Universidade Federal da Paraíba

Centro de Ciências Sociais Aplicadas

Programa de Pós-Graduação em Administração

Curso de Mestrado Acadêmico em Administração

ALUISIO BRUNO ATAÍDE LIMA

ANALISANDO A ADOÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DE BASE TECNOLÓGICA: A gestão do conhecimento como abordagem de investigação

João Pessoa

2013

ALUISIO BRUNO ATAÍDE LIMA

ANALISANDO A ADOÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DE BASE TECNOLÓGICA: A gestão do conhecimento como abordagem de investigação

Dissertação apresentada como requisito parcial para obtenção do título de mestre em Administração no Programa de Pós-Graduação em Administração da Universidade Federal da Paraíba.

Área de Concentração: Administração e Sociedade.

Orientador: Prof. Dr. Guilherme Ataíde Dias

João Pessoa
2013

ALUISIO BRUNO ATAÍDE LIMA

ANALISANDO A ADOÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DE BASE TECNOLÓGICA: A gestão do conhecimento como abordagem de investigação

Dissertação apresentada como requisito parcial para obtenção do título de mestre em Administração no Programa de Pós-Graduação em Administração da Universidade Federal da Paraíba.

Área de Concentração: Administração e Sociedade.

Dissertação aprovada em: 26 de abril de 2013.

Banca examinadora:

Prof. Dr. Guilherme Ataíde Dias (Orientador)
UFPB

Prof. Dr. Carlo Gabriel Porto Bellini (Examinador Interno)
UFPB

Profª. Drª. Emeide Nóbrega Duarte (Examinadora Externa)
UFPB

João Pessoa
2013

Agradecimentos

Agradeço a todos que fizeram parte da minha trajetória neste mestrado.

Em especial, a minha mãe, pois sem ela eu não conseguiria nada.

A minha família pelo apoio.

A Gabriela Medeiros, pelo amor e motivação.

Aos meus amigos, por acreditarem no meu potencial.

Ao meu orientador, professor Guilherme, por ser um guru.

Aos professores e funcionários do PPGA.

A CAPES e CNPQ, pelo suporte financeiro.

A todos, muito obrigado.

“You are young and life is long and there is time to kill today
And then one day you find ten years have got behind you
No one told you when to run, you missed the starting gun
And you run and you run to catch up with the sun, but it's sinking
And racing around to come up behind you again
The sun is the same in a relative way, but you're older
Shorter of breath and one day closer to death”

Pink Floyd, Time

RESUMO

Com a evolução da sociedade do conhecimento, os fatores clássicos de produção estão sendo superados pela informação como o ativo mais importante das organizações. Devido a essa crescente importância, garantir a segurança da informação é crucial para que as organizações obtenham sucesso. Nesse contexto, empresas de base tecnológica que desenvolvem soluções em Tecnologias de Informação e Comunicação são de grande relevância. O objetivo desta pesquisa se caracteriza por investigar como as empresas de base tecnológica procedem para garantir a segurança da informação e verificar se o compartilhamento de conhecimento é o principal meio pelo qual os indivíduos tentam garantir a segurança da informação. Também são objetivos desta pesquisa, investigar o conhecimento que os indivíduos associados a estas empresas têm sobre normas e melhores práticas de segurança da informação, além dos meios tecnológicos utilizados por eles. Para atingir os objetivos, foram escolhidas as empresas participantes do Farol Digital, nas quais foram realizadas entrevistas com seus funcionários utilizando-se de roteiros de entrevistas semi-estruturados como meio de coleta de dados. A análise de conteúdo foi a abordagem escolhida para inferir as conclusões. Utilizou-se como modelos conceituais o modelo de ciclo do conhecimento nas organizações elaborado pro Choo (2006) e o modelo de fatores que influenciam o compartilhamento de conhecimento elaborado por Ipe (2003). Verificou-se que os procedimentos de segurança da informação são desenvolvidos informalmente. Encontrou-se que o compartilhamento de conhecimento geral é constante nas organizações, mas quando o conhecimento é sobre segurança da informação, há muito pouco compartilhamento. Isso é explicado pelo fato do tema segurança da informação ser crítico, de forma que uma informação equivocada que foi compartilhada pode gerar consequências danosas para quem compartilhou, pois a principal vantagem relativa ao compartilhamento de conhecimento é a boa reputação que adquire que compartilha. Desta forma, eles evitam compartilhar conhecimentos relativos à segurança da informação temendo que a sua imagem possa ser negativada e deixam a responsabilidade das decisões de segurança para os líderes e gerentes de projeto.

Palavras-chave: Segurança da Informação; Compartilhamento de conhecimento; Empresas de base tecnológica.

ABSTRACT

Along the rise of the knowledge society, the classical factors of production are being overtaken by the information as the most important asset of organizations. Due to this growing importance, ensure information security is crucial for organizations to succeed. In this context, technology-based companies that develop Information and Communication Technologies (ICT) solutions are of great importance. The objective of this research is characterized by investigating how the technology-based companies proceed to ensure information security and verify if knowledge sharing is the primary mean by which individuals attempt to ensure information security. Also are objectives of this research, investigating the knowledge that individuals associated with these companies have about standards and best practices in information security, besides the technological means used by them. To achieve our goals, we selected the participating companies from Farol Digital, and conducted semi-structured interviews with employees for data collection. Content analysis was the chosen approach to infer conclusions. As conceptual models we used Choo's (2006) knowledge cycle in organizations and the model of factors that influence knowledge sharing developed by Ipe (2003). We found that the information security procedures are developed informally. We also found that knowledge sharing is quite frequent in organizations, except when the knowledge is about information security. We explain this by the fact that the information security is a critical issue, where sharing wrong information can lead to harmful consequences for the sharer because the main advantage for sharing knowledge is the prestige acquired. Thus, they avoid sharing knowledge related to information security fearing that his image can be damaged, passing the responsibility of the security decisions to leaders and project managers.

Key-words: Information security; Knowledge sharing; Technology-based companies.

Lista de figuras

Lista de Quadros

Sumário

1 INTRODUÇÃO

Evidências empíricas e informais indicam que o número de incidentes relacionados à segurança da informação aumentou (AIRC 2008; SYMANTEC 2009) mesmo em organizações que investem em soluções de segurança baseadas em tecnologia. O sucesso na segurança da informação pode ser alcançado quando as organizações investem tanto em recursos técnicos quanto sociais (BULGURCU; CAVUSOGLU; BENBASAT, 2010). O foco da segurança da informação tem mudado em relação aos indivíduos e às perspectivas organizacionais, a observância das políticas de segurança da informação pelos empregados tem surgido como um recurso organizacional chave (BOSS, KIRSCH, 2007; SIPONEN, PAHNILA, MAHMOOD, 2007), pois as pessoas são geralmente o elo mais fraco na segurança da informação (MITNICK; SIMON, 2002; WARKENTIN; WILLISON, 2009).

As organizações criam políticas que provêm guias para os empregados fornecendo informações sobre como garantir a segurança da informação enquanto eles usam sistemas de informações na realização de seus trabalhos (WHITMAN *et al*. 2001). Embora, seja sabido que, em empresas de pequeno e médio porte, tais políticas de segurança podem não existir formalmente, ficando as decisões sobre a segurança a cargo dos funcionários. Para que os indivíduos tomem tais decisões, eles necessitam de conhecimentos sobre segurança da informação.

A gestão do conhecimento tem sido definida como o processo de capturar, armazenar, compartilhar e usar o conhecimento (DAVENPORT; PRUSAK, 1998). Pesquisas anteriores focavam na representação explícita e formal do conhecimento e sistemas de gestão do conhecimento, Davison, Ou e Martinsons (2012) argumentam que muitas vezes a gestão do conhecimento se dá através de sistemas informais. Historicamente, este compartilhamento informal do conhecimento tem acontecido nos "corredores", mas agora também é mediado pela Tecnologia da Informação, através de fóruns, *blogs*, *chats* e *wikis*.

O compartilhamento do conhecimento se torna relevante, particularmente, pelo fato de prover uma ligação entre o conhecimento individual possuído pelos indivíduos e o conhecimento organizacional, onde o conhecimento ganha valor (HENDRIKS, 1999). Vários fatores foram identificados como barreiras ao compartilhamento de informação, como estruturas organizacionais inadequadas e culturas organizacionais não propícias ao compartilhamento (DAVENPORT; PRUSAK, 1998). Assim, tecnologias são utilizadas na tentativa de dar suporte ao compartilhamento de conhecimento. A expectativa é de que elas

possam prover aos indivíduos ferramentas que apoiem e impulsionem suas habilidades de compartilhamento (TAMPOE, 1996).

Empresas de base tecnológica são caracterizadas pela inovação e criação de novos produtos, seja desenvolvendo novas tecnologias ou aplicando tecnologias existentes. O mercado de empresas que desenvolvem soluções em Tecnologia da Informação e Comunicação (TIC) no estado da Paraíba é caracterizado por empresas de base tecnológica de médio e pequeno porte, conforme podemos verificar através do Farol Digital[1], um projeto de parceria entre o SEBRAE-PB e empresas do setor de TIC.

O tema da presente pesquisa se justifica pela observação resultante da experiência prática do autor em trabalhar com o desenvolvimento de produtos de software em empresas de médio e pequeno porte e por conhecer como é o funcionamento de outras. O que foi observado é que não havia a formalização dos procedimentos relativos à segurança da informação por parte das empresas.

O estudo das práticas relativas à segurança da informação e ao compartilhamento de informações poderá trazer contribuições para as empresas do setor das TIC. Pois, elas poderão ter uma visão da situação em que se encontram em relação a tais práticas, poderão reforçar estratégias que se mostram benéficas, consertar ou abandonar comportamentos prejudiciais, além de poderem adotar novas abordagens que melhorem o compartilhamento de informação.

Busca-se com esta pesquisa investigar o que acontece nas organizações que ainda não se adequaram a nova realidade da segurança da informação e não possuem uma política de segurança explícita. Desta forma, procura-se responder a seguinte questão de pesquisa: **De que maneira os indivíduos vinculados a empresas de base tecnológica procedem ao tratar de questões relacionadas à segurança da informação quando da ausência de uma política de segurança explícita na organização?**

A coleta dos dados necessários para responder tal questão foi realizada através da entrevista qualitativa. Foram entrevistados analistas de sistema e desenvolvedores de *software* vinculados a empresas que desenvolvem soluções em TIC, sediadas em João Pessoa e Campina Grande e que são participantes do Farol Digital.

O presente trabalho tem sua estrutura dividida da seguinte maneira: inicialmente são expostos os objetivos da pesquisa, depois se faz uma discussão teórica, abordando os três pilares teóricos da pesquisa, segurança da informação, compartilhamento de conhecimento e

[1] Site do Farol Digital: www.faroldigital.org.br

empresas de base tecnológica. No capítulo posterior, esclarecem-se as características metodológicas e descrevemos como foi feita a coleta de dados. Em sequência, realizou-se a análise dos dados e apresentou-se os resultados dessa análise. Por final, apresentou-se as conclusões, as limitações da pesquisa e sugeriu-se pesquisas futuras.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Conhecer as práticas e comportamentos de disseminação do conhecimento empreendidos pelos indivíduos em organizações de base tecnológica que não apresentam uma política de segurança da informação formal e explícita.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar o nível de conhecimento de guias de melhores práticas em gestão de segurança pelos indivíduos;
- Explicar o compartilhamento de conhecimento como prática utilizada na ausência da política de segurança;
- Identificar os insumos de Tecnologia da Informação utilizados no processo de disseminação do conhecimento;
- Delinear uma proposta de incentivo ao compartilhamento de conhecimento com suporte de TI em empresas de base tecnológica.

