UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE CIÊNCIA DA INFORMAÇÃO

Davidson Lucas Carvalho Dias

A proteção da informação e conhecimento tecnológico no âmbito das transações eletrônicas

Belo Horizonte/ MG
2016

Davidson Lucas Carvalho Dias

A proteção da informação e conhecimento tecnológico no âmbito das transações eletrônicas

Monografia apresentada ao Curso de Especialização da Escola de Ciência da Informação da Universidade Federal de Minas Gerais, como requisito parcial para obtenção do título de Especialista em Gestão Estratégica da Informação.

Área de Concentração: Gestão Estratégica da Informação.

Orientador: Prof. Eduardo Ribeiro Felipe

Belo Horizonte/ MG

2016

RESUMO

O mercado tecnológico mundial encontra-se em constantes mudanças. Em um passado não muito distante, vivia-se em um mercado em que a valorização de uma empresa era dada mediante o tamanho do seu parque tecnológico físico. A tendência de um novo mercado que já e realidade baseia-se em suas informações e do conhecimento, onde o quanto vale uma empresa é mensurado através do número de ativos informacionais que ela possui. Nesta nova realidade a informação e o conhecimento tornam a força motriz para o desenvolvimento, seja este social e/ou econômico. Neste cenário faz-se necessário uma análise de como as informações, conhecimentos e tecnologias geradas a partir destes, são tratadas e protegidas. Este trabalho tem o objetivo de analisar a gestão da informação e do conhecimento, incluindo o processo de proteção de informações e de conhecimentos e os principais vetores de vazamento dos mesmos. A empresa pesquisada apesar de possuir um alto controle de proteção das suas informações e conhecimentos gerados, demonstraram possuir processos inseguros e alguns pontos de vazamento informacional, necessitando de revisar o seu processo com rotinas de auditorias periódicas, para a identificação das variáveis que compõem a gestão e proteção de suas informações, conhecimentos, e principalmente o seu produto de tecnologia final que é a combinação de toda a inteligência gerada. Após esta etapa a organização poderá lidar com um processo mais solido para a gestão e proteção de suas informações e de seus conhecimentos. Em suma, os aspectos mostrado duramente o trabalho remetem a uma situação em que, possivelmente, a empresa aqui utilizada como base do estudo demonstra pequenas falhas em relação aos seus processos, constituído por suas informações e seus conhecimentos. Tal situação aponta a necessidade de ações para a criação de procedimentos para melhores práticas referentes à proteção e gerenciamento de suas informações e de conhecimentos estratégicos, com foco em seu produto final de tecnologia para sua sobrevivência em um mercado cada vez mais exigente e competitivo.

Palavras-chave: Gestão do Conhecimento e da Informação. Tecnologia da Informação. Vazamento de informação e conhecimento. Produto de Tecnologia. Proteção do Conhecimento e da informação.

ABSTRACT

The global technology market is constantly changing. In a not too distant past, people lived in a market in which the valuation of a company was given by the size of your physical technology park. The trend of a new market that already and reality based on their information and knowledge where the valley as a company is measured by the number of informational assets that it owns. In this new reality the information and knowledge become the driving force for development, be it social and / or economic. In this scenario make necessary an analysis of how the information, knowledge and technology generated from them, are handled and protected. This work aims to analyze the management of information and knowledge, including information protection process and knowledge and the main leak vectors thereof. The company researched despite having a high control protection of your information and knowledge generated, shown to have unsafe processes and some informational leakage points Needing to review its process with routine periodic audits to identify the variables that make up the management and protection of your information, knowledge, and especially its end technology product and the combination of all generated intelligence. After this stage the organization can deal with a more solid process for the management and protection of your information and your expertise. In short, respects hard work shown refer to a situation where, possibly, the company used here as basis for the study demonstrates minor flaws compared to its procedures, consisting of their information and their expertise. This situation points to the need for action to the creation of procedures to best practices regarding the protection and management of its information and strategic knowledge, focusing on their ultimate technology product for their survival in an increasingly demanding and competitive market.

Keywords: Knowledge and Information Management. Information Technology. Vazamento of information and knowledge. Product Technology. Protection of knowledge and information.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 **INTRODUÇÃO**

Entendendo como suma de importância a utilização de tecnologia para tomadas de decisões estratégicas o trabalho aqui apresentado discutirá a contribuição da tecnologia da informação, gerada através de conhecimento estratégico e suas formas de proteção voltada a empresa base desta pesquisa, onde McGee e Prusak (1994, p. 3) acrescentam ainda que; as disputas saldáveis entre as organizações são muitas vezes baseadas em suas capacidades de adquirir, tratar, interpretar e utilizar a informação de forma eficaz. Outro ponto de grande relevância é o armazenamento e disseminação do conhecimento, que desempenham um papel imprescindível no crescimento e capacidade de resposta às mudanças ambientais que as organizações são submetidas, com a necessidade de respostas rápidas às mudanças de um mercado dinâmico e incerto como afirma Choo (2006) e Jamil (2006).

Como apontado por Jamil (2006) 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, globalizado e turbulento tendo assim a necessidade de proteção dos seus conhecimentos e informações. Sêmola (2003) concorda com os estudos dos autores McGee e Prusak (1994) e Choo (2006) em relação as mudanças e novidades que surgem no mercado que obrigam as empresas a se adaptarem de forma ágil, e para isso a sua maior aliada é a informação e o conhecimento.

O compartilhamento da informação é a prática comum da gestão moderna, para que as empresas consigam atender na velocidade necessária as suas ações. Diante deste cenário, se torna evidente a necessidade de proteção da informação e do conhecimento, de caráter estratégico, entendendo que na sua maioria são os grandes diferenciais competitivos. 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 intraorganizacional 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.

1.2 **Justificativa**

O avanço das tecnologias geradas a partir do conhecimento tem exercido um papel fundamental para o mercado atual e competitivo, exigindo cada vez mais das organizações. Diante desse contexto e visualizando a empresa alvo deste estudo, onde a utilização de sua base de dados e informação como ferramenta é de grande relevância para o negócio. A aplicação e a utilização de forma adequada dos resultados podem gerar grandes retornos para os negócios. Com esta visão, a pesquisa tende a mostrar como a empresa produz tecnologia de informação, conhecimento e realiza a proteção desde produto final.

1.3 **Objetivos**

O trabalho aqui apresentado tem como objetivo mostrar a importância da proteção da tecnologia geradas através de conhecimento e informação, assim como suas formas de produção e aplicação em um determinado ambiente organizacional, bem como analisar, formas de gestão das informações e seus conhecimentos estratégicos, em determinada empresa base deste estudo.

- Mostrar o processo de produção de conhecimento tecnológico;
- Apontar os principais meios de vazamento informacionais;
- Verificar o processo de proteção das informações e dos conhecimentos tecnológicos gerados.

1.4 **REFERENCIAL TEÓRICO**

1.4.1 **Dado, informação e conhecimento**

Este trabalho tem como base uma relação entre diversos conceitos, que proporcionam um aprendizado sobre o tema, onde os resultados serão melhor absorvidos com um bom entendimento destes. Sendo assim, tem grande importância a apresentação dos conceitos de dado, informação, conhecimento e gestão, que no decorrer do trabalho possam gerar o entendimento esperado.

1.4.1.1 **Dados**

Como apontado por Jamil (2006), o ponto de partida para a base de uma informação está representado pelos dados, para o entendimento e a construção de uma escada progressiva, sendo que os dados representam o primeiro degrau.

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, que quando classificados, relacionados e armazenados, são bases para a criação da informação. O dado por si só, solto sem relacionamento, não tem valor.

Brackett (1999, citado por AYRES, 2000, p.10) diz que: Os dados podem estar tanto numa forma primitiva quanto derivada. Dados primitivos são aqueles obtidos por medição ou observação de um objeto ou evento do mundo real. Dados derivados dizem respeito àqueles obtidos a partir de outros dados.

Dados podem estar numa forma elementar ou composta. Por dado elementar entende-se um fato que não pode ser subdividido sob pena de perder o significado. Já um dado composto surge a partir da concatenação de fatos individuais. Em forma geral, dados têm um relacionamento com informação em uma contextualização direta, sendo que os mesmos serão agrupados e processados resultando em informação (JAMIL, 2006).

1.4.1.2 **Informação**

McGee e Prusak (1994, p.24) afirmam que a informação deve informar, enquanto os dados absolutamente não têm essa obrigação. A informação deve ter um topo, enquanto os dados

podem ser ilimitados. Informação é uma mensagem, nas suas mais diversas formas como mostrado por Davenport e Prusak, (1998, p.4). Ler um Jornal, assistir à televisão, ler um livro, escutar uma música, uma conversa, são formas de emissão e recepção de informações. A informação deve ser sempre reutilizável, não havendo uma depreciação ou deterioração pelo seu uso, o seu valor é dado por quem a utiliza, sendo que a mesma informação pode ser muito importante e valiosa para um, mas não passar de mais uma informação, que não trará nenhuma agregação, para outro. Usar, absorver, assimilar, manipular, transformar, produzir e transmitir informação, são ações desenvolvidas durante todo o tempo.

Segundo Rezende e Abreu (2006), a informação tem inestimável valor quando é usada para conhecer situações e características das pessoas, processos, sistemas, recursos financeiros, tecnologias, entre outros. Isso pode gerar poder para quem possuir tais informações, seja pessoa física ou uma organização. Durante a vida de uma empresa são geradas, coletadas e armazenadas informações diversas, que constroem um histórico. Este histórico, em um processo sistêmico, será importante para as ações organizacionais contemporâneas e futuras.

McGee e Prusak (1994) dizem 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.

