que compõem o processo de análise de risco, tratado por Sêmola (2003). Para a análise foi perguntado às empresas se existe, em seus processos organizacionais, uma estratégia de análise de risco da informação segundo as variáveis ameaças, vulnerabilidades, impactos e medidas de segurança.

Em relação à variável ameaça, a Empresa 1 diz não possuir conhecimento sobre. A Empresa 2 não deixa claro que não possui conhecimento sobre ameaças, enquanto a Empresa 3 diz não possuir qualquer mecanismo para identificação dessa variável. Quanto às variáveis vulnerabilidades e impactos, nenhuma das empresas possui ainda uma percepção da abrangência delas. Somente a variável medidas de segurança é percebida pelas Empresas 2 e 3, mesmo assim em um nível

superficial e para processos específicos. Já a Empresa 1 diz desconhecer essa variável. Diante do exposto pelas respostas revela-se que as três empresas não possuem ainda um processo estruturado de análise de risco, sendo que as Empresas 2 e 3 ainda relatam pequenas medidas de segurança em alguns processos. Dessa forma, se torna necessário tratar a ameaça de perda de informações e de conhecimentos com a saída de colaboradores.

Para a continuidade da pesquisa, foi perguntado às empresas como é feito para que as informações e conhecimentos essenciais sejam preservados de forma constante.

As empresas demonstraram não fazer análises de incidentes que possam acontecer e ameaçar a integridade das informações e dos conhecimentos organizacionais. A Empresa 1 relatou um processo isolado e sem estruturação para tentar garantir a salvaguarda de informações e de conhecimentos. As Empresas 2 e 3 demonstraram, através de suas respostas, que ainda não têm processo estruturado para garantir a proteção das informações e dos conhecimentos.

#### **4.4 Os quatro níveis de proteção da informação e do conhecimento**

O trabalho desenvolvido por Sêmola (2003) se junta à proposição do modelo apresentado por Beal (2008), que propõe uma referência para enquadrar as empresas seguindo níveis em relação a suas práticas de proteção da informação e do conhecimento estratégico, conforme relatado no referencial teórico.

Para situar as empresas em relação a seu enquadramento, perguntou-se como elas tratam o termo vazamento de informações e de conhecimentos, e as consequências trazidas por ele. Como complemento, foi solicitado às empresas que relatassem se existia uma política de gestão do vazamento de informações e de conhecimentos, sendo que, se possuísem, descrevessem-na de forma breve.

De acordo com as respostas, todas as empresas pesquisadas se encontram no nível um, que é o nível inicial. Beal (2008) relata que as empresas que se encontram neste nível tratam os problemas relacionados à proteção da informação e do conhecimento de forma isolada e dependem de iniciativas individuais dos envolvidos para que haja solução dos problemas detectados em relação a essa proteção. A autora ainda ressalta que, neste nível, a documentação do processo é incompleta ou inexistente, e a organização não possui uma forma estruturada e formalizada para as ações e responsabilidades referentes aos ativos informacionais.

#### **4.5 Recomendações para as empresas pesquisadas**

De acordo com os resultados alcançados, pode-se utilizar da contribuição de alguns autores para descrever ações que auxiliarão as empresas com a gestão e proteção de suas informações e de seus conhecimentos estratégicos. Essas ações devem seguir as seguintes recomendações propostas:

- a) De Sordi (2003) recomenda a criação de um ciclo com práticas de gestão do conhecimento, pois a construção deste poderá proporcionar a melhoria no compartilhamento dos conhecimentos já existentes na organização ou o aprimoramento de seu potencial inventivo, por meio da criação de novos conhecimentos e ideias que agregarão valor em seus produtos e/ou serviços.
- b) Vasconcelos (2007) ressalta a importância da identificação de vetores de vazamento de conhecimentos para uma avaliação quanto a sua forma, intencional ou não intencional, e avaliação de suas consequências, se positivas ou negativas, proporcionando controles que reduzirão os impactos negativos e potencializarão os positivos.