3 REFERENCIAL TEÓRICO

3.1 SEGURANÇA DA INFORMAÇÃO

A habilidade de uma organização atingir seus objetivos é baseada na utilização significativa e produtiva dos seus recursos (ANDERSON; CHOOBINEH, 2008). A forma e a fonte de ameaças a esses recursos mudou com o desenvolvimento de sistemas de computador, redes eletrônicas, armazenagem de dados e troca de informação (GERBER; VON SOLMS, 2001). Tecnologias de informação dão suporte, controlam e gerenciam processos de negócios e se tornaram um dos recursos mais valiosos e vulneráveis (ANDERSON; CHOOBINEH, 2008).

A informação se tornou um recurso vital para o negócio. Ela é de extremo valor para a organização e, como qualquer outro recurso valioso, a informação deve ser adequadamente protegida (WILLS, 1999 *apud* GERBER; VON SOLMS, 2001). Segundo o padrão ISO/IEC 17799:2005, segurança da informação é a proteção da informação contra várias ameaças, de forma a garantir a continuidade do negócio e minimizar os riscos.

Nos últimos tempos, tem sido amplamente aceito que a segurança da informação deixou de ter uma imagem apenas técnica e passaram a existir várias facetas que devem ser consideradas na criação de um ambiente de TI seguro (VON SOLMS, 2001). Von Solms (2001) caracteriza essas facetas como dimensões, das quais se destacam as dimensões da Política, da Organização, das Pessoas, da Técnica e da Consciência.

Os códigos de melhores práticas de gerência da segurança da informação afirmam que antes de qualquer implementação de segurança ser posta em prática, deve existir uma política de segurança da informação. Não se pode controlar a segurança da informação se não existe um *framework*[2] de referência, a política de segurança é esse *framework* básico de referência. Assim, a dimensão da política também inclui subpolíticas, procedimentos e padrões que governa as ações relevantes com respeito à segurança da informação (VON SOLMS, 2001).

A segurança da informação, enquanto questão organizacional, deve ser estruturada e organizada. A dimensão da organização não se refere apenas à estrutura organizacional, mas também a vários aspectos como a relação da segurança da informação com as

[2] No contexto desta pesquisa, *framework* é definido genericamente como uma estrutura real ou conceitual que serve de suporte ou guia para a construção de algo que expande esta estrutura em algo útil (ROUSE, 2005).

responsabilidades dos cargos, a comunicação entre os papéis na segurança da informação e o envolvimento da alta gerência (VON SOLMS, 2001). Tais preocupações são essenciais para o sucesso da implementação da segurança da informação.

As dimensões da técnica, das pessoas e da consciência são fortemente relacionadas, podendo ser resumidas na dimensão da consciência. Esta dimensão tem atraído a atenção das organizações, pois não basta investir em tecnologias, se as pessoas não forem cuidadosas com suas informações, não tiverem as capacidades necessárias para utilizar as tecnologias, nem forem conscientes quanto a segurança da informação, essas tecnologias não servirão para protegê-las.

A segurança da informação existiu mesmo antes da invenção do computador (DLAMINI; ELOFF; ELOFF, 2009). Segundo Russell e Gangemi (1991 *apud* DLAMINI; ELOFF; ELOFF, 2009), a segurança da informação é tão antiga quanto a informação. Desde que ela começou a ser transmitida e armazenada passou a requerer proteção, como por exemplo, os imperadores romanos, que buscavam através da codificação proteger as mensagens enviadas.

As inovações e desenvolvimentos do século XXI vieram com uma forte dependência da infraestrutura de TI. O futuro da segurança da informação permanece obscuro, mas duas coisas permanecem certas: infraestruturas de TI são vulneráveis e sempre haverá pessoas motivadas a explorar essas vulnerabilidades (DLAMINI; ELOFF; ELOFF, 2009). Assim como as TIC provêm novas oportunidades para as organizações expandirem, elas também apresentam oportunidades para pessoas com intenções criminosas (CHOO, 2011).

Basicamente, a segurança da informação refere-se à preservação da confidencialidade, integridade e disponibilidade das informações e dos sistemas que usam, armazenam e transmitem informações (ISO, 2005). A confidencialidade trata de prevenir ou detectar a divulgação indevida de informação. Integridade, diz respeito à informação não ser modificada por pessoas não autorizadas. E disponibilidade refere-se a permitir que apenas pessoas autorizadas tenham acesso a informação (SIPONEN; BASKERVILLE; HEIKKA, 2006).

Questões de segurança da informação não são mais uma preocupação exclusiva de organizações de alto risco, como militares ou setores do governo. Os prejuízos causados por uma falha de segurança podem ser enormes em termos financeiros, de confiabilidade e credibilidade da organização (CAVUSOGLU; CAVUSOGLU; RAGHUNATHAN, 2004). Recentemente, tivemos na mídia mundial, exemplos como o *site* Wikileaks, que vazou

informações confidenciais de diversos governos, como também o vazamento de dados de usuários da PlayStation Network (PSN).

Durante muito tempo as organizações trataram a segurança da informação como um subproduto, senão como um "mal necessário que dificulta a produtividade" (CONRAY-MURRAY, 2003), entretanto, lentamente a segurança da informação tem se promovido, passando a ser considerada parte das operações de negócios (CONNER; COVIELLO, 2004).

A evolução dos recursos de informações tem introduzido novos problemas gerenciais que requerem novas políticas, tecnologias e capacidades organizacionais (GORDON; LOEB, 2002; KARYDA; KIONTOUZIS; KOKOLAKIS, 2005). A segurança da informação é agora uma questão de gerência, nessa perspectiva, soluções técnicas são importantes, mas o foco deve ser nas ações gerenciais para promover a segurança no ambiente da informação (RANSBOTHAM; MITRA, 2009).

3.1.1 Gerência da Segurança da Informação

A gerência da segurança da informação é o processo de administrar pessoas, políticas e programas com o objetivo de garantir a continuidade das operações enquanto mantém o alinhamento estratégico com a missão organizacional (CAZEMIER *et al.*, 2000 apud CHOOBINEH *et al.*, 2007). Ela é interessada nas questões estratégicas, táticas e operacionais que se relacionam com o planejamento, análise, design, implementação e manutenção do programa organizacional de segurança da informação (CHOOBINEH *et al.*, 2007).

Historicamente, a gerência da segurança da informação é relacionada a estabelecer controles técnicos e físicos, mas pesquisas mostram que sua ênfase vai além dos controles técnicos e incorpora processos e questões organizacionais (CHOOBINEH *et al.*, 2007). O crescente uso, dependência e valor dos sistemas computadorizados tem aumentado a importância de incorporar esses processos e questões organizacionais no gerenciamento do risco de segurança (DRUCKER, 1992; BLAKLEY; McDERMOTT; GERR, 2001).

Segundo Von Solms (2005), a gerência da segurança da informação é formada pela liderança e comprometimento da gerência, políticas de comprometimento e conscientização dos usuários, procedimentos, processos e tecnologias, todas trabalhando em conjunto para proteger os ativos das organizações.

Ainda de acordo com Von Solms (2005), a gerência da segurança da informação se divide em duas partes: gerência operacional da segurança da informação e gerência do

cumprimento da segurança da informação. As atividades da gerência operacional da segurança da informação dão falsa impressão de que a segurança da informação é um trabalho essencialmente técnico. Ter uma política de segurança escrita não garante o seu cumprimento, para isso são realizadas as atividades da gerência do cumprimento da segurança da informação.

Vários guias para gerência da segurança da informação tem sido propostos, eles tentam prover as melhores práticas para gerência da segurança da informação. Como exemplo, temos: TCSEC/Orange Book, GMITS, CobiT, IT Baseline Protection Manual. As organizações usam estes guias e para demonstrar comprometimento com as práticas de segurança tentam aplicar certificações que atestam o cumprimento de regras e práticas (SIPONEN; WILLISON, 2009).

3.1.2 Políticas de Segurança da Informação

Existem vários controles e medidas que podem e necessitam ser implementados dentro de uma organização para garantir o funcionamento efetivo da segurança da informação, mas indubitavelmente o mais importante desses controles é a política de segurança da informação (HONE; ELOFF, 2002). Há um crescente consenso entre as comunidades acadêmicas e práticas de que a política de segurança da informação é a base para a disseminação e execução de práticas de segurança dentro do contexto organizacional (DOHERTY; FULFORD, 2006).

A política de segurança da informação é um documento de direcionamento para segurança da informação dentro de uma organização (JISC, 2001), em essência, a política de segurança é documentada para explicar a necessidade de segurança e seus conceitos para os usuários dos recursos informacionais. Ela deve ser um complemento aos objetivos do negócio e deve refletir a vontade da organização operar em uma maneira segura (HONE; ELOFF, 2002).

Os documentos da política de segurança devem ser escritos pela alta gerência e devem ser o “o que” da segurança na organização, são considerados como políticas de alto nível. Enquanto que as políticas técnicas ou de implementação, denominadas de políticas de baixo nível, são criadas a partir da política de alto nível, ela é o “como” e é usada para executar a política de segurança (MACFARLANE *et al*, 2012). Ambas as políticas de alto e baixo nível são descritas na literatura pelo termo política de segurança.

As políticas de alto nível expressam os objetivos e preocupações de segurança no seu mais alto nível de abstração. São declarações sobre a importância dos recursos informacionais e definições sobre as responsabilidades da gerência e dos empregados em proteger esses recursos. As políticas de baixo nível seguem as políticas de alto nível, elas definem processos organizacionais que dizem como a organização deve funcionar no que diz respeito à segurança. Elas ajudam a identificar áreas de vulnerabilidade e necessidades de controle. Geralmente, também indicam medidas alternativas de segurança e sanções para aqueles que não sigam a política. Baskerville e Siponen (2002) incluem mais um nível, o nível de meta-política, no qual é definido o plano de criação e manutenção da política de segurança.

A política dever ser clara, concisa e fácil de seguir (MADIGAN; PETRULICH; MOTUK, 2004), mas acima de tudo ela deve ser realista. Ela deve ser implementável e executável na prática (HONE; ELOFF, 2002). Se ela não é bem desenvolvida, não será executada propriamente e os objetivos de segurança não serão alcançados (MADIGAN; PETRULICH; MOTUK, 2004).

Hone e Eloff (2002) definem os elementos que devem estar contidos num documento de política de segurança para que a mesma seja completa:

> Necessidade e escopo da segurança da informação, objetivos da segurança da informação, definição de segurança da informação, gerência do comprometimento com a segurança da informação, aprovação da política de segurança da informação, propósitos da política de segurança da informação, princípios da segurança da informação, papéis e responsabilidades, violações da política de segurança da informação e ações disciplinares, referências cruzadas e elementos gerais.

Os empregados são considerados como sendo potenciais ameaças a segurança da informação e também é reconhecido que eles podem contribuir para proteção da informação e dos recursos tecnológicos, desempenhando ações benéficas (BULGURCU; CAVUSOGLU; BENBASAT, 2010). As organizações criam as políticas de segurança da informação estipulando quais os papéis que os funcionários devem desempenhar, mas a simples existência de tais controles não se traduz automaticamente em comportamentos desejáveis, pois os funcionários podem não se sentirem motivados a desempenhá-los (STANTON *et al.* 2005).

Uma política de segurança pode ser utilizada como a fundação sobre a qual os aspectos operacionais da cultura da segurança na empresa podem ser construídos (HARLOW,

2001). O estilo de escrita da política deve refletir a cultura organizacional para garantir a aceitação do documento pelos empregados das organizações (HONE; ELOFF, 2002).