Já Davenport e Prusak (1998) não falam somente sobre a importância da informação, mas que existe a necessidade da gestão da informação, pois uma mesma informação pode ter diversos significados e valores dentro da empresa, sendo todos válidos.

Como mostra Rezende e Abreu (2006), com um pouco mais de entendimento sobre informação, visualiza-se que o dado é a base para a construção da informação e esta, por conseguinte, é Matéria prima para a geração do conhecimento, sendo que tal geração depende do talento humano e suas capacidades de transformar e protegê-la.

1.4.1.3 **Conhecimento**

Para Davenport e Prusak (1998, p. 19), o “conhecimento é a informação na sua forma 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.

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.

Nonaka e Takeuchi (1997) mencionam que o conhecimento está ligado as ações, e apontam que o conhecimento expresso em números e palavras, organizados como conhecimento explícito, como sendo apenas um grão de areia; onde o conhecimento representativo é aquele que se encontra nas pessoas, denominado tácito. Os autores, baseando-se nos trabalhos de Michel Polanyi (1997 citado por NONAKA; TAKEUCHI, 1997), falam em dois tipos de conhecimentos: o conhecimento explícito que está nos documentos, bases de dados, produtos e processos, e conhecimento tácito o qual faz parte das ações, contextos e experiências pessoais.

Choo (2006) afirma que há conhecimento na organização quando é reconhecido o relacionamento sinérgico entre o conhecimento tácito e o conhecimento explícito, e quando são desenvolvidos processos capazes de criar novos conhecimentos através da transformação do conhecimento tácito em conhecimento explícito. A este processo pode-se dizer que é uma gestão, uma forma de lidar com a garantia de manutenção do conhecimento na organização, resguardando-o para sua identificação, armazenamento, disseminação, aplicação e desenvolvimento.

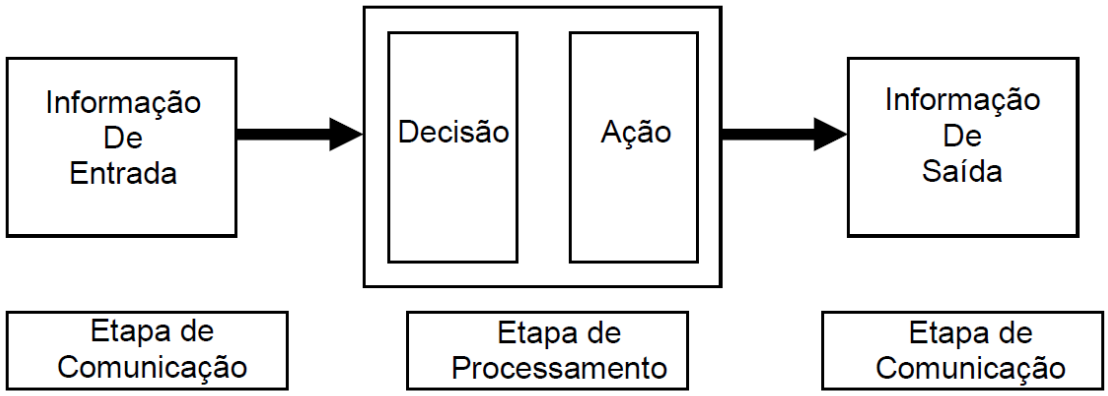
1.4.2 **Gestão da Informação e Gestão do Conhecimento**

1.4.2.1 **Gestão da Informação**

Segundo Melo (2006), o fluxo da informação depende de recursos físicos, como por exemplo, uma linha telefônica, um canal de televisão, uma rede de computadores, um modem; e também depende de recursos lógicos como os protocolos de comunicação, programas de controle de transmissão e recepção da comunicação. A junção dos recursos físicos e lógicos proporciona o meio de transmissão da informação. A origem da informação pode ser tanto interna, quanto externa a uma organização. Uma vez que a informação é

recebida ela deve ser usada de forma imediata ou, então ser armazenada, como um registro em um banco de dados, para uso em momento oportuno. O fluxo da informação é composto por etapas e estas contêm processos que se utiliza de ações para alcançar objetivos definidos de cada etapa. Às ações, é adicionada a decisão, em que se compõem o processo de utilização da informação para geração de novas informações, conforme mostrado na (FIG. 1)

FIGURA 1 – Processamento de informações



FONTE: MELO, 2006, p.32.

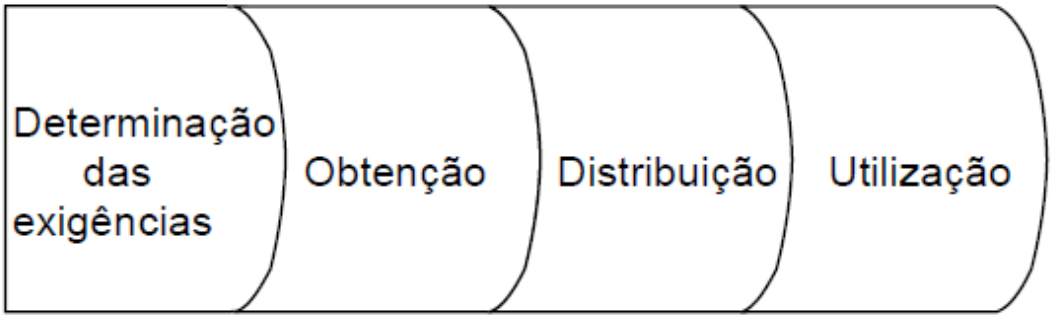
Melo (2006) afirma que todo fluxo de informação se inicia com a coleta de dados, alimentando o fluxo pela primeira vez. Todas as outras fases do fluxo dependem da coleta de dados, a qualidade da informação final também depende da coleta de dados. Se houver algum problema e/ou falha na coleta destes dados, esta será replicada por toda a cadeia do fluxo da informação. Para haver um processo de gestão de informações, deve acontecer pelo menos uma entrada de informação, seu processamento, e gerar pelo menos uma saída. O cuidado não deve ser tomado apenas na coleta de dados para que não haja erros, mas também no processamento e na comunicação, pois, se algum erro for gerado por estes processos, o mesmo perdurará até o fim do fluxo da informação, comprometendo a integridade da mesma. Outro fator relevante para ser analisado no fluxo da informação é a retroalimentação ou feedback. A informação contida na retroalimentação, muitas das vezes, é quem vai alimentar o fluxo da informação em posteriores utilizações deste fluxo, isso pode ser considerado como a alimentação por histórico.

1.4.2.1.1 *Processos de Gestão da Informação*

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 (FIG. 2)

FIGURA 2 – Processo de gerenciamento da informação



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

Segundo Davenport e Prusak (1998), embora se gaste muito tempo e recurso para fazer o levantamento das informações que são necessárias à empresa, mesmo no melhor caso, estas são insuficientes. Fazendo a inserção do método de avaliação dos principais processos estratégicos, que são responsáveis pelo sucesso da organização, analisando os pontos chaves para a organização e efetuando levantamento de necessidades informacionais; com todos esses procedimentos ainda ficará faltando alguma variável. Nem sempre os gerentes e os funcionários conhecem os fatores corretos para a execução de sua análise. Devido a todos os fatos expostos, o processo de gerenciamento da informação deve ser bem compreendido, começando pela determinação das exigências.

Mintzberg (2004) afirma que informações estruturadas têm seu campo de atuação limitado e fracassam quando a abordagem deve ser intangível, diferente das abordagens econômicas ou quantitativas, em relação a aspectos importantes, inerentes ao processo em questão. Davenport e Prusak (1998) chamam a atenção para o fato de que a informação não-estruturada gera os melhores resultados, mas não devemos, de forma nenhuma, desprezar as informações estruturadas, a melhor forma de lidar com este fato, é construir um sistema que possibilite a junção das informações estruturadas com as não-estruturadas no atendimento a solicitações ocasionais com direcionamentos imprecisos. Isso nos leva ao segundo passo da gestão da informação que trata da obtenção de informações.

Davenport e Prusak (1998) afirmam que, uma vez definida a exigência da informação, o próximo passo de sua gestão é o processo de obtenção de informações. Este processo deve ser ininterrupto. Para isso, se faz necessário um sistema de aquisição contínua de informações. Estes autores também afirmam que a distribuição está relacionada ao modo

como a informação é formatada. Muitos gerentes e executivos sabem que necessitam de informações que são imprescindíveis ao embasamento de suas decisões, mas não sabem onde se encontram tais informações de forma a resgata-las. As informações não se estabelecem em um único lugar, elas são fragmentadas, e cada um dos fragmentos pode ser encontrado em um setor diferente da empresa. Por isso a distribuição da informação se torna um processo mais complexo do que possa parecer, mesmo porque existe a eminente necessidade de identificação de quem precisa de qual informação para que o processo de distribuição se torne efetivo e eficaz. O fator tempo também é muito importante para este passo, pois existe em consenso que a informação correta deve chegar à pessoa certa, na hora exata de sua necessidade. Para isso, são utilizadas diversas soluções tecnológicas em termos de sistemas que são, de maneira geral, híbridos, ou seja, compostos de pessoas, documentos e computadores, para garantir a obtenção dos objetivos. Mas não adianta uma distribuição eficaz se não houver um uso efetivo da informação entregue.

Mesmo não havendo uma garantia de sucesso com o uso da gestão da informação, esta deve ser sempre bem estruturada, pois será a base para a construção do conhecimento organizacional. E este sim deve gerar resultados esperados, mas também depende um uma gestão eficaz (DAVENPORT; PRUSAK, 1998).