c) Sêmola (2003) recomenda a criação de um comitê corporativo de proteção da informação e do conhecimento para orientar as ações corporativas de proteção e todas as etapas do processo de segurança. Além disso, este comitê deve alinhar o plano de ação às diretrizes estratégicas do negócio, agregando valor e viabilizando o melhor retorno sobre o investimento.

d) Sêmola (2003) também propõe a criação de processos de identificação de vulnerabilidades, ameaças, impactos e medidas de segurança, sendo que os impactos devem ser medidos segundo sua intensidade, e as ameaças, segundo a probabilidade de acontecerem efetivando uma quebra de segurança.

e) Beal (2008) propõe a criação de índices para verificação do enquadramento da organização segundo suas práticas de proteção das informações e dos conhecimentos, encaixando-a em um dos níveis de maturidade na gestão da segurança da informação e do conhecimento.

De forma geral, essas recomendações somente serão possíveis de serem implantadas se houver a cumplicidade dos executivos da empresa, sem esquecer da participação efetiva de todos os colaboradores, independente de seus níveis hierárquicos.

## 5 CONSIDERAÇÕES FINAIS

Este artigo foi desenvolvido com o objetivo principal de analisar como as empresas de base tecnológica gerenciam e protegem suas informações e seus conhecimentos estratégicos, como sugeridos pela própria literatura aqui discutida, além de ainda oferecer sugestões de implantação de processos estruturados. Este objetivo foi plenamente atingido, pois foram colhidos dados que indicaram uma ausência de processos estruturados para o tratamento da gestão e da proteção de informações e conhecimentos estratégicos.

A pesquisa analisou o vazamento dos conhecimentos nas organizações, e as empresas pesquisadas mostraram ter consciência sobre a importância desse conceito, pois é através do conhecimento que elas desenvolvem seus processos e produtos. No entanto, indicaram ausência de processos estruturados para lidar com este vazamento. A pesquisa mostrou que as empresas necessitam estar mais atentas sobre a proteção e a gestão da informação e do conhecimento estratégico organizacional. Elas conseguem identificar poucos vetores de vazamento desses conhecimentos.

Duas das três empresas pesquisadas conseguem identificar impactos positivos do vazamento de alguns conhecimentos. Este ponto é importante, pois, conforme descrito na literatura, na maioria das empresas há apenas a visualização de pontos negativos do vazamento de informações e conhecimentos. Outro fato é que duas empresas observam os vazamentos como processos intencionais e não intencionais, sendo que a maioria das ações relatadas é intencional, gerando algum ganho para a organização.

Foi possível, com base nos autores estudados, propor alguns processos iniciais. Esta proposição é para que as empresas pesquisadas, e as empresas de forma geral, que se encontram no mesmo nível de estruturação, comecem a construir processos formais visando a gestão e proteção de suas informações e conhecimentos estratégicos.

O discurso que as empresas apresentaram está aliado ao que a literatura fornece de visão quanto à necessidade de um gerenciamento efetivo do conhecimento e à proteção de suas informações e conhecimentos. Mas essas mesmas empresas sugerem, com suas respostas à pesquisa, que na

prática se encontram distantes de se preocuparem efetivamente com tais processos. Não são reservados nem planejados os investimentos necessários para se colocar em prática o que elas ressaltam em seus discursos.

Em suma, as empresas pesquisadas participam de um grupo de organizações que sobrevivem de relacionamentos baseados em informações e conhecimentos para o desempenho de suas atividades, criação de competitividade e manutenção de suas estratégias. Essas empresas possuem certa consciência sobre a necessidade de processos que gerenciem e protejam seus ativos informacionais e seus conhecimentos estratégicos, mas não investem efetivamente no desenvolvimento dos mesmos. Isso abre um campo para atuação de profissionais que atuam com a referida estruturação.