É importante que os usuários entendam a segurança em algum nível, mas existem algumas barreiras (COX; CONNOLY, 2001). O número de brechas de segurança que envolve o mau uso dos recursos de informação destaca a importância das organizações reduzirem tais comportamentos (D'ARCY; HOVAV; GALLETA, 2009). A melhor forma de garantir a viabilidade de uma política de segurança é se certificar que os usuários entendam e aceitem as precauções necessárias. (WHITMAN *et al.*, 2001).

3.1.3 Conscientização da política de segurança da informação

Ao explanar a conscientização da segurança da informação, Bulgurcu, Cavusoglu e Benbasat (2010) a definem como a combinação do conhecimento geral que o empregado tem sobre segurança da informação com o conhecimento sobre a política de segurança da sua organização. A consciência sobre a segurança da informação no geral é o conhecimento e entendimento que o empregado tem sobre potenciais questões sobre segurança da informação, enquanto que a consciência sobre a política de segurança é o conhecimento e entendimento sobre os requisitos prescritos na política de segurança da organização e os objetivos desses requisitos.

A consciência sobre a segurança da informação no geral se distingue da consciência sobre a política de segurança, por exemplo, uma pessoa pode estar consciente de que ao se utilizar senhas, é necessário tomar algumas precauções, mas ele pode não saber que a política de segurança da informação da sua organização exige que a senha deve ser trocada periodicamente e dever ter tamanhos e composição de caracteres predeterminados.

Garantir que os empregados se conscientizem e sigam os procedimentos chave de segurança da informação da organização se torna essencial para a efetividade da segurança da informação. Sobre as formas de se buscar a sensibilização dos empregados, Karjalainen e Siponen (2011) citam algumas abordagens existentes na literatura, como as que usam sanções e dissuasão (STRAUB, 1990; SIPONEN; PAHNILA; MAHMOOD, 2007), campanhas de marketing (MCLEAN, 1992) e treinamento (PUHAKAINEN; SIPONEN, 2010).

De acordo com o padrão ISO/IEC 17799 (2005), a conscientização de segurança está aliada a educação e treinamento. Tais atividades devem ser adequadas e relevantes aos papéis, responsabilidades e habilidades das pessoas, e devem incluir informações sobre ameaças conhecidas, quem contatar para conselhos sobre segurança e canais apropriados para

reportar incidentes de segurança da informação. Garantir a consciência da segurança da informação pode direta e indiretamente mudar os conjuntos de crenças sobre a conformidade com a política de segurança da informação. Isto implica que a criação de uma cultura de consciência da segurança aumentará a segurança da informação. Bulgurcu, Cavusoglu e Benbasat (2010) sugerem que os programas de treinamento e conscientização reforcem também a auto-eficácia dos empregados sobre a adequação.

3.2 CONHECIMENTO COMO ATIVO DA ORGANIZAÇÃO

Nos últimos anos, vários autores tem argumentado que existe uma mudança no pensamento das organizações (GRANT, 1996). Os fatores clássicos de produção têm se tornado secundários (DRUCKER, 1992) e a informação tem se tornado o ativo dominante nas organizações. Embora, muitos questionem que esse ativo seja o conhecimento e não a informação (COAKES, 2004). O conhecimento é considerado como um dos mais valiosos recursos da organização, pois ele representa ativos intangíveis, rotinas operacionais e processos criativos, que são difíceis de imitar (GRANT, 1996; SAMBAMURTHY; SUBRAMANI, 2005) e devem ser manipulados para obter vantagem competitiva (COAKES, 2004).

A crescente importância do conhecimento na sociedade contemporânea faz necessária a mudança no pensamento a respeito da inovação nas organizações (NONAKA, 1994). Cada vez mais o conhecimento é distribuído entre indivíduos, equipes e organizações (SAMBAMURTHY; SUBRAMANI, 2005). Considerações detalhadas sugerem que o conhecimento é uma faca de dois gumes, enquanto pouco leva a ineficiência, muito leva a rigidez e contraprodução (MARCH, 1991).

A área de estudos organizacionais que ressalta a importância do conhecimento como principal recurso é a visão da firma baseada em recursos. Ela tenta explicar como algumas firmas conseguem estabelecer posições de vantagem competitiva sustentável e assim atingirem resultados superiores. A visão da firma baseada em conhecimento é uma consequência da visão baseada em recursos, ela foca no conhecimento como o recurso estratégico mais importante da firma (GRANT, 1996).

A perspectiva baseada em conhecimento postula que os serviços prestados dependem da forma como os recursos tangíveis são combinados e aplicados, o que é uma função do *know-how* da empresa, ou seja, o conhecimento. Esse conhecimento é manifestado dentro da organização através de múltiplas entidades que incluem a cultura e identidade da

empresa, rotinas, políticas, sistemas, documentos e indivíduos (GRANT, 1996a, 1996b; SPENDER, 1996).

O desenvolvimento da teoria da firma baseada no conhecimento levanta uma questão: o que é conhecimento? (GRANT, 1996). Existem dificuldades associadas com a definição e identificação do conhecimento (SCHLTZE; LEIDENER, 2002). O conhecimento é um conceito multifacetado, com seus significados em múltiplos níveis. Vários fatores determinam a natureza da sua criação, gestão, valoração e compartilhamento (NONAKA, 1994).

3.3 DADO, INFORMAÇÃO E CONHECIMENTO

Embora os termos “informação” e “conhecimento” sejam usados alternadamente com frequência, há uma clara distinção entre eles (NONAKA, 1994). A chave para distinguir entre informação e conhecimento não é encontrada no conteúdo, estrutura, precisão ou utilidade do suposto conhecimento ou informação. Muitos autores, muito notadamente na literatura de TI, abordam a questão do conhecimento através da distinção entre conhecimento, informação e dado (ALAVI; LEIDENER, 2001). Uma definição muito comum e com pouca variação é que dados são fatos e números crus, informação são dados processados e o conhecimento é a informação autenticada (DRESKE, 1981; MACHLUP, 1983; VANCE, 1997). Por ser a definição mais comum, esta última foi adotada como referência no desenvolvimento desta pesquisa.

A discussão sobre o conceito de conhecimento existe, pelo menos, desde os tempos da Grécia antiga. Vários estudos existem diferenciando dado, informação e conhecimento. Algo comum nesses estudos é a existência de uma hierarquia entre os conceitos, caracterizando uma pirâmide que tem o dado na base e ascende para o conhecimento no topo (FAUCHER; EVERETT; LAWSON, 2010). Entretanto, Tuomi (1999) sugere que esta ordem deve ser inversa, onde o conhecimento deve antes existir para que a informação possa ser formulada e para que o dado possa ser mensurado para formar informação.

Os dados emergem por último, apenas depois de haver informação e conhecimento disponíveis. Não existem pedaços de fatos isolados, ao menos que alguém os tenha criado usando o seu conhecimento. Os dados emergem apenas se uma estrutura de significado, ou semântica, é primeiro definida e assim usada para representar a informação (TUOMI, 1999).

Os dados existem como solução para o problema de representar a informação em uma forma que possa ser modelada, representada e processada. O conhecimento de um indivíduo é articulado de forma que se torne focado e estruturado, se isso é feito através de um contexto linguístico e conceitual ele pode se tornar verbal e textual e nesse momento temos informação. Para armazenar esse conhecimento articulado, a informação deve ser dividida em pedaços que não tem significado. Assim, criam-se dados ao colocar a informação em estruturas predefinidas que definem seu significado completamente. Esta hierarquia reversa mostra a informação como um produto que é criado do conhecimento. Toda essa discussão em torno das definições de dado, informação e conhecimento ainda é muito polêmica, estando longe de chegar a uma conclusão.

3.4 PERSPECTIVAS DO CONHECIMENTO

Uma porção significante do conhecimento que as organizações buscam adquirir está incorporada em indivíduos (SONG; ALMEIDA; WU, 2003). O conhecimento é definido como uma crença justificada que aumenta a capacidade de um indivíduo agir efetivamente (NONAKA. 1994). Existem várias perspectivas possíveis pelas quais o conhecimento pode ser visto. Alavi e Leidner (2001) elencam cinco perspectivas pelas quais o conhecimento pode ser visto, sendo elas: estado da mente, um objeto, um processo, uma condição de obtenção de acesso à informação ou uma capacidade.

A perspectiva do conhecimento como um estado da mente permite que os indivíduos expandam seus conhecimentos e aplique-os nas necessidades organizacionais (ALAVI; LEIDNER, 2001). Na segunda perspectiva, onde o conhecimento é definido como um objeto (CARLSSON et al., 1996; McQUEEN, 1998; ZACK, 1998a), o conhecimento pode ser visto como uma coisa a ser manipulada e armazenada (ALAVI; LEIDNER, 2001).

O conhecimento pode ser visto como um processo de simultaneamente conhecer e agir (CARLSSON et al., 1996; McQUEEN, 1998; ZACK, 1998a), essa perspectiva é focada na aplicação da expertise (ZACK, 1998a). Na quarta visão, onde o conhecimento é visto como uma condição de acesso à informação (MCQUEEN, 1998), o conhecimento organizacional deve ser organizado de forma que o acesso e a recuperação do conteúdo sejam facilitados. Ela é uma extensão da visão do conhecimento como um objeto e foca especialmente na acessibilidade aos objetos de conhecimento (ALAVI; LEIDNER, 2001).

Por último, o conhecimento pode ser visto como uma capacidade com o potencial de influenciar futuras ações (CARLSSON et al., 1996). O conhecimento não é uma capacidade para realizar uma ação específica, mas a capacidade de usar informação (WATSON, 1999). O aprendizado e a experiência resultam em uma habilidade de interpretar informação e verificar que a informação é necessária na tomada de decisão (ALAVI; LEIDNER, 2001).

As diferentes visões do conhecimento levam a diferentes percepções na gestão do conhecimento (CARLSSON et al., 1996). A maior implicação destas várias concepções de conhecimento é que cada perspectiva sugere uma estratégia diferente para gerenciar o conhecimento e uma perspectiva diferente do papel dos sistemas em apoiar a gestão do conhecimento (ALAVI; LEIDNER, 2001).

3.5 CONHECIMENTO TÁCITO X CONHECIMENTO EXPLÍCITO

Inspirado no trabalho de Polanyi (1962, 1967), Nonaka (1994) aborda as duas dimensões do conhecimento nas organizações: tácita e explícita. A dimensão tácita do conhecimento, referida como conhecimento tácito, se baseia na ação, experiência e envolvimento em um contexto específico, sendo composta por elementos cognitivos e técnicos. A dimensão explícita do conhecimento, referida como conhecimento explícito, é articulada, codificada e comunicada em forma simbólica ou em linguagem natural (ALAVI; LEIDNER, 2001).

Algo de potencial problema nesta classificação é o pressuposto geralmente adotado de que o conhecimento tácito tem mais valor que o conhecimento explícito, visto que tem recebido maior interesse e atenção do que o conhecimento explícito. (ALAVI; LEIDNER, 2001). Tais dimensões não são estados dicotômicos do conhecimento, mas são mutuamente dependentes e reforçam qualidades do conhecimento. O conhecimento tácito compõe o background necessário para o desenvolvimento e interpretação do conhecimento explícito (POLANYI, 1975).

3.6 GESTÃO DO CONHECIMENTO

O recente interesse no conhecimento organizacional tem impulsionado a questão de gerenciar o conhecimento para o benefício da organização (ALAVI; LEIDNER, 2001). A emergência desta disciplina coincide com o desenvolvimento da economia baseada no

conhecimento, onde a ênfase tem mudado dos fatores tradicionais de produção para o conhecimento (JASIMUDDIN, 2008).