1.4.2.2 **Gestão do Conhecimento**

Segundo Sveiby (1998), o conceito de gestão do conhecimento nasceu no início da década de 90 e logo se expandiu para todo o mundo empresarial e territorial. O autor diz que é uma ferramenta administrativa para agregar valor a uma informação e/ou a um conhecimento. Ao filtrá-la, otimizá-la e direcioná-la, auxiliam profissionais a alcançarem os conhecimentos e informações de que eles necessitam para o desempenho satisfatório em ações que lhes competem. Stewart (1998) diz que, a gestão do conhecimento é a prática de agregar valor a uma informação e distribuí-la para que gere conhecimentos em outras pessoas. Mas os processos da gestão do conhecimento são mais complexos do que se parece. Existe um fator que é o principal dificultador do processo de gestão do conhecimento que é a natureza humana em que guarda para si, e a sete chaves, todo seu conhecimento; com medo de que outras pessoas possam possuí-los e superá-la. Essas pessoas que retêm os conhecimentos ameaçam a manutenção do nível de conhecimento que a empresa possui por elas serem a única fonte de armazenamento de tais conhecimentos, e como tal, se saírem da empresa, por qualquer motivo, levarão um patrimônio que a empresa pode ter investido para sua construção. Para isso, Vasconcelos (2000) relata que existe uma necessidade eminente, por parte da empresa, de construir uma habilidade que retenha os conhecimentos tácitos –

aqueles que se encontram nas pessoas – transformando-os em explícitos – aqueles documentados – de forma a garantir a posse de maior quantidade de conhecimentos produzidos pela organização. Para Choo (2006), enquanto o conhecimento permanecer em sua forma tácita, a empresa não possui condições para fazer com que seu uso seja de forma dinâmica e ampla, cumprindo assim seu papel mais nobre dentro da organização. Transformar este conhecimento tácito em explícito é a forma que a empresa tem para, pelo menos em partes, manter o seu capital intelectual, como é conceituada essa forma de patrimônio de conhecimento organizacional. Mas alguns autores visualizam as formas de gestão do conhecimento um pouco diferentes.

Davenport e Prusak (1998) salientam que a gestão do conhecimento necessita de ferramentas para provê-la, mas não se deve construí-la centralizada em tecnologias de informação. A gestão do conhecimento é muito mais do que estas tecnologias. Porém o uso de tecnologias da informação viabiliza uma eficácia no processo de gestão do conhecimento. Os autores discorrem que estas tecnologias não criam conhecimentos, o que é uma necessidade contínua das organizações, e nem tão pouco têm como lidar com conhecimentos tácitos, elas trabalham com conhecimentos que possam ser explicitados, codificados. Mas diante de todos estes fatos não se pode desprezá-las, pois o volume de conhecimentos que fazem parte do contexto de uma organização nos dias de hoje fazem com que a sua gestão seja difícil sem o uso de ferramentas tecnológicas que propiciem tal. O mais importante de todos estes fatos é frisar a importância da criação contínua do conhecimento organizacional. Segundo Choo (2006), há quatro maneiras de criar conhecimento organizacional se utilizando do manuseio de conhecimentos tácitos e explícitos, incitando um relacionamento entre eles. A primeira é através da socialização, em que é gerado conhecimento tácito no processo de experiências compartilhadas. Esta forma se dá através de uma observação participativa periférica, o ator que criará conhecimento participa do processo de maneira secundária e mantém sua atenção na observação do que está sendo executado pelo detentor do conhecimento, ou seja, o aprendiz observa o profissional experiente. Este aprendiz passa um tempo fazendo esta observação e quando se sente preparado ele sai do papel periférico e se torna o centro.

Choo (2006) afirma que a segunda maneira é a exteriorização, nessa forma acontece a transformação de conhecimento tácito em explícito pelo compartilhamento de metáforas, analogias, modelos ou histórias. Ela pode ser iniciada por um processo de reflexão coletiva em que aconteçam diálogos. Choo (2006) apresenta a combinação como sendo a terceira maneira de criação do conhecimento. O autor diz que “combinação é o processo em que

partes incompatíveis de conhecimento explícito existente se combinam e levam à produção de novo conhecimento explícito". (CHOO, 2006, p. 208).

A quarta maneira defendida por Choo (2006) é a internalização, que é o processo de aprendizagem e socialização mediante a repetição de uma tarefa, afim de que aquele conhecimento que está explícito no processo, ou até mesmo naquela máquina, seja absorvido e se torne um conhecimento tácito para aquele participante. Este processo tem ligação direta com o indivíduo que pode adquirir tal conhecimento através de experiência de realização de uma atividade, simulações, interpretações de papéis, ou ainda através de histórias que possam vir a ser fisicamente vivenciadas, transformando-se em experiência.

Para atender tais inquietações, De Sordi (2003) afirma que existe um conjunto de processos que governam os rumos do conhecimento organizacional, sendo que estes processos comporão a gestão do conhecimento. O autor afirma que a criação, disseminação e utilização do conhecimento proporcionarão a completa obtenção dos objetivos da organização, sendo que pode haver variação na quantidade e abrangência dos passos que compõem o processo informacional.

1.4.3 **Proteção da Informação e do Conhecimento**

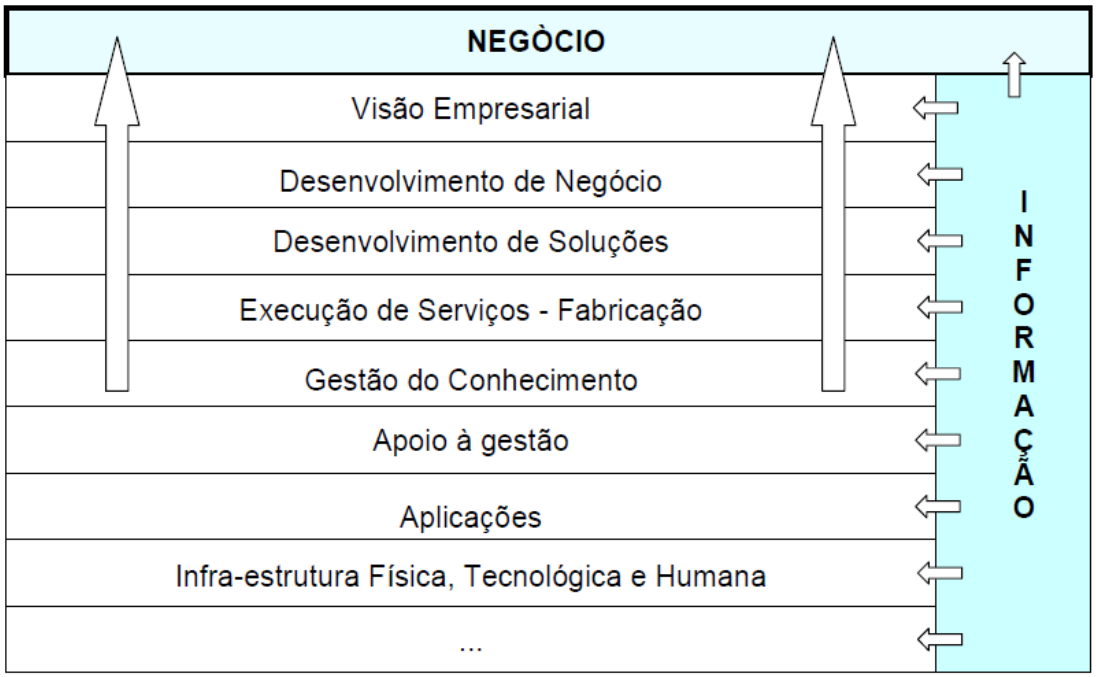
1.4.3.1 **Proteção**

Da etimologia desta palavra Houaiss (1981) afirma a palavra proteção vem do latim e pode-se entender como proteção a segurança do objeto em questão. O que mais interessa sobre proteção no contexto deste trabalho são as duas últimas colocações de que é aquilo que protege de um agente exterior e ainda sobre a garantia da sobrevivência. Estas definições ilustram de forma ampla o uso da proteção relacionada à informação e ao conhecimento.

1.4.3.2 **Proteção da informação**

Segundo Sêmola (2003), é inegável que todas as empresas, independentemente 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 poio à tomada de decisão. Cada vez mais as empresas se tornam dependentes da informação e por isso eleger sua proteção como fator importante. A FIG. 3 mostra um panorama da informação em relação aos processos de negócio (FIG. 3).

FIGURA 3 – Onipresença da Informação nos principais processos de negócio



FONTE: SÊMOLA, 2003, p. 2.

Sêmola (2003) afirma que há décadas atrás, as informações eram tratadas de forma centralizada e com pouca automação em seu fluxo pela organização. Mas hoje graças aos altos índices de conectividade e compartilhamento, existem diversas ferramentas tecnológicas que possuem a capacidade de lidar com a informação de forma automatizada; gerando possibilidade de manusear grandes bases de informações em frações de segundo. Com grandes possibilidades de exploração das informações vêm grandes problemas para garantir que tais processos aconteçam da forma em que foram planejados, sem a entrada de elementos que possam prejudicar o processo ou fazer com que ele gere resultados fora do esperado. Por isso devem se considerar os riscos que envolvem este novo processo. Quanto maior o volume do tráfego de informações no processo, maior o nível de dependência que a empresa terá em relação ao mesmo e, por conseguinte às informações. Quanto maior for a dependência da organização em relação a este processo, maior será o risco ao qual ela estará submetida. Também no mesmo aspecto maior será o número de pontos que terão acessos às informações, que podem assim se concretizar como ponto de vazamento da informação, o que, novamente, direciona a necessidade de uma análise de risco para direcionar ações de proteção à Informação.