## REFERÊNCIAS

- ALBRECHT, Karl. A 3ª revolução da qualidade. *HSM Management*, São Paulo, v. 3, n. 17, p. 108-112, nov./dez. 1999.
- BEAL, Adriana. *Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. 1. ed. 2. reimpr. São Paulo: Atlas, 2008.
- CHIAVENATO, Idalberto. *Recursos humanos na empresa*. 3. ed. São Paulo: Atlas, 1997. v. 5.
- CHOO, Chun Wei. *A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões*. 2. ed. São Paulo: Editora Senac São Paulo, 2006.
- DAVENPORT, Thomas H; PRUSAK, Laurence. *Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação*. Trad. Bernadette Siqueira Abrão. São Paulo: Futura, 1998.
- DE SORDI, José O. *Tecnologia da informação aplicada aos negócios*. São Paulo: Atlas, 2003.
- FERREIRA, Aurélio Buarque H. *Minidicionário Aurélio*. Rio de Janeiro: Nova Fronteira, 1977.
- HOUAISS, Antônio. *Dicionário básico escolar Koogan-Larousse*. Rio de Janeiro: Larousse do Brasil, 1981.
- JAMIL, G. L. *Gestão da informação e do conhecimento em empresas brasileiras: estudo de múltiplos casos*. Belo Horizonte: C/ Arte, 2006.
- VASCONCELOS, Maria Celeste Reis Lobo de. *Proteção ao conhecimento: análise dos impactos positivos e negativos do vazamento de conhecimento em empresas no Brasil e na Inglaterra*. São Paulo: KM Brasil, 2007.
- LUNDVALL, B. *National systems of innovations: towards a theory of innovation and interactive learning*. London: Pinter Publishers, 1992.
- McGEE, James; PRUSAK, Laurence. *Gerenciamento estratégico da informação: aumente a competitividade e eficiência de sua empresa utilizando a informação como uma ferramenta estratégica*. Trad. Astrid Beatriz de Figueiredo. Rio de Janeiro: Elsevier, 1994.
- MENDES, Judas Tadeu Grassi. *Finanças empresariais*. Fae Business School. Curitiba: Associação Franciscana de Ensino Superior Bom Jesus, 2002.
- MICHEL, Maria Helena. *Metodologia e pesquisa científica em ciências sociais*. São Paulo: Atlas, 2005.
- MINTZBERG, H. *et al. O processo da estratégia: conceitos, contextos e casos selecionados*. Porto Alegre: Bookman, 2006.

MOHAMED, S. *et al.* Understanding *one aspect of the knowledge leakage concept: people*. In: EUROPEAN AND MEDITERRANEAN CONFERENCE ON INFORMATION SYSTEMS (EMCIS), Costa Blanca/Alicante/Spain, July 2006.

REZENDE, Denis Alcides; ABREU, Aline França. *Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas*. 4. ed. São Paulo: Atlas, 2006.

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

SIMON, Imre. MAC 333 A revolução digital e a sociedade do conhecimento. 1999. Disponível em: <<http://www.ime.usp.br/~is/ddt/mac333/aulas/tema-11-24mai99.html>>. Acesso em: 19 abr. 2008.

STAIR, R. M.; REYNOLDS, G. W. *Princípios de sistemas de informação*. Porto Alegre: Editora Bookman, 2008.

STEWART, Thomas A. *A riqueza do conhecimento: o capital intelectual e a organização do século XXI*. Rio de Janeiro: Campus, 2002.

TEIXEIRA FILHO, Jayme. *Gerenciando conhecimento*. Rio de Janeiro: SENAC, 2000. 191 p.

VASCONCELOS, Maria Celeste Reis Lobo de. *Proteção ao conhecimento: análise dos impactos positivos e negativos do vazamento de conhecimento em empresas no Brasil e na Inglaterra*. São Paulo: KM Brasil, 2007.

VASCONCELOS, Maria Celeste Reis Lobo de. *Cooperação universidade/empresa na pós-graduação: contribuição para a aprendizagem, a gestão do conhecimento e a inovação na indústria mineira*. 248 p. Tese (doutorado) – Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2000.

WIELINGA, B. *et al.* *Knowledge engineering and management - The common KADS methodology*. Cambridge: The MIT Press, 2000.

YATES-MERCER, Penelope; BAWDEN, David. Managing the paradox: the valuation of knowledge and knowledge management. *Journal of Information Science*, United Kingdom, v. 28, n. 1, p. 19-29, 2002.

YIN, Robert K. *Estudo de caso: planejamento e métodos*. 3. ed. Porto Alegre: Bookman, 2005.