A gestão do conhecimento nas organizações está se tornando importante e até mesmo um fator decisivo de competitividade (HANISCH *et al*., 2009) e tem desenvolvido a necessidade de gerenciar o dado, a informação e o conhecimento tão bem para usá-los para obter vantagem competitiva (RANDEREE, 2006).

As soluções de negócio não são criadas de improviso, elas são geradas usando a experiência coletiva da firma, a gestão do conhecimento consiste de processos e ferramentas para efetivamente capturar e compartilhar dados assim como usar o conhecimento coletivo dos indivíduos dentro de uma organização (OFEK; SARVARY, 2001; RANDEREE, 2006).

O conhecimento existe em múltiplos níveis dentro das organizações, para Delong e Fahey (2000), os níveis se dividem em individual, de grupo e de organização. Roos e Von Krogh (1992) adicionam os níveis de departamento e de divisões. É central para a perspectiva da gestão do conhecimento, a noção que os indivíduos nas organizações possuem conhecimento (SPENDER; GRANT, 1996) que devem ser transferidos para o nível de grupos e de organização como um todo de forma que pode ser utilizado para atingir os objetivos da organização (NONAKA, 1994).

A literatura da área do aprendizado individual contribui para a noção de que o conhecimento das organizações reside nos indivíduos (IPE, 2003). No nível individual, Lowendahl, Revang e Fosstenlokken (2001) identificam três tipos de conhecimento: o *know-how*, o *know-what* e o conhecimento disposicional. *Know-how* inclui o conhecimento baseado na experiência, que é subjetivo e tácito. O *know-what* inclui conhecimento relacionado a tarefas, sendo objeto em natureza. O conhecimento disposicional é definido como o conhecimento pessoal que inclui talentos, aptidões e habilidades.

A forma de gerenciar o conhecimento com sucesso está sendo vista como dependente das conexões entre os indivíduos dentro das organizações (BROWN; DUGUID, 1991; McDERMOTT, 1999). Entretanto, na prática, a falta de compartilhamento de conhecimento tem sido uma das principais barreiras para a gestão efetiva do conhecimento nas organizações (DAVENPORT; PRUSAK, 1998; HENDRIKS, 1999).

3.7 COMPARTILHAMENTO DE CONHECIMENTO

Na sociedade baseada em conhecimento, a principal ênfase das organizações está nos processos de compartilhamento de conhecimento, o qual cresce como sendo crucial para o

sucesso das organizações (BARRET *et al*., 2004). De acordo com Cohen e Levinthal (1990), o compartilhamento de conhecimento é um fator crítico para a habilidade de uma organização responder criticamente à mudança, inovar e atingir sucesso competitivo. Ele é importante por promover uma ligação entre a organização e o indivíduo, pois, leva o conhecimento que existe nos indivíduos para o nível organizacional, onde é convertido em valor econômico e competitivo para a organização (HENDRIKS, 1999).

Os indivíduos nas organizações sempre criaram e compartilharam conhecimento, além disso, o compartilhamento do conhecimento é considerado como uma função natural dos ambientes de trabalho (CHAKRAVARTHY; ZAHEER; ZAHEER, 1999 *apud* IPE, 2003). Embora os indivíduos constituam apenas um nível no qual o conhecimento reside nas organizações, o compartilhamento de conhecimento individual é imperativo para a criação, disseminação e gerenciamento do conhecimento em todos os outros níveis dentro de uma organização (IPE, 2003).

O compartilhamento extensivo de conhecimento dentro das organizações aparenta ser mais uma exceção do que uma regra (BOCK; LEE; ZMUD, 2005). Acumular conhecimento e avaliar cautelosamente o conhecimento oferecido pelos outros são tendências humanas naturais (DAVENPORT; PRUSAK, 1998 *apud* IPE, 2003).

Compartilhamento de conhecimento é basicamente a ação de tornar o conhecimento disponível para outros dentro da organização (IPE, 2003). Ele implica o relacionamento entre pelo menos duas partes: uma que possui o conhecimento e outra que adquire o conhecimento (HENDRIKS, 1999). O uso do termo “compartilhar” envolve alguma ação consciente por parte do indivíduo que possui o conhecimento (IPE, 2003).

Baseado em uma revisão de literatura relacionada a compartilhamento de conhecimento, Ipe (2003) lista os principais fatores que influenciam o compartilhamento de conhecimento entre indivíduos nas organizações: **natureza do conhecimento**, **motivação para compartilhar**, **oportunidade de compartilhamento** e a **cultura do ambiente de trabalho.** Além desses fatores, podemos adicionar um fator identificado por Siemsen et al (2009): **segurança psicológica.**

As oportunidades para compartilhar conhecimentos nas organizações podem ser formais ou informais. Oportunidades formais incluem programas de treinamento, times estruturados e sistemas tecnológicos que facilitam o compartilhamento (IPE, 2003). Oportunidades informais incluem relacionamentos pessoais e redes sociais que facilitam a aprendizagem e o compartilhamento (BROWN; DUGUID, 1991; NAHAPIET; GHOSHAL, 1998).

Embora os canais formais de compartilhamento sejam importantes para facilitar o compartilhamento do conhecimento, pesquisas indicam que a maior parte do conhecimento é compartilhada em situações informais (PAN; SCARBROUGH, 1999; TRURAN, 1998). Assim como afirmado por Stevenson e Gilly (1991), mesmo quando existem canais de comunicação claramente designados em uma organização, os indivíduos tendem a se comunicar através de relacionamentos informais.

A prevalência de comunicação por canais informais ocorre pelo fato do conhecimento organizacional informal ser tipicamente tácito e dinâmico (DAVISON; OU; MARTINSONS, 2012) não sendo facilmente suportado por sistemas formais (MARTINSONS; WESTWOOD, 1997) requerendo que os indivíduos se envolvam em altos níveis de relações interpessoais.

Iniciativas informais de compartilhamento são amplas e importantes pelo fato delas facilitarem a abstração do conhecimento tácito, menos estruturado e altamente contextual (DAVISON; OU; MARTINSONS, 2012). O conhecimento explícito, por sua vez, pode ser facilmente codificado, armazenado e transferido através do tempo e espaço independentemente dos indivíduos (LAM, 2000). A característica tácita do conhecimento é um impedimento natural para o sucesso do compartilhamento de conhecimento entre indivíduos nas organizações (DAVISON; OU; MARTINSONS, 2012).

O conhecimento explícito tem uma vantagem natural sobre o conhecimento tácito em termos de sua capacidade de ser fácil de ser compartilhado entre os indivíduos. Entretanto, não se deve assumir que ele realmente é facilmente compartilhado nas organizações (IPE, 2003). A capacidade de articular conhecimento não deve ser equiparada com a disponibilidade para uso por outros na organização.

O conhecimento é intimamente ligado com as ocupações e egos das pessoas e não flui facilmente através da organização (DAVENPORT *et al*, 1998). As pessoas não compartilham conhecimento sem uma forte motivação pessoal (STENMARK, 2001). Os fatores motivacionais podem ser divididos em internos e externos. Fatores internos incluem o poder percebido relacionado ao conhecimento e a reciprocidade que resulta do compartilhamento. Fatores externos incluem o relacionamento com o recebedor e as recompensas por compartilhar (IPE, 2003). Na prática, o compartilhamento não pode ser forçado, mas encorajado e facilitado.

O conhecimento deve ser visto como mais do que apenas explícito ou tácito. Independente se o conhecimento é tácito ou explícito, o valor atribuído a ele tem também um impacto significante em como e se os indivíduos o compartilham (IPE, 2003). O

conhecimento cada vez mais é percebido como sendo comercialmente valioso e sua posse é reconhecida tanto por indivíduos quanto pela organização (BROWN; WOODLAND, 1999; JARVENPAA; STAPLES, 2001). Quando os indivíduos percebem o conhecimento que eles possuem como um bem valioso, o compartilhamento do conhecimento se torna um processo mediado por decisões sobre o que compartilhar, quando compartilhar e com quem compartilhar (ANDREWS; DELAHAYE, 2000).

A grande importância dada ao conhecimento nas organizações e o valor atribuído aos indivíduos que possuem o tipo certo de conhecimento levam a criação da noção de poder em torno do conhecimento (IPE, 2003). Se os indivíduos percebem que o poder vem do conhecimento que eles possuem, é mais provável que eles acumulem o conhecimento ao invés de compartilhá-lo (DAVENPORT, 1997; GUPTA; GOVINDARAJAN, 2000).

A reciprocidade, ou o dar e receber conhecimento, pode facilitar o compartilhamento se os indivíduos virem que o valor que eles ganham depende do quanto eles compartilham seu próprio conhecimento com os outros (HENDRIKS, 1999).

Um dos fatores externos que influenciam a motivação de compartilhar conhecimento é o relacionamento entre o emissário e o receptor (IPE, 2003). O que aponta para questões de status e poder entre quem compartilha e quem recebe. Tais questões influenciam se e como o conhecimento é. Indivíduos com menos status e poder tendem a direcionar o conhecimento para aqueles com mais poder e status, enquanto indivíduos com mais poder e status tendem a direcionar o conhecimento mais para os seus pares do que para aqueles com menos status e poder (HUBER, 1982).

Recompensas e penalidades para indivíduos que compartilham e não compartilham conhecimento também influenciam o processo de compartilhamento de conhecimento (IPE, 2003). A probabilidade dos indivíduos compartilharem conhecimento com outros membros da organização está positivamente relacionada com as recompensas e negativamente relacionada com as penalidades (O'REILLY; PONDY, 1980).

Como o compartilhamento do conhecimento não ocorre sem custos para os seus participantes, a expectativa de que os benefícios superarão estes custos é um importante determinante do compartilhamento de conhecimento. (BOCK; LEE; ZMUD, 2005). O compartilhamento é mais provável de ocorrer quando os indivíduos percebem que os incentivos excedem os custos (KELLY; THIBAUT, 1998). A falta de recompensas suficientes para compensar os custos do compartilhamento é uma barreira comum para o compartilhamento (CONSTANT *et al*, 1994).

Segurança psicológica está relacionada com um "senso de um empregado ser capaz de mostrar-se e empregar-se sem o medo de consequências negativas para sua imagem, status ou carreira" (KAHN, 1990, p. 708 apud SIEMSEN et al, 2009). A falta de segurança psicológica em um relacionamento é uma barreira para o compartilhamento de conhecimento.

Teoricamente, a segurança psicológica deveria aumentar a motivação para compartilhar, entretanto, a segurança psicológica não deve ser vista como um motivador por si só. Mais do que isso, ela reduz a relutância de compartilhar, levando as pessoas a falar sem medo de humilhação ou incerteza da recepção quando elas não estão confiantes sobre o conhecimento que pretendem compartilhar (SIEMSEN et al, 2009).

Quando a frequência de comunicação entre um empregado e seus companheiros aumenta, também aumenta a motivação para compartilhar conhecimento com eles, pois aumenta a segurança psicológica na perspectiva do empregado (SIEMSEN et al, 2009).

Os líderes podem influenciar se os membros do grupo se veem de forma competitiva ou cooperativa e o conforto dentro do grupo (EDMONDSON, 1999 *apud* SIEMSEM et al, 2009). Quando os líderes são benevolentes, consideram falhas como oportunidade de aprendizado e tratam os membros do grupo com respeito à segurança psicológica dos membros do grupo aumenta (SIEMSEN et al, 2009).