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. O autor também coloca que esta segurança pode ser considerada como a prática da gestão de

riscos de incidentes que acarretam no comprometimento da confidencialidade, integridade e disponibilidade, que são os pilares da segurança da informação. A confidencialidade é uma ligação com o grau de sigilo que a informação deve conter visando a limitação de seu acesso e seu uso ser apenas por pessoas que possuem esse direito. A integridade é relacionada com a confiança que se tem na informação, fazendo com que os processos que promovem sua modificação sejam legítimos e que não haja alterações indevidas, sejam intencionais ou acidentais. Já a disponibilidade é um complemento, mas com mesma importância das abordagens anteriores, de que a informação gerada ou adquirida deve estar disponível para seus usuários no instante em que eles necessitem, para qualquer finalidade. A garantia da solidez dos pilares descritos anteriormente deve ser construída através de uma análise de risco que envolve variáveis que incidirão sobre a informação.

1.4.3.2.1 *A análise do risco em proteção da informação*

Segundo Sêmola (2003), a análise do risco deve ser feita atentando para o estudo e compreensão de algumas variáveis que o compõe. Estas variáveis são:

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, consequentemente, causando impactos aos negócios de uma empresa. São ameaças os desastres naturais, falta de treinamento sobre a correta forma de manuseio da informação por parte de seus usuários, ações intencionais para acesso não autorizado de invasores, espiões, ladrões, criadores e disseminadores de vírus eletrônico, incendiários, entre outros.

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. Existem vulnerabilidades físicas – instalações prediais fora do padrão, falta de controle de acesso pessoal às salas onde se encontra o armazenamento das informações, falta de equipamentos de combate à incêndio, entre outros; naturais – proximidade de rios ou encostas instáveis, alta umidade, altas e baixas temperaturas; comunicação – falta de identificação de atores no processo de construção da informação e seu manuseio; e humanas – ausência de treinamento, compartilhamento de informações confidenciais, não execução de rotinas de segurança, sabotagens, vandalismos, roubo, invasões ou guerras.

Impactos – traz a abrangência das consequências causadas por um incidente de segurança sobre processos de negócio.

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. Essas medidas têm a obrigação de mitigarem o risco inerente ao bem estar dos ativos informacionais. Estas medidas têm caráter preventivo, detectáveis e corretivas. 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. Sendo que este comitê tem o objetivo de representar os interesses da empresa diante os desafios que a sociedade da informação e do conhecimento impõe ao negócio. Este comitê tem a responsabilidade de criar processos e procedimentos que vão mitigar o risco em relação aos ativos informacionais. É parte desse procedimento buscar formas para que as ameaças não explorem as vulnerabilidades, podendo assim, causar impactos na organização. Para isso as ameaças devem ser cada vez mais conhecidas, para que haja um controle sobre as mesmas; e as vulnerabilidades sejam cada vez menores, reduzindo o número de portas de entrada para as ameaças. Dentro de tal artifício, outro fator a ser considerado pelo comitê de segurança da informação é o impacto, causado pela exploração de uma vulnerabilidade por uma ameaça, que poderão tomar aspectos positivos ou negativos diante a quebra de segurança, dependendo do ativo informacional que estiver envolvido no incidente. O autor afirma ainda que cada empresa terá, de forma única, o seu processo de análise de riscos e de proteção da informação e conhecimento. Este é outro aspecto que tem características muito semelhantes à informação, mas que merece uma atenção especial na atual sociedade da informação e do conhecimento. Tais fatores se veem aguçados diante da atual forma de trabalho das organizações: em rede. No presente o sistema produtivo, através de procedimentos que são complementares, cria-se uma cadeia onde uma empresa participa do processo de produção da outra, formando assim uma rede.

1.4.3.3 **Proteção do Conhecimento**

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 fazer o vazamento destes conhecimentos de forma anônima é muito menor do que dois anos atrás, mas ainda é maior do que se fazia na década de 70. Esta 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.

Estes novos processos constroem um contexto em que as empresas se veem no processo de qualificação através de uma forma conjunta a outras empresas. Isso propõe uma cooperação entre estas, para a criação de novos conhecimentos. Porém elas podem ser concorrentes em determinados momentos. Este mecanismo de competição e cooperação é contrário, em grande medida a lógica da dinâmica capitalista, pois o sucesso de uma organização é medido através de resultados obtidos diante um planejamento construído sob conhecimentos estratégicos. Em certos contextos, a cooperação pode ser uma condição para a sobrevivência da organização, mas esta sobrevivência também é baseada em diferenciais competitivos que são construídos através de informações e conhecimentos estratégicos. Isso torna clara a percepção da necessidade de se proteger o conhecimento estratégico nas organizações participantes desta sociedade em rede. (TEIXEIRA, 2005).

Ainda neste contexto outro fato a ser ponderado é sobre a forma de compartilhamento dos conhecimentos no trabalho em rede das empresas, pois, um conhecimento estratégico compartilhado quando não deveria, ou partilhado com o parceiro errado, pode fazer com que o diferencial competitivo da empresa seja reduzido. Por outro lado, a empresa deve ficar atenta à externalização de conhecimentos e informações proporcionada pelo relacionamento entre as empresas no desempenho de suas funções nesta cadeia de produção. Isso pode proporcionar a absorção de todo o conhecimento disponibilizado. Essa dinâmica traz grandes desafios para as organizações modernas, pois, cria a necessidade de bom entendimento do processo para utilizar da melhor forma todo, ou parcialmente, o conhecimento disponibilizado por suas parceiras; mas para isso a empresa deve ter um alto grau de entendimento do contexto da rede a qual ela está inserida. (VASCONCELOS, 2007).

Segundo Vasconcelos (2007), as empresas têm agregado valor aos seus produtos através de relacionamentos em rede, em que existe a necessidade de compartilhamento de conhecimentos. De forma isolada, as organizações ficariam alheias à maioria das tecnologias e dos conhecimentos estratégicos, gerando uma dificuldade na manutenção desta empresa em seu mercado. Para ilustrar o exposto pode-se citar uma empresa que fabrica tubos de aço para construção de oleodutos, em que os tubos não possuem costuras, ou seja, não existem emendas e têm que resistir a uma determinada pressão. Esta empresa

depende de seu fornecedor que faz a extração do minério de qualidade para sua fusão, transformando-o em sua forma líquida dentro das especificações técnicas pré-estabelecidas. Depois a dependência fica por conta de um prestador de serviços de transporte desta matéria prima, que deve conservar algumas características para não comprometer sua qualidade, como por exemplo, a alta temperatura para manter o minério em forma líquida até chegar à empresa que iniciará o processo de produção dos tubos. Terminada a produção surge a necessidade de um novo transporte, que dessa vez tem particularidades diferentes, como por exemplo, a ausência de qualquer tipo de colisão do tubo e empilhamento máximo de três tubos, em que entrará outro prestador de serviço que possua tal expertise. Então o produto será entregue ao cliente solicitante do mesmo. Todo este processo gera informações importantes que devem ser acompanhadas tanto pelo fabricante do tubo, quanto pelo cliente que o usará na construção de seu oleoduto. Qualquer alteração no processo poderá comprometer a segurança de operação do oleoduto quando montado. Para isso deve haver uma troca constante de informações entre as empresas participantes do processo, sendo que cada uma terá papéis que se alternarão. Esta alternância se dá na medida em que uma empresa se torna emissora da informação – passando uma norma técnica, por exemplo – e a parceira receba-a, adquirindo conhecimento; e esta receptora, para que haja a correta produção, adequa seu processo produtivo para atender à norma técnica, acontecendo assim o aprendizado. A todo o momento existe a cooperação entre os membros. A esse processo denomina-se rede de empresas (LUNDVALL, 1992; MCGEE; PRUSAK, 1994; CHOO, 2006; JAMIL, 2006).

Segundo Kale *et al*. (2000), a maior motivação para a construção de uma rede de empresas é pela possibilidade de acesso ou aquisição de informações críticas, Know-How ou capacitações vindas dos parceiros. Com o novo ambiente de negócios exigindo novos tipos de relacionamentos, é reduzida a forma conservadora do relacionamento interempresarial. Algumas alianças em rede tradicionais transformaram-se em parcerias competitivas, ou seja, as empresas trocam experiências para resolução de problemas e/ou construção de novos processos, mas podem ser concorrentes em outro contexto. Tal fato gera uma resposta mais eficaz às ameaças e às oportunidades ambientais.

Neste ambiente em rede, que tem como principal requisito o compartilhamento de conhecimentos, as empresas que fazem parte da rede podem ser tanto parceiras quanto concorrentes, dependendo da situação. Neste contexto a informação e o conhecimento, que são fatores cruciais para a competitividade da empresa, são compartilhados, explorados e aplicados para que toda a rede alcance seus objetivos. Esta estrutura suscita uma

necessidade eminente de criar políticas para a proteção do conhecimento organizacional. (VASCONCELOS, 2007).

Seguindo a mesma linha de raciocínio, Beal (2008) coloca o conhecimento como sendo um dos ativos organizacionais, e, portanto, deve-se criar uma classificação para a proteção do mesmo. Esta classificação direcionará ações e até mesmo orçamento para a construção de sua proteção. Deve-se fazer uma análise de risco quanto a cada um dos conhecimentos que devem ser trabalhados pela organização para direcionar as ações de proteção de cada um deles. Para isso há uma avaliação seguindo alguns aspectos como, por exemplo, a gravidade do impacto – catastrófica, alta, média e baixa – causado por danos ou perda de determinado conhecimento e a probabilidade de que ocorra algum incidente com aquele conhecimento. Esta avaliação é explicitada no (QUADRO 1):

QUADRO 1
Matriz de Risco

QUADRO 1 – Matriz de risco.