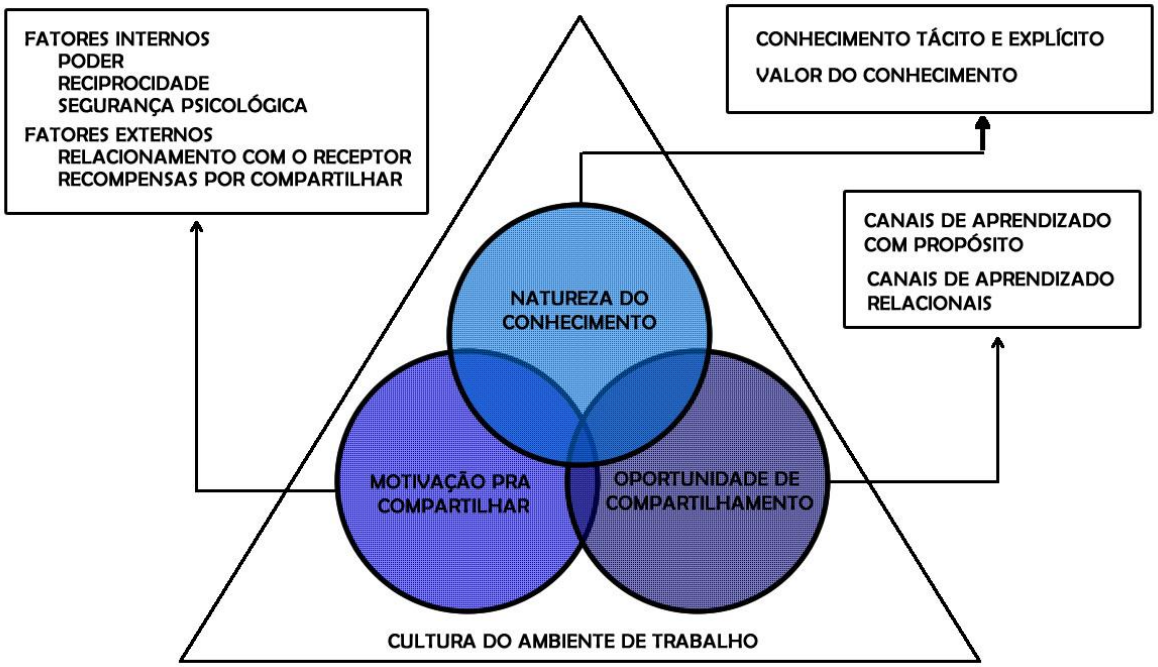
Os fatores citados até agora são importantes para entender o compartilhamento do conhecimento entre os indivíduos, mas todos eles são influenciados pela cultura do ambiente de trabalho (IPE, 2003). A cultura organizacional tem sido bastante reconhecida como a maior barreira para a criação, compartilhamento e uso efetivo do conhecimento (DE LONG; FAHEY, 2000).

A cultura foi definida por Schein (1985) como um padrão de pressupostos básicos desenvolvidos por um grupo que trabalha desenvolvendo soluções para problemas diários. Quando esses pressupostos funcionam bem, eles são repassados aos novos membros. Dessa forma, a cultura se reflete nos valores, normas e práticas da organização, onde os valores se manifestam em normas que moldam práticas específicas (DE LONG; FAHEY, 2000).

Delong e Fahey (2000) identificaram alguns aspectos da cultura organizacional que influenciam o compartilhamento de conhecimento: a cultura forma pressupostos sobre quais conhecimentos são importantes; ela controla o relacionamento entre os níveis de conhecimento (organizacional, de grupo e individual); e ela cria o contexto para a interação social. Além disso, a cultura determina as normas relativas à distribuição de conhecimento entre a organização e os indivíduos (STAPLES; JARVENPAA, 2001).

A relação entre os fatores pode ser visualizada na Figura 1. Segundo Ipe (2003), a natureza do conhecimento, a motivação para compartilhar, as oportunidades para compartilhamento e a cultura do ambiente de trabalho são todos conectados e influenciam uns aos outros de forma não linear. De acordo com o modelo, os três primeiros fatores estão inseridos dentro da cultura do ambiente de trabalho.

Figura 1- Fatores que influenciam o compartilhamento de conhecimento entre indivíduos nas organizações



Fonte: Adaptado de Ipe (2003).

3.8 ORGANIZAÇÃO DO CONHECIMENTO

Choo (2006), ao tentar responder a questão "Como as organizações usam a informação?" reúne em seu livro os principais meios pelos quais as organizações usam a informação de forma estratégica. Ele introduz uma estrutura conceitual no qual os processos são interligados e podem ser administrados de forma a criar a organização do conhecimento.

Assim, Choo (2006) ressalta que a criação e uso da informação tem papel decisivo em três arenas distintas. Na primeira, a organização usa a informação pra dar sentido às mudanças do ambiente externo. Essa criação de significado constrói para os membros da organização um consenso sobre o que é a organização e sobre o que ela está fazendo. Na

segunda arena, a organização cria, organiza e processa a informação de modo a gerar novos conhecimentos por meio de aprendizado. E na terceira arena, as organizações buscam e avaliam informações para tomar decisões importantes.

Para Choo (2006), as três arenas, embora sejam tratadas como processos independentes, são processos interligados e a forma com que elas se comunicam mutuamente demonstra uma visão holística do uso da informação. Ainda segundo Choo (2006), as três arenas podem ser vistas como três camadas concêntricas, onde cada camada interna produz o fluxo de informação para as camadas subjacentes. A informação flui do ambiente exterior sendo progressivamente assimilada para permitir a ação da organização, conforme apresentado na Figura 2.

Figura 2 – A Organização do Conhecimento

Fonte: Adaptado de Choo (2006).

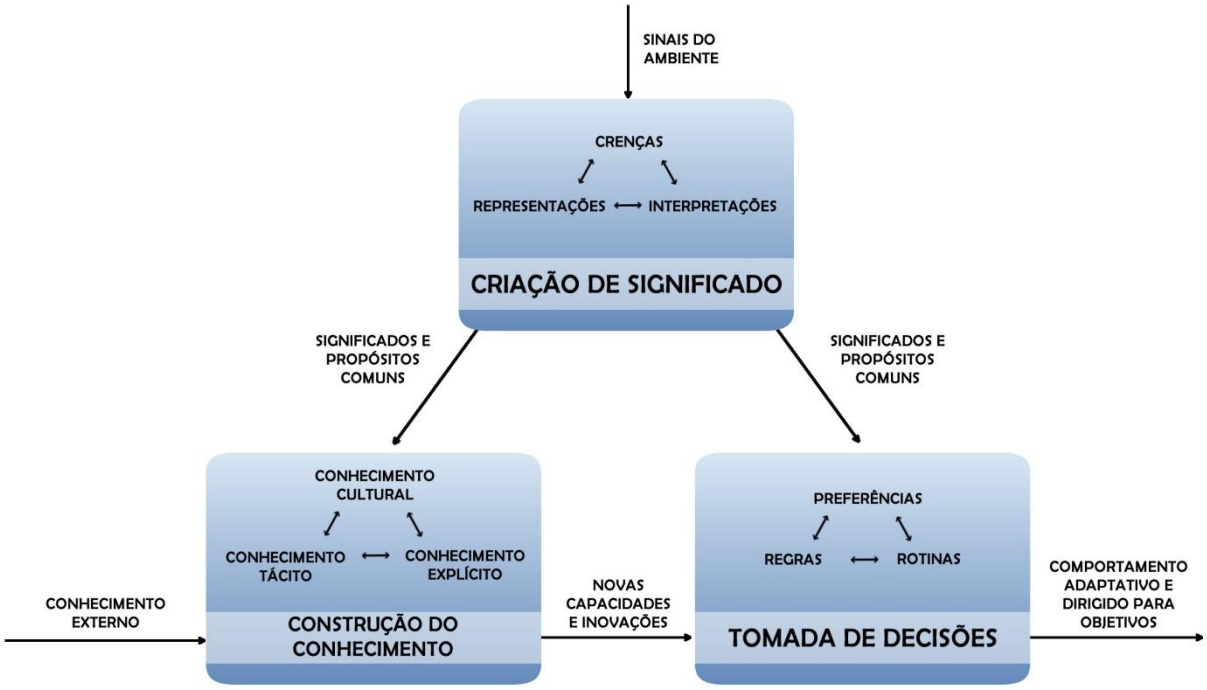
3.9 O CICLO DO CONHECIMENTO

O modelo de organização do conhecimento é uma descrição estática, assim, Choo (2006) propõe uma configuração chamada por ele de ciclo de conhecimento, através da qual é possível entender as dinâmicas da organização do conhecimento. Ele afirma que o ciclo do

conhecimento ilustra claramente como a criação de significado, a construção do conhecimento e a tomada de decisões funcionam juntas, permitindo o aprendizado e a adaptação das organizações.

No ciclo do conhecimento, existe um fluxo de informação entre a criação de significado, a construção do conhecimento e a tomada de decisões, de modo que a informação usada em um modo oferece aos outros modos mais recursos e um contexto mais elaborado. Tal ciclo é ilustrado na Figura 3.

Figura 3 – O Ciclo do Conhecimento



Fonte: Choo (2006).

De acordo com Choo (2006) é através da criação de significados que os membros das organizações representam e negociam crenças e interpretações a fim de criar significados e objetivos comuns. Esses significados e objetivos comuns servem para especificar as questões que os membros consideram importantes para o bem estar da organização e que são relevantes, além de ajudar a definir uma identidade organizacional coletiva. Portanto, os membros da organização utilizam os significados e propósitos comuns para acessar o que é importante e apropriado, além de reduzir a ambiguidade e incerteza da informação.

A organização busca explorar suas especializações e desenvolver novas capacidades caminhando em direção de seus objetivos. Esse movimento pode ser impedido

por lacunas no conhecimento necessário para fazer a transição entre significado e ação. Ao perceber essas lacunas a organização inicia a busca e criação desse conhecimento. Seja individual ou coletivamente, os membros da organização constroem novos conhecimentos ao converter, compartilhar e sintetizar seu conhecimento tácito e explícito, assim com relacioná-lo com o conhecimento proveniente de fora da organização. O resultado da construção do conhecimento são novas capacidades e inovações que melhoram capacidades existentes e criam novas. Os benefícios dessas inovações são avaliados de acordo com as regras e preferências no processo de tomada de decisão.

Ainda de acordo com Choo (2006), os significados e propósitos comuns, como também os novos conhecimentos e capacidades, convergem para a tomada de decisão em uma atividade que leva à seleção e ao início da ação. A tomada de decisão é estruturada pelas premissas, regras e rotinas que são selecionadas de acordo com os significados e identidades comuns. Os novos conhecimentos e inovações fornecem novas alternativas que expandem o repertório de ações. As regras e rotinas especificam os critérios racionais para a avaliação das alternativas e as condições objetivas para perceber situações que podem precisar de novas regras.

Um resumo sobre os detalhes de todos os modos de uso da informação organizacional é apresentado no Quadro 1. Nele são apresentados a ideia central, os resultados e os principais conceitos de cada um dos modos.

Quadro 1 – Modos de uso da informação organizacional

Modo	**Ideia Central**	**Resultados**	**Principais conceitos**
Criação de significado	Organização interpretativa: Mudança ambiental → Dar sentido aos dados ambíguos por meio de interpretações. A informação é interpretada.	Ambientes interpretados e interpretações partilhadas para criar significado.	Interpretação, seleção e retenção.
Construção do conhecimento	Organização aprendiz: Conhecimento existente → Criar novos conhecimentos por meio da conversão e partilha dos conhecimentos. A informação é convertida.	Novos conhecimentos explícitos e tácitos para a inovação.	Conhecimento tácito. Conhecimento explícito. Conversão do conhecimento.
Tomada de decisões	Organização racional: Problema → Buscar e	Decisões levam a um comportamento racional e	Racionalidade limitada. Premissas decisórias.

	selecionar alternativas de acordo com os objetivos e preferências. A informação é analisada.	orientado para objetivos.	Regras e rotinas.