Gravidade do impacto	Probabilidade de ocorrência do incidente					
	F Impossível	E Improvável	D Remota	C Ocasional	B Provável	A Freqüente
I Catástrofe			/////////	XXXXXX	XXXXXX	XXXXXX
II Alta				/////////	XXXXXX	XXXXXX
III Média					/////////	/////////
IV Baixa						

FONTE: BEAL, 2008, p.23.

NOTA: XXXXXX: Imperativo reduzir os riscos.
/////////: Medidas de proteção adicionais requeridas.
Em branco: As medidas básicas de proteção adotadas pela organização são consideradas suficientes para manter os riscos em níveis aceitáveis.

Beal (2008) através desta matriz de risco mostra que quanto mais frequente for a ocorrência do incidente e maior os impactos, devem ser tomadas medidas não só de segurança propriamente ditas, mas também deve haver um trabalho de redução dos riscos envolvidos. Em contrapartida, quanto mais baixo for o nível de impacto e menos frequente a possibilidade de ocorrência do incidente, menores são as medidas de segurança a serem construídas.

Stewart (2002) salienta que o risco não é algo negativo, pelo contrário, ele é positivo, primeiro por deixar os gestores sempre atentos às agitações ambientais em relação ao negócio da organização, e depois por ter uma ligação direta com recompensas em processos. Desta forma o risco tem que ser gerenciado e não eliminado, ou seja, escolher em que processo de conhecimento apostar e proteger as apostas; sem esquecer que em alguns pontos não se deve apostar de forma nenhuma. Esta proteção deve ser bem construída seguindo a orientação de custo X benefício, sempre com o foco nos conhecimentos que são de maior importância estratégica para a empresa, mas sem deixar de avaliar todos os outros conhecimentos.

Diante dos fatos relatados, Beal (2008) descreve como estratégia para a proteção do conhecimento, além de sua classificação, o uso de processos referentes a boas práticas que podem ser utilizados; como por exemplo, ITIL (It infrastructure library) – que é um conjunto de documentos para registrar as melhores práticas na área de gestão de serviços da tecnologia da informação, elaborado pelo governo do Reino Unido; COBIT (Control objectives for information and related technology) – conjunto de diretrizes para a gestão e auditoria de processos, práticas e controles de tecnologia da informação; e as normas ISO/IEC 17799[1] e ISO 27000 (International Organization for Standardization – ISO – rede que reúne entidades padronizadoras de 148 países, com escritório central em Genebra na Suíça e entidades associadas em todos os países) – que tratam da gestão da segurança da informação e corresponde a um código de práticas para esta gestão.

Em especial a ISO 17799 possui algumas áreas de controle que são mais utilizadas para a construção dos processos de proteção da informação e do conhecimento:

- Políticas de segurança – recomendações para a formalização de diretrizes, princípios e regras que orientarão e apoiarão a implantação e manutenção da proteção;

- Classificação e controle dos ativos – recomendações sobre a realização de inventário dos ativos informacionais e atribuições de responsabilidades;

- Segurança em pessoas – que são recomendações para mitigar os riscos de erros humanos, fraudes e retenção de conhecimentos para si;
- Gestão das operações e comunicações – visa garantir a operação correta e segura dos recursos de processamento de informações e conhecimentos, bem como garante integridade;

- Controle de acesso – que são recomendações para o controle e monitoração de acesso às informações e conhecimentos.

Beal (2008) afirma que existem outras áreas, mas as especificadas ficam diretamente relacionadas com o conhecimento. Tais normas e boas práticas nasceram do relacionamento com a informação, mas são estendidas facilmente ao conhecimento devido às características do mesmo.

Beal (2008) salienta ainda a necessidade do relacionamento da lei brasileira dos direitos autorais (Lei 9.610 de 19 de fevereiro de 1998) como uma ferramenta poderosa para a construção e manutenção da proteção do conhecimento, juntamente com a lei das patentes (Lei 9.279 de 14 de maio de 1996). Todas estas normas e leis servem de base para a criação de processos de proteção do conhecimento, mas para uma organização, segundo a autora, não adianta construir as melhores e mais modernas medidas de segurança se não houver uma responsabilidade "compartilhada por todos os integrantes da organização, exigindo, para a eficácia das medidas de proteção, o estabelecimento de uma estrutura organizacional capaz de planejar e implementar a segurança desejada". (BEAL, 2008, p.51).

Ainda segundo Beal (2008), é comum as empresas atribuírem as atividades de construção da proteção do conhecimento e das informações aos setores de Tecnologia da Informação. Geralmente os orçamentos que se referem aos investimentos em segurança da informação e conhecimento são módulos do orçamento do setor de Tecnologia da Informação, isso reflete em ações tomadas apenas pela equipe deste setor; o que coloca em risco a qualidade da proteção alcançada por estas ações, devido à construção, através de ferramentas tecnológicas, de barreiras de proteção que ficam apenas no âmbito mecânico sem considerar aspectos físicos, humanos e de gestão de processos. Para serem alcançados os objetivos de proteção, deve haver uma conscientização de presidentes, diretores, gerentes, líderes e demais colaboradores em relação à importância do sigilo quanto alguns processos organizacionais, e no que isso implica para a organização e para cada colaborador. Muitas empresas investem uma grande parte de seu orçamento, relacionado à segurança, na construção de cartilhas explicativas sobre as melhores práticas para a proteção do conhecimento organizacional e de suas informações, além de informar sobre os possíveis danos causados pelo vazamento dos mesmos e suas consequências.

Stewart (2002) afirma que a proteção do conhecimento não deve ser embasada em um único processo, como por exemplo, o da retenção do conhecimento através da explicitação do tácito em sistemas computacionais e posterior criação de barreiras de segurança para a

garantia dos mesmos. Não é suficiente criar reservatório ou estoque de conhecimentos e ferramentas de proteção dos mesmos para que se garanta a proteção. As organizações devem trabalhar com uma análise ampla das variáveis envolvidas, com ênfase na redução das ameaças e das vulnerabilidades referentes ao processo de gestão do conhecimento, tornando conhecidas as rotas de vazamento do conhecimento e da informação para que haja um correto direcionamento das ações de proteção dos mesmos.

1.4.4 **Vazamento da informação e conhecimento**

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

As organizações devem, cada vez mais, aprimorarem seus processos de proteção da informação e do conhecimento diante da amplitude e complexidade de seus papeis dentro da empresa. O desafio da construção da segurança se faz em camadas ou fases, onde particiona-se todas as variáveis envolvidas e o trabalho a ser realizado em áreas, para tornar mais claro o entendimento de cada uma das partes. Usando essa tecnologia, fase ou camada que deve ter uma ênfase maior é a descoberta do vazamento de informações e conhecimentos, abordando suas rotas, envolvidos e suas consequências, 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 incontroláveis pela organização que fazem parte dos principais processos em seu dia-a-dia, como por exemplo, pessoas, parceiros e o próprio ambiente. (STEWART, 2002).

Ainda não há muitos estudos sobre o tema vazamento de conhecimentos (knowledge leakage); outros termos são utilizados com mesma significância, como por exemplo, fuga de conhecimento (knowledge loss), exposição do conhecimento (knowledge disclosure) e escoamento de conhecimento (knowledge seepage). 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; em que 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).
O vazamento do conhecimento acontece nas fases de sua criação e gerenciamento, e ainda tem relação direta com a fase de absorção e transferência, além da interação das organizações com seus ambientes de trabalho. A autora lembra também que as consequências deste vazamento podem ser negativas, mas ao contrário do que a maioria dos profissionais da informação e do conhecimento acham, elas também podem ser positivas. (VASCONCELOS, 2007).

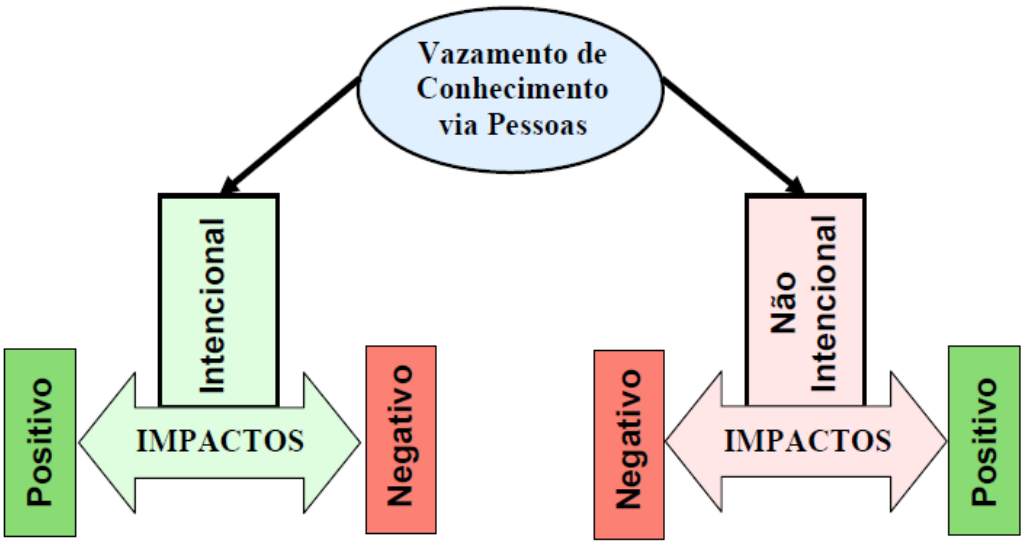
Kaplinsky *et al* (2006, citado por VASCONCELOS, 2007) salientam que o vazamento de conhecimento deve ser avaliado segundo um relacionamento ponderado entre perdas e ganhos no contato de ações estratégicas em desenvolvimento de empresas em rede. Segundo os autores deve-se fazer uma apreciação em que são levadas em consideração várias áreas de estudo como a Gestão do Conhecimento e da Inovação, recursos humanos, análise e planejamento estratégico, cadeia de suprimentos, análise e gestão do isco, análise de produtividade, confiança, cadeias de valor, pesquisa e desenvolvimento, competências essenciais, entre outras, para que haja uma boa análise do vazamento do conhecimento. Os autores falam que a bibliografia disponível é falha quanto à abordagem e consequências positivas em algumas situações de vazamento de conhecimento. Outras visões falhas, segundo os autores, é o fato de não haver discussão sobre o grau de intencionalidade do vazamento do conhecimento, além das técnicas para construção de má política e estratégia de proteção do conhecimento organizacional.