Fonte: Choo (2006).

3.9.1 Criação de significado

As empresas estão percebendo que a sua sobrevivência no mercado depende da forma como elas dão sentido ou influenciam o ambiente e de renovar constantemente o significado dos ambientes que mudam dinamicamente (CHOO, 2006). A adaptação é um desafio para as empresas, pois elas devem perceber e criar significados. Perceber as mensagens importantes do ambiente não é uma tarefa fácil, pois a empresa está imersa em um ambiente complexo e imprevisível. A tarefa de criar significado fica mais difícil quando a empresa quer interferir no ambiente.

Weick (1995 *apud* CHOO, 2006) reúne várias discussões sobre a criação de significado e apresenta sete propriedades identificadas como parte da criação de significado. Segundo estas propriedades, a criação de significado é um processo: fundado na construção de uma identidade, retrospectivo, interpretativo de ambientes perceptíveis, social, contínuo, focado em e por pistas extraídas e governado mais pela plausibilidade do que pela precisão.

A criação do significado é fundada na construção de uma identidade, ela começa quando o indivíduo não consegue confirmar sua identidade. O ambiente funciona como um ambiente onde as pessoas se projetam, ao mesmo tempo em que tentam moldar o ambiente, as pessoas reagem a ele.

Ela é retrospectiva porque trabalha com fatos que já ocorreram. No momento do fato, o olhar do indivíduo sobre o mesmo afetará a maneira como ele interpretará esse fato com o seu olhar retrospectivo. O indivíduo depende da memória, que pode ser precisa ou não, assim os valores e prioridades servem para esclarecer o que é importante e significativo na experiência vivida.

Na criação do significado as pessoas em uma organização criam parte do ambiente que as cerca, este é o processo que Weick (1995 *apud* CHOO, 2006) chama de interpretação. Uma maneira de interpretar é dividir as experiências e agrupá-las, assim é dado valor cognitivo a dos fatos e objetos, criando matéria-prima para a criação de significado.

Toda criação de significado é feita em grupos, por isso ela é social (CHOO, 2006). Mesmo quando sozinhas, as pessoas criam significado considerando a reação das outras pessoas que serão afetadas e que são significativas. Além disso, a criação de significado é contínua, é um fluxo de projetos e atividades que constituem a vida da empresa e que nunca terminam.

De acordo com o Weick (1995 *apud* CHOO, 2006) pistas extraídas são "estruturas simples, conhecidas, sementes a partir das quais as pessoas dão um sentido mais amplo ao que está ocorrendo", a partir delas as ideias podem ser conectadas em redes de significados. A interpretação de pistas depende do contexto organizacional. De acordo com Choo (2006), a criação de significados é mais governada pela plausibilidade do que pela precisão devido às pessoas se comportarem pragmaticamente quando criam significado.

Choo (2006) resume a criação de significado como um processo social contínuo em que os indivíduos observam fatos passados, recortam pedaços da experiência e selecionam determinados pontos de referência para tecer redes de significados. O principal desafio da criação de significado é diminuir ou eliminar a ambiguidade e criar significados comuns para que a organização possa agir coletivamente.

As organizações dão significados a seu ambiente, sua identidade e suas ações através de processos. Tudo começa com o processo de interpretação, nele os indivíduos recortam a experiência, selecionam significados e retêm interpretações racionais (CHOO, 2006). Tal processo é executado através de sequências interligadas de interpretação → seleção → retenção (ISR). Weick (1995 *apud* CHOO, 2006) adiciona o processo, chamado por ele de mudança ecológica, precedendo a interpretação. Esta sequência de processos é ilustrada na figura 4. Enquanto que no Quadro 2 são resumidos os principais pontos dos processos que formam a criação de significado.

Quadro 2 – O Método de criação de significados

	Origens	**Processos**	**Resultados**
Interpretação	Dados brutos do ambiente	Isolar os dados brutos Agir ou criar aspectos do ambiente que serão acompanhados	Dados ambíguos como matéria prima para a criação de significado
Seleção	Dados ambíguos oriundos do processo de interpretação Interpretações que já funcionaram antes	Selecionar e criar significados ou interpretações para os dados ambíguos	Ambiente interpretado ou significativo

Retenção	Ambiente interpretado no processo de seleção	Armazenar o ambiente interpretado como produto da criação de significado bem-sucedida	Interpretações para serem usadas em futuras sequências ISR

Fonte: Choo (2006).

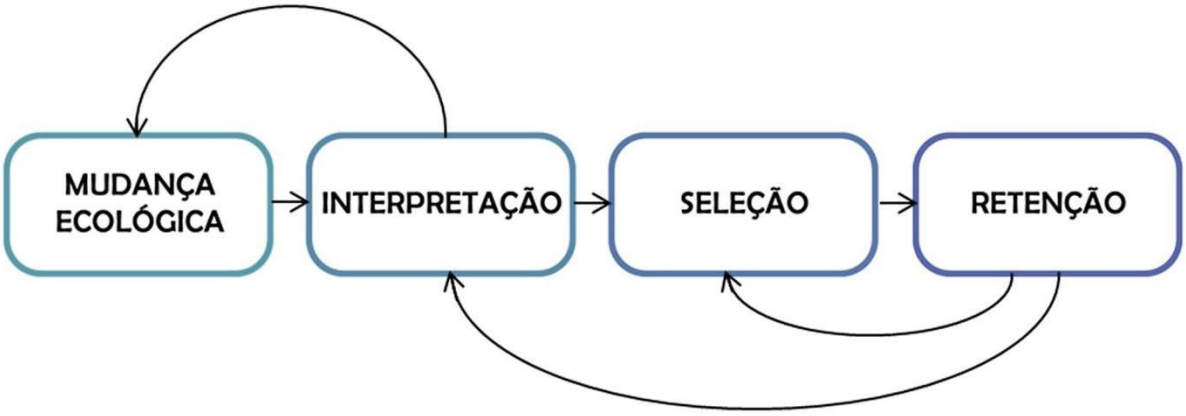
O processo de interpretação começa com alguma mudança no ambiente da organização que provoca variações nos fluxos de experiência e afeta os participantes da empresa (CHOO, 2006), são os dados brutos sobre essas mudanças que constituem a origem do processo. Algumas dessas mudanças são separadas para serem observadas mais atentamente, isso é feito isolando e rotulando pedaços de experiências e criando aspectos do ambiente a serem observados. O resultado da interpretação é uma série de dados ambíguos que serão matéria-prima para outros processos de criação de significado.

Choo (2006) descreve a seleção como o processo onde são escolhidos os significados que poderão ser atribuídos aos dados ambíguos provenientes da interpretação. Esses possíveis significados vêm dos sentidos e interpretações passados que se mostraram razoáveis. As interpretações passadas são usadas em comparação aos dados atuais, de forma a revelar configurações plausíveis (CHOO, 2006). Como resultado do processo de seleção, tem-se um ambiente interpretado que é significativo por oferecer uma explicação causal ao que está acontecendo.

Os ambientes interpretados e significativos, resultado de uma criação de significado bem sucedida são armazenados no processo de retenção para que possam ser acessados no futuro como possíveis significados a serem atribuídos a novas situações ambíguas (CHOO, 2006).

Na sequência interpretação-seleção-retenção, a interpretação pode ser comparada com dizer ou fazer, a seleção com ver e a retenção com pensar ou lembrar. Estes três processos estão interligados em ciclos, onde o *feedback* entre os mesmos amplifica ou atenua as mudanças observadas no ambiente externo e acelera ou restringe as informações que influenciam a escolha de interpretações e a retenção de significados (CHOO, 2006).

Figura 4 – Processos de criação de significado numa organização



Fonte: Choo (2006)

3.9.2 Construção do conhecimento

Para Choo (2006), a base da criação do conhecimento em uma organização é a conversão do conhecimento tácito em conhecimento explícito e vice-versa. De acordo com o modelo de Nonaka e Takeuchi (1995 *apud* CHOO, 2006) existem quatro maneiras de criar conhecimento organizacional através da interação e conversão entre conhecimento tácito e explícito: socialização, exteriorização, combinação e internalização. Conforme ilustrado na Figura 5.

Figura 5 – Processos de conversão do conhecimento organizacional

Fonte: Nonaka (1994).

Através do processo de socialização, o conhecimento tácito é criado através do compartilhamento de experiências. Choo (2006) exemplifica o processo de socialização através da forma como o aprendiz aprende o ofício com seu mestre através da observação, da imitação e da prática, da mesma maneira os empregados de uma organização aprendem novas capacidades por meio do treinamento.

A exteriorização é o processo pelo qual o conhecimento tácito se torna explícito. Isso se dá pelo compartilhamento de metáforas, analogias, modelos ou histórias, o que acontece em diálogos ou reflexões coletivas e também em documentos e relatórios.

O processo de combinação se caracteriza pela criação de conhecimento explícito reunindo conhecimentos explícitos provenientes de diversas fontes. Os indivíduos nas organizações combinam os seus conhecimentos explícitos através da troca de documentos, como relatórios e memorandos, essa combinação pode ser apoiada pelo uso de TIC.

O conhecimento explícito é absorvido como conhecimento tácito através do processo de internalização. Choo (2006) destaca que para que isso aconteça, é necessário que o conhecimento explícito seja vivido ou experimentado pelo indivíduo, seja pessoalmente, através da realização de uma atividade, ou seja, indiretamente através de simulações ou histórias.

Choo (2006), explica que essas maneiras de converter o conhecimento se retroalimentam. Tudo começa com um indivíduo que tem um *insight* para realizar suas tarefas, esse *know-how* tácito é compartilhado com os outros através da socialização. Em uma organização pode existir conhecimento explícito construído por um ou mais pessoas ou grupos, e esses conhecimentos podem ser combinados gerando novos conhecimentos, que serão posteriormente internalizados.

Sendo criadoras de conhecimento, as empresas se tornam repositórios de capacidades que resultaram dos conhecimentos dos indivíduos. Assim, para Choo (2006), administrar o conhecimento organizacional é administrar as capacidades da organização.

3.9.3 Tomada de decisões

As regras especificam os papéis, métodos e normas que estruturam a tomada de decisão nas organizações. Ao seguir rotinas e procedimentos, certas visões de mundo são institucionalizadas, hábitos de aquisição e transmissão de informações são formados e valores e normas são estabelecidos de forma que podem influenciar a maneira como a organização lida com a escolha e com a incerteza (CHOO, 2006). O que se espera dessa combinação de cultura, comunicação e consenso é que as decisões sejam mais eficientes e que o comportamento decisório seja mais racional.

No fluxo do ciclo do conhecimento, depois que os significados foram criados e o conhecimento necessário para agir foi construído, a organização precisa agora escolher entre as opções disponíveis. Em um mundo ideal, uma escolha racional exigiria que todas as alternativas disponíveis fossem analisadas, mas no mundo real, esses requisitos de avaliação de informações não são factíveis.

Simon (1957 *apud* CHOO, 2006) sugere que a capacidade da organização tomar decisões é limitada pelo princípio da racionalidade limitada, que diz que a mente humana é limitada para resolver questões complexas. Ele identifica três categorias de limites: capacidade mental, hábitos e reflexos; conhecimento e informação que possui; valores e conceitos.