1.4.4.1 **Vetores do vazamento de conhecimento**

Kaplinsky et al (2006, citado por VASCONCELOS, 2007) dizem que existem seis pontos chaves que são vetores de vazamento do conhecimento, a saber: fornecedores, clientes, concorrentes, os colaboradores, o relacionamento da empresa com o sistema de inovação e as 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.

Com base nos processos anteriormente tratados, Mohamed et al (2006) propõem um modelo que orientará a análise do vazamento de conhecimento através do fluxo de pessoas na organização. O modelo é muito simples e serve de base para uma análise de forma estruturada do vazamento de conhecimento, e posterior construção de estratégias que promovam a proteção dos conhecimentos envolvidos, conforme exposto na (FIG. 4).

FIGURA 4 – Taxonomia do vazamento de conhecimento através das pessoas



FONTE: MOHAMED *et al.*, 2006, p. 5.

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 empresas 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.

Mohamed *et al* (2006) desenvolveram uma pesquisa para se desvendar as possíveis rotas de vazamento do conhecimento com o foco nas pessoas das empresas. Para nortear a análise dos dados foi utilizada a taxonomia de vazamento de conhecimento, que trata o vazamento como intencional e não intencional com impactos positivos e negativos.

Toda a análise do vazamento de conhecimento com seus vetores, bem como o processo de gestão do conhecimento devem servir de base para a correta utilização de técnicas que possam sempre trazer benefícios para a organização que os constroem. Para isso é necessário um relacionamento entre a proteção da informação e do conhecimento, uma vez que um dos processos importantes para que haja bons resultados, obtidos pelo uso de conhecimentos e informações, é a proteção do conhecimento e também das informações organizacionais. (MOHAMED *et al*, 2006).

1.4.5 **Correlação entre a proteção da informação e do conhecimento**

Segundo Beal (2008), as ações pertinentes ao processo de proteção do conhecimento se aplicam à proteção da informação, devido a características em comum que os objetos possuem. A autora coloca uma forma de aplicação da proteção da informação que também é voltada ao conhecimento.

1.4.5.1 **Nível de maturidade da proteção da informação e do conhecimento organizacionais**

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

- No nível inicial, que é o Nível 1, os problemas são tratados de forma isolada e dependem de iniciativas individuais dos envolvidos. 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;

- No Nível 2 que é reativo, já existe uma política de segurança corporativa e desenvolve 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;

- 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 acontecimentos 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;

- Já o 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 desenvolvimento de conhecimentos leva em consideração os princípios para sua proteção. Existe todo um trabalho de análise e gestão do risco no contexto ao qual a organização está inserida. Este nível propõe uma monitoração constante das agitações do ambiente para haver uma reação imediata à problemas de proteção relacionadas a mudanças organizacionais, estratégicas ou tecnológicas, além de promover os ajustes necessários.

Beal (2008) lembra 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 a proteção do conhecimento e das informações, um formato que se encaixará em um dos níveis propostos.

Sêmola (2003) lembra que independente do nível em que a organização se enquadra, ou dos processos que são construídos, o importante é manter boas práticas, procedimentos e mecanismos eficazes na proteção do conhecimento e da informação, para impedir ameaças de explorarem as vulnerabilidades, e ainda reduzam as vulnerabilidades, para controlar os impactos relacionados à organização. O autor lembra ainda que é difícil separar processos que são exclusivos para a proteção da informação e outros que são exclusivos ao conhecimento. Dessa forma as ações são conjuntas e complementares em todos os tipos de empresas, independentemente de seus ramos de atividades ou forma jurídica. Deve haver sempre a preocupação com as melhores práticas.

2 **DESENVOLVIMENTO**

Em um mercado extremamente competitivo, o setor bancário possui uma gama de clientes bem extensa, buscando cada vez mais clientes e a fidelização dos já existentes, o setor que encabeça a lista dos que mais incentivam a utilização de créditos rotativos das mais diversas formas, também é o que mais consome tecnologia para proteção das informações, seja essa ligada diretamente ao negócio, ou a proteção das informações de seus clientes.

2.1 **Contextualização – Interna e Externa**

A empresa base deste estudo atua no setor de impressos de segurança, é uma organização de médio porte com mais de 60 anos atuando no mercado gráfico com a produção de formulários de segurança, documentos pré-impressos, formulários para impressora a laser, cheque em formulário contínuo, talões personalizados e magnetizados eletronicamente, cartões de plástico com tarja e cartões com chip.

Com escritório na Região Metropolitana de Belo Horizonte/MG e representantes autônomos em todo país, a empresa oferece como principal produto cartões em PVC com tarja e chip atendendo as principais bandeiras nacionais, como Cabal e Elo, e internacionais, como Visa e Mastercard.

A Empresa começa atuando no setor gráfico em 1947, com a editoração e impressão de livros, e cadernos de informação. Em 1950 passa a trabalhar em sede própria e atuar no mercado de impressão de talões de cheque, o qual tem predominado até os tempos de hoje, porém com um volume muito inferior. Em 1997 a empresa passa a atuar em outro seguimento do mercado de pagamentos bancários, iniciando a produção de cartões de crédito. Hoje a organização conta com 486 funcionários, distribuídos nas mais diversas áreas de atuação.

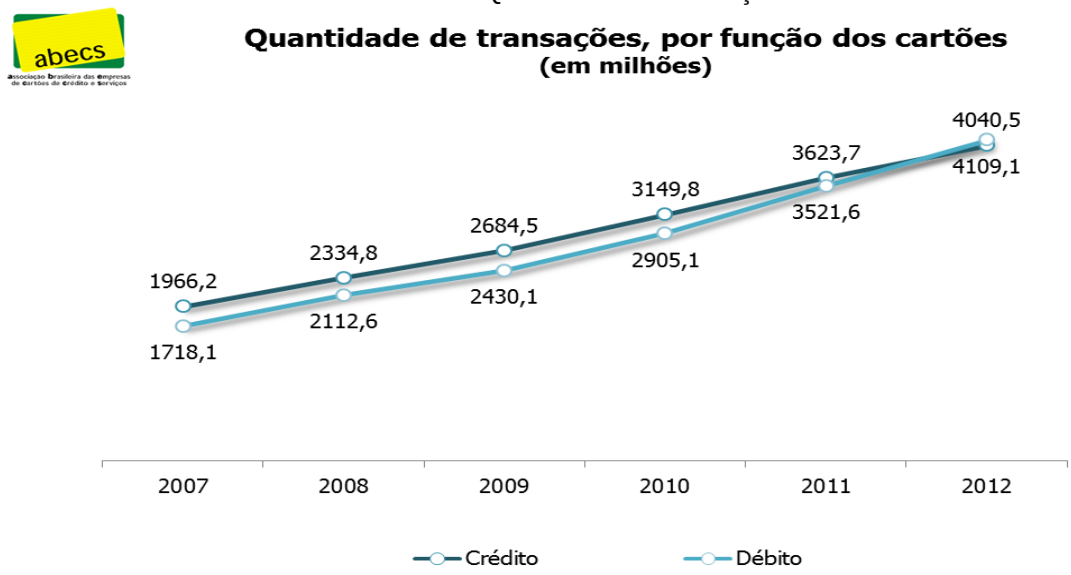
2.1.2 **O mercado de cartões**

Nos últimos dez anos, uma forte expansão do mercado brasileiro de cartões de pagamento, que segundo pesquisas da ABECS (Associação Brasileira das Empresas de Cartões de e Serviços), cresceu uma taxa média de 23% ao ano entre 2002 e 2011. A evolução refere-se ao faturamento das transações feitas com cartões de crédito, cartões de débito e cartões de rede e loja. Apenas em 2011, esse crescimento foi de 24%, o que permitiu ao setor registrar um total de R$ 670 bilhões de faturamento no ano passado.

A quantidade de transações feitas com cartões de pagamento evoluiu de forma semelhante, com uma média de crescimento de 20% ao ano no mesmo período – em 2011, foram realizadas 8,3 bilhões de transações. O volume de cartões em circulação no país também cresceu notoriamente nos últimos dez anos: de 183 milhões, em 2002, para 687 milhões, em 2011 – o que em média, representa pouco mais de 3,5 unidades por brasileiro. Hoje, 72% da população têm algum tipo de cartão de pagamento na carteira, e o hábito de uso não está muito distante disso: gira em torno de 69% da população.

Os dados mostram que o brasileiro tem optado cada vez mais pelo uso dos cartões em seus dispêndios diários e, aos poucos tem deixado de lado outros meios de pagamento mais antigos, como o dinheiro em espécie e o cheque. O uso deste último, por exemplo segue uma rota inversa à dos cartões, caindo em média 8,2% ao ano na última década. Além da óbvia questão da praticidade, a substituição desse meio de pagamento encontra impulso na garantia de recebimento (FIG. 5).

FIGURA 5 – Quantidade de transações



FONTE: ABECS, 2010.

A substituição de meios de pagamento ocorre de maneira natural, já que os benefícios são incontestáveis. Segurança, prazo para pagamento, parcelamento sem juros, acesso a crédito, programas de milhagem, agilidade e conveniência são algumas das vantagens de imediata percepção.

Não só o consumidor tem notado e utilizado os benefícios dos cartões, mas o varejo tem percebido cada vez mais um grande aumento no número de vendas relacionado aos cartões e seus benefícios. Junto a essa fatia os fornecedores de cartões e meios de pagamento eletrônicos, com um mercado em plena ascensão como mostra os números da Abecs aproveitam para se manter cada vez mais nesse mercado rentável, exigente, com difícil atuação, porém e os números não mentem, bastante lucrativo.

2.2 **Desenvolvimento (produção de conhecimento)**

Com a alta utilização dos cartões como meio de pagamento, o setor bancário tem a previsão de permanecer crescente no mercado, as economias em desenvolvimento vão puxar as taxas de crescimento da indústria de meios de pagamentos na próxima década, como mostra MOREIRA, J (2015). Em 2014, o setor faturou US$ 1,09 trilhões - 54% nas nações desenvolvidas e 46 % nas em desenvolvimento.

Privacidade e segurança são as maiores preocupações dos usuários desses serviços, assim o setor bancário busca cada vez mais soluções para a proteção de dados e dos conhecimentos produzidos por eles dentro das organizações. Com esta visão a empresa

aqui apresentada como base de estudo realiza a personalização dos cartões e mantem uma área de estudo para a constante evolução da segurança dos dados, tendo assim a dupla necessidade de proteção da informação e conhecimento gerados por ele e demandada pelos contratantes.

O principal foco do produto que garante a segurança de todos os dados são as técnicas de gravação, realizadas de forma complexa e segura nos chips de dados, sendo eles de contato ou por proximidade. Para que todo o processo atenda as altas exigência do mercado cada fabricante desenvolve suas tecnologias sempre seguindo os manuais de personalização EMV Europa Master e Visa, mas com características especificas para cada fabricante, desenvolvidas e guardadas como parte principal do negócio, esta tecnologia é contratada pelos parceiros e os mais diversos emissores de cartões para meios de pagamento.
Parte desta tecnologia garante que os dados dos clientes e utilizadores dos cartões como meio de pagamento seja gravada de forma extremamente segura e que de forma alguma seja possível realizar copias dos dados já personalizados. Com este entendimento a organização busca a proteção da informação e dos conhecimentos contratados e produzidos por ela.

2.2.1 **Personalização eletrônica de cartões**

A personalização dos cartões com chip consiste em gravar de forma segura os dados necessários para a realização das transações com chip, para este processo a empresa, desenvolve e utiliza, alguns níveis de segurança, o mais relevante e de grande importância para o negócio, é a utilização das chaves para a gravação e preparação dos dados.

A preparação dos dados é parte fundamental para o desenvolvimento do negócio, que consiste em gerar os dados que serão gravados no chip, utiliza recurso de informação e conhecimento produzido pela empresa especificamente para esta finalidade, alimentado com as informações dos clientes, fornecidas pelos parceiros contratantes. Após este processo as informações geradas são gravadas e protegidas com as chaves de personalização.

A utilização das chaves para a preparação de dados e personalização dos cartões, assim como o seu armazenamento são tecnologias desenvolvidas e protegidas. As chaves utilizam sistemas complexos para realizar a proteção dos dados que serão gravados nos chips dos cartões. As chaves são partes lógicas aleatórias, que combinadas formam uma chave

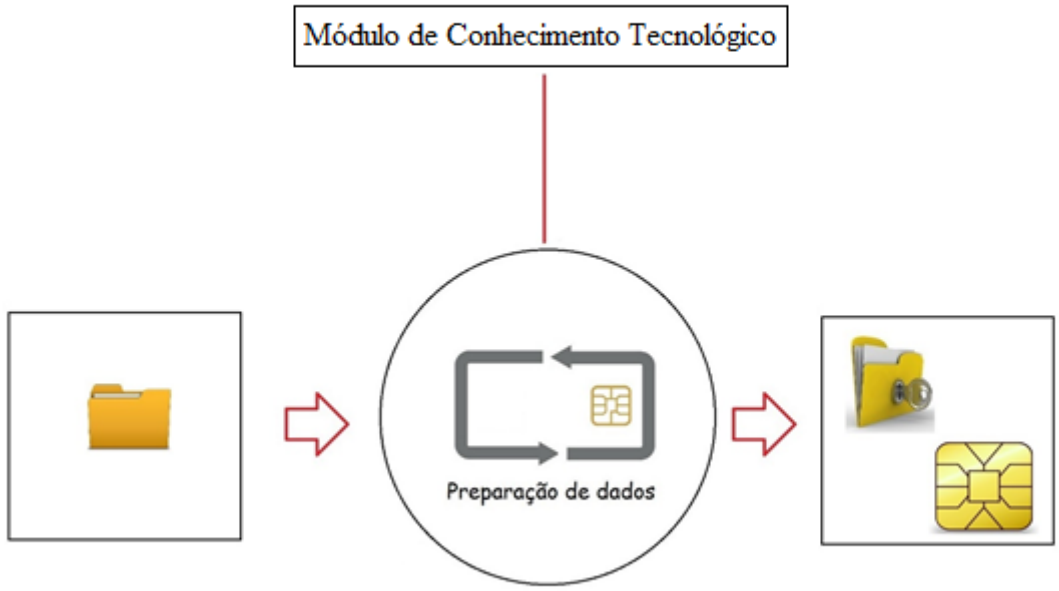
mestra, que guarda os dados sensíveis dentro do chip dos cartões, através de sistemas complexos desenvolvidos pela empresa. As informações utilizadas para a elaboração dos sistemas assim como todo o conhecimento gerado para esta finalidade, devem ser protegidos.

2.2.2 **Produto do conhecimento**

O produto final decorrente do conhecimento aplicado, é chamado pela empresa de Data Preparation, produto este que é oferecido e comercializado em diversas formas aos seus parceiros e clientes, sempre levando em consideração entregar o produto adequado às necessidades do contratante, com um nível alto de segurança para o produto informacional e sua tecnologia agregada.

A cada entrega de produto, há um foco secundário, a proteção da tecnologia desenvolvida sem influenciar no produto final. O resultado é um módulo de conhecimento tecnológico que realizará o processamento das informações internamente, apresentando como resultado de saída as informações necessárias para a personalização dos chips de cartões para meios de pagamento, sempre adequando as necessidades do contratante (FIG. 6).

FIGURA 6 – Fluxo de utilização tecnologia de preparação de dados



FONTE: Empresa base do estudo, 2015.

2.3 **Relevância do Armazenamento Seguro das Informações**

Em vista que parte do negócio está diretamente ligado ao conhecimento produzido tendo diretamente como consequência a tecnologia de gravação, este deve ser armazenado de forma segura, assim a empresa busca melhorias e constante inovações para atender a este quesito.

Para que se entenda melhor as dimensões das informações produzidas e manipuladas durante o processo, a junção de todo o conhecimento através de uma única pessoa pode caracterizar um vazamento informacional, onde seria possível reproduzir uma cópia do ambiente em local externo para a aprovação de transações ou produção de cartões para meios de pagamento indevidamente.
Fato este que obriga cada vez mais a incansável busca da proteção do conhecimento, tendo como verdade para este que, mesmo que a tecnologia seja copiada ou reproduzida de forma falha e grotesca, as informações e conhecimento produzidos pela empresa não sofram violações ou sejam acessadas. Sempre garantindo que todas as informações sejam integras.

2.3.1 **Principais meios de vazamento informacional**

Como em qualquer processo de geração de conhecimento que o resultado seja a tecnologia, estamos sujeitos a um vazamento informacional, tanto de peculiaridades desenvolvidas para o negócio quanto vazamento de informações sensíveis de clientes e parceiros, conjunto de informações este que é de grande importância para o desenvolvimento do negócio. Dentro da demanda, conseguimos observar alguns pontos de vazamento informacional, pontos estes que são constantemente monitorados e rigorosamente corrigidos quando necessário, mas necessitam de melhorias.

A disseminação errada da informação, conhecimento ou tecnologia, divulgação das informações trabalhadas ou em desenvolvimento que são classificadas como estritamente confidencial a terceiros ou partes que não estão envolvidas no processo.

Falhas humanas e comprometimento de informações. A divulgação ou exposição de dados e informações pertinentes ao processo de geração da tecnologia, bem como senhas e usuários de acesso de forma proposital ou involuntária.

Falhas nos processos decorrentes da utilização errada ou não utilização dos procedimentos internos, manuais de referência e recomendações das auditorias.

Comprometimento de partes físicas, logicas e pessoas envolvidas diretamente nos processos. Falhas de equipamentos físicos que operem sem um plano de contingência adequado e revisado por pessoas responsáveis e indicadas para esta função. Além de tentativas com sucesso de corromper pessoas que armazenem parte do processo tecnológico, gerados através das informações e conhecimento produzidos, a fim de replicar ou copiar este ambiente.

Vazamento de tecnologia, por terceiros envolvidos diretamente no processo. Mesmo quando houver partes indiretamente ligadas a organização (empresa) envolvidas no processo de geração de conhecimento, estas nunca devem estar sem acompanhamento ou com posse de informações pertinentes ao produto final fora do ambiente da organização ou sem autorização com nível de classificação adequada.

2.3.2 **Proteção do conhecimento**

Seguindo as recomendações do PCI - Payment Card Industry e orientações da bandeira Mastercard e VISA e consultando a convenção EMV – Europe Master e VISA, são desenvolvidos os procedimentos de segurança para a proteção do conhecimento da organização.