Devido a essa racionalidade limitada, os indivíduos ao tomar decisões comportam-se de duas maneiras diferentes. Primeiro, eles procuram um curso de ação que seja satisfatório ou suficientemente bom, em vez de buscarem o melhor. Essa busca pela alternativa satisfatória reflete ai treinamento, experiência e os objetivos dos participantes. Em

segundo, as organizações e atores organizacionais simplificam o processo decisório, eles aplicam regras e rotinas de modo a reduzir a certeza e ambiguidade (CHOO, 2006).

A racionalidade exige um olhar para o futuro, pois as consequências das ações estão no futuro. Assim, a racionalidade se baseia em previsões, e portanto, baseiam-se em crenças e expectativas sobre a probabilidade de fatos incertos. Tversky e Kahneman (1974 *apud* CHOO, 2006) identificam três grupos de princípios que são usados para avaliar a probabilidade e prever valores: representatividade, disponibilidade e ancoragem e ajuste.

O princípio da representatividade é utilizado quando as pessoas avaliam a probabilidade de um fato ou objeto pertencer a uma determinada categoria, essa avaliação é feita através da comparação de um fato ou objeto com estereótipos que são representativos em uma categoria. A representatividade pode captar o aprendizado de uma experiência passada, mas pode levar a erros sistêmicos caso o tamanho da amostra não seja considerado, ou se a adequação da solução do passado aos problemas do passado não forem analisadas.

De acordo com Choo (2006), as pessoas utilizam o princípio da disponibilidade para avaliar a probabilidade ou plausibilidade de determinado desenvolvimento. Elas se lembram de casos conhecidos e recentes, o que pode ajudar economizando tempo na busca de precedentes relevantes, mas pode levar a desvios, caso a pessoa lembre apenas de casos ou informações fáceis de guardar.

Enquanto que a ancoragem e ajuste são utilizados quando as pessoas tentam calcular o valor de algo, elas partem de um valor inicial (âncora) e fazem ajustes até chegar a uma estimativa final. Ela pode ser útil para fornecer estimativas razoáveis, mas pode levar a erros se o ajuste for insuficiente ou se desconsiderar interdependências relevantes.

3.10 EMPRESAS DE BASE TECNOLÓGICA

A conceituação do que são empresas de base tecnológica (EBT) não é um problema trivial. Segundo Cortês *et al*. (2005), elas podem ser definidas, de forma sintética, como empresas que realizam esforços tecnológicos significativos e concentram suas operações na fabricação de “novos” produtos.

O grande patrimônio dessas empresas está no conhecimento técnico e administrativo que os seus colaboradores possuem e que permite o desenvolvimento contínuo dos projetos e produtos (VALERIO; VALERIO, 2006). Uma característica das empresas de base tecnológica é que o seu quadro de mão-de-obra é formado por profissionais de alto nível de qualificação, como mestres e doutores.

Em seu estudo sobre as pequenas e médias empresas, Machado et al. (2001. p. 7) se utiliza do conceito proposto pelo OTA - Office of Technology Assesment – do congresso americano, aliado a definição de pequenas e médias empresas do SEBRAE pra desenvolver uma definição de pequenas e médias empresas de base tecnológica:

> Micro e pequenas empresas de base tecnológica são empresas industriais com menos de 100 empregados, ou empresas de serviço com menos de 50 empregados, que estão comprometidas com o projeto, desenvolvimento e produção de novos produtos e/ou processos, caracterizando-se, ainda, pela aplicação sistemática de conhecimento técnico-científico. Estas empresas usam tecnologias inovadoras, têm uma alta proporção de gastos com P&D, empregam uma alta proporção de pessoal técnico-científico e de engenharia e servem a mercados pequenos e específicos.

Para as empresas de base tecnológica, o conhecimento é de suma importância. A geração e aproveitamento de conhecimento em setores de alta tecnologia demanda que o conhecimento seja continuamente reabastecido (LANE; LUBATKIN, 1998). Além disso, aquisição e exploração do conhecimento são processos predominantemente sociais (KOGUT; ZANDER, 1992), dessa forma o capital social pode ser crítico para o sucesso em longo prazo das empresas de base tecnológica (YLI-RENKO; AUTIO; SAPIENZA, 2001).

Novas empresas de base tecnológica são elementos chave para o desenvolvimento econômico regional e nacional (MALECKI, 1991 *apud* WESTHEAD, 1997), elas contribuem direta e indiretamente para a criação de empregos, são fontes de inovação tecnológica e podem estimular a competitividade (WESTHEAD, 1997). As empresas de base tecnológica desempenham um papel de destaque na inovação nas áreas de produtos e serviços, com inovações que tem o potencial de formarem a base econômica no futuro (STOREY; TETHER, 1998).

A exploração de uma invenção ou inovação tecnológica implica em substanciais riscos tecnológicos (STOREY; TETHER, 1998). Geralmente, novas empresas baseadas em tecnologia desenvolvem produtos ou serviços que se encontram em fases menos maduras de desenvolvimento, o que implica grande incerteza quanto a trajetória dessas tecnologias, mas, que por outro lado, representa um grande potencial para a expansão do mercado (MACHADO *et al.*, 2001).

A conceituação encontrada na literatura sobre empresas de base tecnológica é bastante diversificada, quando não divergente (CORTÊS *et al.,* 2005). Autores como Ferro e Torkomian (1988 *apud* CORTÊS *et al.,* 2005) sugerem que o conceito deva ser aplicado a empresas que dispõem de competência rara ou exclusiva em termos de produtos ou processos, viáveis comercialmente, que incorporam grau elevado de conhecimento científico. Já

Stefanuto (1993), propõe considerar como EBTs as empresas que em cada país se situem na fronteira tecnológica do seu setor.

Assim, uma definição proveitosa deve ser capaz de distinguir adequadamente empresas que tenham a tecnologia como atividade crítica para seu desempenho competitivo daquelas que têm a capacitação tecnológica como papel de menor relevância (CORTÊS *et al*, 2005).

Tal conceito deve ser capaz deve ser capaz de discriminar a ênfase da dimensão da tecnologia de produto da dimensão da tecnologia de processos (CORTÊS *et al*, 2005). Assim, Cortês *et al. (*2005) atentam que com tais definições se distinguiriam empresas cujas capacidades produtivas estejam empenhadas no desenvolvimento de produtos novos daquelas empresas que se empenham em modernizar suas bases produtivas, mas que suas operações se concentram em bens e serviços há muito existentes no mercado.

Ainda segundo Cortês *et al. (*2005), é necessário distinguir as EBT das empresas que atuam com produtos inovadores para os seus mercados, mas não realizam esforços tecnológicos, como exemplo, temos empresas que se dedicam apenas a montagem de artigos eletrônicos padronizados, sendo baseadas em licenciamento de tecnologia.

4 MÉTODO

Neste capítulo, apresenta-se os procedimentos metodológicos utilizados na realização da pesquisa. Aborda-se aspectos que são relacionados com a caracterização da pesquisa, o contexto e os indivíduos a serem investigados. Também se define o instrumento utilizado na coleta dos dados e os procedimentos adotados na análise e interpretação dos dados obtidos.

A caracterização da pesquisa se dá através dos pressupostos descritos por Burrell e Morgan (1979), segundo tais pressupostos a presente pesquisa se identifica com o paradigma interpretativista. Como tal, sua posição ontológica é nominalista, em relação à epistemologia é antipositivista, a natureza humana é voluntarista e sua abordagem metodológica é ideográfica.

Quanto ao seu objetivo, a presente pesquisa se caracteriza como exploratória. Assim como define Sampieri et al (1991), os estudos exploratórios são realizados normalmente quando o objetivo é investigar um problema pouco estudado, servindo para aumentar o grau de familiaridade com fenômenos relativamente desconhecidos. Tais estudos exploratórios são comuns nas investigações de comportamento, principalmente quando há pouca informação.

Para atingir os objetivos da presente pesquisa adotou-se a abordagem qualitativa. Pesquisas qualitativas estão interessadas em como as pessoas interpretam suas experiências, como elas constroem seus mundos e qual o significado que elas atribuem a suas experiências (MERRIAM, 2009). Na tentativa de definir algo complexo como a pesquisa qualitativa, Merriam (2009) identifica quatro características que são chaves para o entendimento da natureza da pesquisa qualitativa: o foco é no processo, no entendimento e no significado; o pesquisador é o instrumento primário de coleta de dados e análise; o processo é indutivo; e o produto é ricamente descritivo.

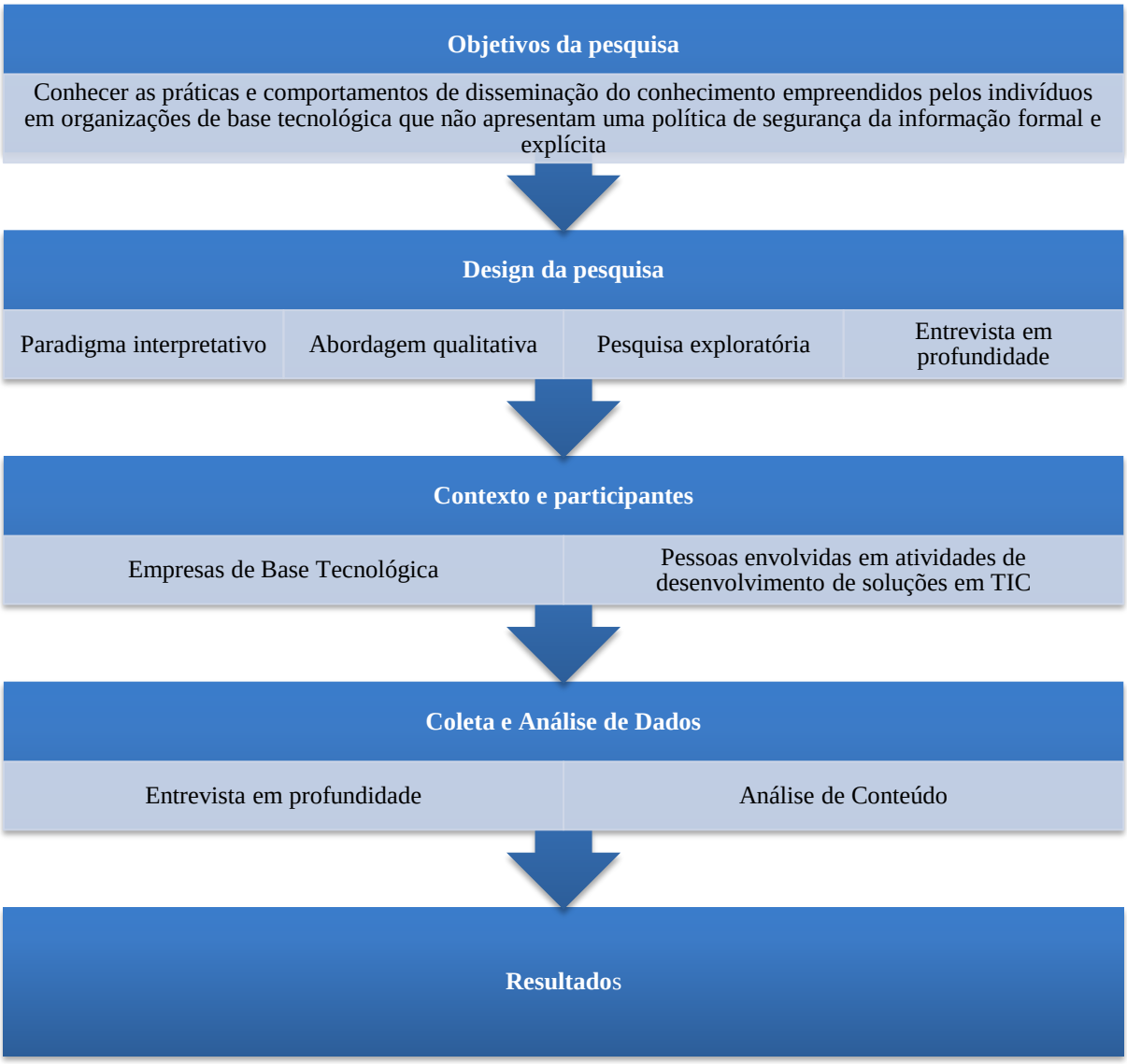
Ainda caracterizando a presente pesquisa, de acordo com os tipos de pesquisa qualitativa de Merriam (2009), ela é classificada como pesquisa qualitativa básica. Diferente dos outros tipos de pesquisa qualitativa, que têm uma dimensão adicional, a pesquisa qualitativa básica tenta entender qual o sentido que as pessoas dão para suas vidas e experiências. Os dados são coletados através de entrevistas, observações ou análises de documentos. A análise dos dados envolve a identificação de padrões recorrentes que caracterizam os dados. Os resultados são esses temas ou padrões identificados e a

interpretação geral será o entendimento do pesquisador sobre o entendimento do participante sobre o fenômeno de interesse.