Todos os dados e informações que transitam para a preparação e personalização dos dados eletronicamente nos cartões para meios de pagamento, tem como obrigatoriedade, estar protegida de falhas ou vazamento. Qualquer ameaça de comprometimento das informações empregadas no processo, deverá ser identificada imediatamente é o processo será interrompido e qualificado como comprometido. Para cada área do processo, que são definidas como preparação e personalização, são definidas pessoas chaves, que são responsáveis por informar e serem informados de qualquer falha.

Em nenhum momento poderá haver pessoas que atuem em todas as fases do processo, por questões de segurança. Todo o conhecimento de uma área não deverá ser divulgado a outra sem a necessidade correlata. Garantido assim que mesmo tendo conhecimento de todo o processo, somente uma pessoa não seja capaz de reproduzi-lo.

Todo o conhecimento desenvolvido estará armazenado sobre duplo controle, mesmo quando aplicado, ou em produção, este é executado com a dependência de duas ou mais pessoas. Garantindo um nível a mais de segurança, tendo em vista que duas ou mais pessoas não seriam corrompidas facilmente.

2.3.2.1 **Segurança nas fases do processo**

Durante todo o processo de desenvolvimento do conhecimento e informação, até o produto final de tecnologia, nenhum dado ou informação são divulgados ou disseminados sem estar com um nível de segurança adequado, sendo proteção física para equipamentos ou criptografias seguindo as recomendações dos manuais de referência para arquivos de texto ou configurações.

Todo o processo deve estar protegido, com níveis de acesso restritos e especificados claramente neste em texto claro. Todo o acesso deverá ser previamente justificado e monitorado.

2.3.2.2 **Visão geral e auditoria**

Uma vez aplicada, todas as proteções correlatas as fases do processo, seja em desenvolvimento, produção, teste ou esboço, caberá ainda auditorias com prazos a definir, para garantir que todo o procedimento está sendo cumprido, e que as falhas sejam reduzidas, todo o processo de auditoria ocorre de forma ímpar aos colaboradores, sendo realizado por terceiros devidamente autorizados e sempre acompanhados pelos responsáveis internos e envolvidos na produção da tecnologia.

O auditor devidamente autorizado e acompanhado, ainda que audite todas as fases do processo, não terá acesso as informações de características estratégicas ao produto de conhecimento. Ficando com a tarefa de verificar somente se a mesma é armazenada e disseminada em tempo e forma correta, podendo realizar questionamentos, mas em momento algum solicitar informações sobre a tecnologia desenvolvida.

3 **CONSIDERAÇÕES FINAIS**

Este trabalho foi elaborado com o objetivo de visualizar como a empresa base do estudo, gerencia e protege suas informações e seus conhecimentos estratégicos, como sugerido pelo decorrer do trabalho, com o objetivo de analisar parte deste processo, onde a informação da fatia de mercado muito especifica, impulsionou a criação de uma área de produção de conhecimento estratégico onde o seu produto final é uma tecnologia que reflete grande parte da receita bruta da empresa.

O produto de tecnologia que é gerado através do conhecimento garante a personalização de cartões para meios de pagamento utilizando chip de contatos, este que é imprescindível para a sobrevivência da organização neste setor, onde segurança e privacidade na manipulação dos dados garante vida longa e saudável aos negócios. Parte primordial da atuação da empresa é resumida a tecnologia de gravação onde todo o processo de preparação de dados para a realização da mesma e desenvolvido através da base de dados, conhecimento e informação, que é constantemente manipulada pela empresa, onde o resultado é um módulo de conhecimento tecnológico que é constantemente utilizado, modificado e comercializado pela organização, em suas diversas formas atendendo as diversas demandas de mercado.

Para que toda a tecnologia desenvolvida juntamente com sua base de conhecimento, seja assertiva durante a utilização do cliente final e principalmente, não se perca ou seja violada, acessada indevidamente ou disseminada de forma errada, em nenhuma hipótese, observamos no decorrer do trabalho que a empresa emprega mantem diversas formas de proteção do conhecimento, armazenando de forma segura todos os seus produtos de conhecimento e suas informações para desenvolvimento

Observa-se no decorrer do trabalho que são apresentados alguns pontos de vazamento informacional, onde a tecnologia desenvolvida e informações sensíveis de cliente e parceiros combinadas ou separadas são disseminadas de forma incorreta, deixando brechas para que ocorra falhas humanas, por pessoas que estejam envolvida ou até mesmo dentro do processo, não cumprimento ou desconhecimento de normas e procedimentos, vazamento de informações por terceiros envolvidos nos processo onde dados, informação e conhecimento estejam expostos de forma evidente ou sendo manipuladas .

Tendo conhecimento desses prováveis pontos de vazamento informacional, vimos que a empresa conta com procedimentos e proteções do conhecimento. Todo o conhecimento

produzido e manipulado é tratado de forma segura, seguindo normas e procedimentos internos, seguindo grandes níveis de exigência, evitando ao máximo que pessoas não autorizadas tenha acesso as informações e conhecimento desenvolvidos, evitando assim que ocorram vazamentos informacionais. Porém mesmo evidenciando um alto nível de segurança, observamos que apesar de haver auditorias nos processos, não se sabe os prazos para ocorram nem suas periodicidades. Mesmo tendo um setor interno de auditoria, não foi possível identificar ao longo da pesquisa um procedimento ou rotina de auditoria interna estruturadas e com rotinas pré-estabelecidas para garantir que todo o processo de proteção do conhecimento está sendo aplicado, e que sua tecnologia está segura.

Em resumo entende-se que a empresa produz com uma base de dados e informação amplas um produto de conhecimento estratégico, muito especifico e extremamente complexo, ligado diretamente ao negócio. No qual o seu desafio além de desenvolver este produto é armazenar de forma segura e eficiente suas informações e conhecimento, garantindo um produto de tecnologia seguro e exclusivo, para competir no mercado atual de constante mudanças tecnológicas.

REFERÊNCIAS

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.

BRACKETT, Michael H. Business Intelligence Value Chain. **DM Review**, [S.L], mar., 1999. Disponível em: <http://www.dmreview.com/channels/business_intelligence.html> Acesso em: 30 maio 2008 *apud* AYRES, Nilce Miranda. **Fatores Condicionantes de uma Gestão Estratégica da Informação:** uma contribuição na evolução da administração da informação e da tecnologia nas organizações. 2000. 170 f. Dissertação (Mestrado em Engenharia de Produção) – Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Santa Catarina, Florianópolis, 2000.

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. Tradução Bernadette Siqueira Abrão. São Paulo: Futura, 1998.

DE SORDI, José O. **Tecnologia da Informação aplicada aos negócios.** São Paulo: Atlas, 2003.

DADOS. In: FERREIRA, Aurélio Buarque H. **Minidicionário Aurélio**. Rio de Janeiro: Nova Fronteira, 1977.

PROTEÇÃO. In: 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.

KALE, P.; SINGH, H.; PERLMUTTER,H. Learning and protection of proprietary assets in strategic alliances: building relational capital. **Strategic Management Journal**, [S.L], v. 21, p. 217-237, 2000.

KAPLINSKY, Raphael. *et al*. Towards a Taxonomy of Knowledge Leakage: literature and Framework. In: KNOWLEDGE AND LEARNING TRACK BAM CONFERENCE, September, 2006,Belfast. **Anais.** [S.L : s.n], 2006 *apud* 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.

McGEE, James; PRUSAK, Laurence. **Gerenciamento estratégico da informação:** aumente a competitividade e eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. Tradução de Astrid Beatriz de Figueiredo. Rio de Janeiro: Elsevier, 1994.

MELO, Ivo Soares. **Administração de Sistemas de Informação.** São Paulo: Pioneira Thomson Learning, 2006.

MINTZBERG, Henry. **Ascensão e queda do planejamento estratégico.** Porto Alegre: Bookman, 2004.

MOHAMED, S. *et al*. Understanding one aspect of the knowledge leakage concept: people. In: EUROPEAN AND MEDITERRANEAN CONFERENCE ON INFORMATION SYSTEMS, july, 2006, Costa Blanca; Alicante; Spain. **Anais***.* [S.L : s.n], 2006.

NONAKA, Ikujiro; TAKEUCHI, Hirotaka. **The Knowledge-Creating Company:** how Japanese companies create the dynamics of innovation. USA: Oxford University Press, 1995. 304p.

POLANYI, Michel. The Tacit Dimension In: PRUSAK, L. (Ed.). **Knowledge in Organizations.** Newton, MA: Butterworth-Heinemann, 1997 *apud* NONAKA, Ikujiro; TAKEUCHI, Hirotaka. **The Knowledge-Creating Company:** how Japanese companies create the dynamics of innovation. USA: Oxford University Press, 1995. 304p.

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.

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

STEWART, Thomas A. **Capital Intelectual**: a nova vantagem competitiva das empresas. 10. ed. Rio de Janeiro: Campus, 1998.

SVEIBY, Karl E. **A nova riqueza das organizações:** gerenciando e avaliando patrimônios de conhecimento. Rio de Janeiro: Campus, 1998.

TEIXEIRA, F. L. C. (Org.). **Gestão de Redes de Cooperação Interempresariais:** em busca de novos espaços para o aprendizado e a inovação. Salvador: Casa de Qualidade, 2005.

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. 2007. 248 f. Tese (Doutorado em Informação Gerencial e Tecnológica) – Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2000.

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.

WIELINGA, B. *et al*. **Knowledge Engineering and Management:** the Common KADS Methodology. Cambridge, MT: The MIT Press, 2000.