4.1 TRAJETÓRIA DA PESQUISA

Para melhor visualização e entendimento, as etapas da realização da pesquisa estão resumidas no gráfico a seguir.

Figura 6 – Trajetória da Pesquisa



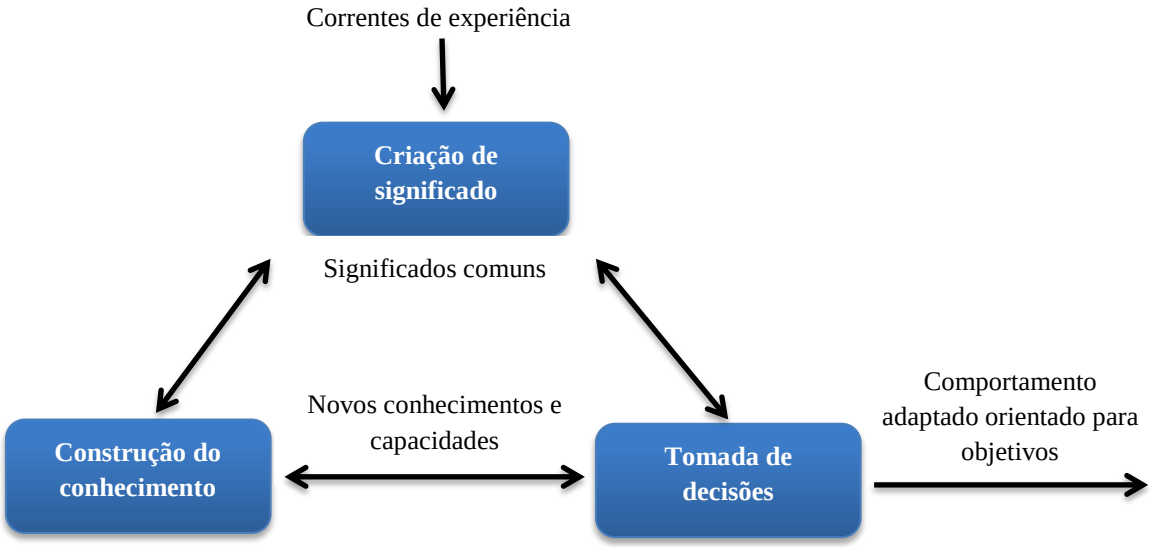
Fonte: Elaboração própria, 2013.

4.2 MODELO TEÓRICO

Para responder a questão de pesquisa e atender o objetivo principal desta pesquisa utilizou-se como aporte teórico o ciclo do conhecimento proposto por Choo (2006) e uma adaptação do modelo de fatores que influenciam o compartilhamento proposto por Ipe (2003). O ciclo do conhecimento representa o fluxo de informação entre três modos de uso da informação do qual emerge o conhecimento organizacional. Os processos que compõem estes modos de uso e suas propriedades caracterizam o uso da informação dentro das organizações. Enquanto que o modelo de fatores representa os principais influenciadores do compartilhamento de conhecimento e as relações que eles tem entre si.

De acordo com o ciclo proposto por Choo (2006), no primeiro modo, a criação de significado, uma mudança no ambiente faz com que os membros da organização negociem crenças e interpretações de forma a criar significado e objetivos comuns. No segundo modo, a construção do conhecimento, os membros da organização se deparam com uma lacuna de conhecimento, que pode ser a necessidade de uma capacidade para resolver determinado problema, durante este modo o conhecimento é construído, principalmente através do compartilhamento de conhecimento, o que o torna crucial para as aspirações deste presente trabalho. No terceiro modo, a tomada de decisões, os indivíduos escolhem, dentre as opções, qual a estratégia que tomarão para agir. Os três modos se retroalimentam, de modo que os resultados de um modo servem como insumos para a execução dos outros. O ciclo do conhecimento com os seus modos e processos é detalhado em seções anteriores. Uma representação gráfica simplificada do mesmo é apresentada na Figura 7.

Figura 7 – O Ciclo do Conhecimento Simplificado



Fonte: Choo (2006).

Deste modelo teórico retiraram-se as categorias que guiarão a análise do conteúdo, as mesmas são divididas de acordo com os modos do ciclo do conhecimento, propostos por Choo (2006). Orientado pelo objetivo da pesquisa, as categorias tratam de comportamentos desempenhados pelos indivíduos. Assim, as categorias identificadas na teoria são apresentadas no Quadro 3.

Quadro 3 – Categorias comportamentais

Modo	Categoria
Criação de Significado	Mudança no ambiente Interpretação Seleção Retenção
Construção do conhecimento	Socialização Exteriorização Combinação Internalização
Tomada de decisão	Representatividade Disponibilidade Ancoragem e ajustes

Fonte: Elaboração própria, 2013.

Ainda como fonte de categorias utilizadas na análise, tem-se o modelo de fatores que influenciam o compartilhamento proposto por Ipe (2003), ao qual se adicionou uma categoria, que fornece as categorias expostas no Quadro 4.

Quadro 4- Categorias motivacionais

Fator		**Categoria**
Natureza do conhecimento		Conhecimento Tácito e Explícito
		Valor do conhecimento
Oportunidade de compartilhamento		Canais de aprendizado com propósito
		Canais de aprendizado relacionais
Motivação para compartilhar	Fatores Internos	Poder
		Reciprocidade
		Segurança Psicológica
	Fatores Externos	Relacionamento com o receptor
		Recompensas por compartilhar
Cultura do Ambiente de trabalho		Cultura do ambiente de trabalho

Fonte: Elaboração própria, 2013.

Desta forma, as categorias de comportamentais e as categorias motivacionais foram utilizadas para classificar trechos das entrevistas e serviram como insumos para a análise de conteúdo.

4.3 CONTEXTO DA PESQUISA

Assim como em qualquer abordagem de pesquisa, deve ser definida a unidade de pesquisa a ser usada, o que geralmente inclui grupos, indivíduos, organizações ou comunidades (GRAY, 2012). Esta pesquisa tem como unidade de análise indivíduos que trabalham com o desenvolvimento de soluções em TIC, nas funções comumente conhecidas como analista de sistema ou desenvolvedor de *software*, tais indivíduos foram escolhidos por que são os responsáveis, na prática, pelo desenvolvimento das soluções. São eles que possuem o conhecimento necessário e buscam outros conhecimentos quando não os possuem. Como é característico das pesquisas qualitativas, a amostragem se deu por forma não-probabilística por conveniência de acessibilidade.

O contexto da pesquisa são as empresas de base tecnológica de pequeno e médio porte, mais precisamente aquelas que têm como atividade fim o desenvolvimento de soluções

em TIC e que fazem parte do Farol Digital. O Farol Digital é um projeto do SEBRAE-PB, em parceria com outras instituições ligadas ao setor, que visa promover o desenvolvimento e o fortalecimento do setor de TIC nas cidades de João Pessoa, Campina Grande, Patos e Cajazeiras. No momento desta pesquisa, o projeto conta com a participação de 172 empresas.

A escolha das empresas do Farol Digital se deu pelo fato delas se caracterizarem como pequenas e médias empresas de base tecnológica de acordo com a classificação de Machado *et al* (2001). Assim como determina a classificação, elas são empresas de serviço com menos de 50 empregados, que tem forte característica de uso de conhecimento técnico-científico e desenvolvem tecnologias inovadoras para um mercado pequeno e específico.

As 172 empresas participantes do Farol Digital são de especialidades diferentes e para a presente pesquisa foram escolhidas as empresas que tem como finalidade o desenvolvimento de *software*. Seguindo o critério de conveniência de acessibilidade, buscou-se por empresas sediadas nas cidades de João Pessoa e Campina Grande, embora sejam cidades geograficamente próximas, também são as cidades com maior relevância, dentro do estado da Paraíba, quando se trata de empresas de desenvolvimento de *software*.

A dificuldade inicial na escolha das empresas esteve nas informações referentes às empresas contidas no *site* do Farol Digital, como endereço físico, telefone e e-mail de contato, além de *site,* o que dificultou o contato com as mesmas. Superadas essas dificuldades, foram selecionadas as empresas mais reconhecidas no mercado de TIC e as empresas que demonstravam em seus websites um portfólio de produtos e clientes reconhecidamente importantes.

A fase inicial de contato com as empresas se deu através do e-mail de contato comercial fornecido pelas mesmas no site do Farol Digital ou no próprio site da empresa. Foi enviado um e-mail apresentando a pesquisa e solicitando participação para 16 empresas de João Pessoa e cinco empresas de Campina Grande. A proporção de empresas escolhidas por cidade reflete a proporção de empresas participantes do Farol Digital em cada cidade. Deste contato inicial, apenas uma empresa, de João Pessoa, retornou o contato e as entrevistas foram prontamente agendadas.

A segunda fase de contato com as empresas se deu de forma presencial. Durante a visita às empresas selecionadas, seis empresas não foram localizadas, não sendo identificado se elas não existem mais ou apenas mudaram de endereço, em uma empresa não foi possível contato com o responsável, uma empresa estava realizando reformas em sua sede e sete empresas solicitaram um contato formal por e-mail para que fosse realizado o agendamento das entrevistas. Devido a distância, as empresas de Campina Grande foram contatadas por

ligação telefônica, sendo possível falar com o responsável em apenas duas empresas. Uma empresa se dispôs a participar, enquanto que a outra empresa, devido a problemas internos, não poderia participar da pesquisa.

Assim, na terceira fase de contato com as empresas foram enviados os e-mails para os endereços fornecidos na segunda fase. Dos sete e-mails enviados, apenas três empresas responderam, sendo duas confirmando as entrevistas e uma dizendo que não seria possível a realização. Às outras empresas que não responderam foi enviado o mesmo e-mail por mais duas vezes, num intervalo de uma semana, os quais foram novamente ignorados. Depois de encerradas as tentativas de contato com as empresas, as entrevistas agendadas foram realizadas.

4.4 COLETA DE DADOS

Seguindo as características da pesquisa qualitativa, a coleta de dados foi realizada através de entrevistas qualitativas. DeMarrais (2004 *apud* Merriam, 2009) define uma entrevista como um processo no qual um pesquisador e um participante se envolvem em uma conversa focada em relações relacionadas ao tema da pesquisa. Na entrevista, o objeto de investigação são as experiências, ideias, valores e estruturas simbólicas do entrevistado (GODOI, MATTOS, 2006).

A entrevista proporciona ao pesquisador recolher dados através da linguagem do sujeito, permitindo conhecer como ocorreram os fenômenos. Permitindo, inclusive, que o pesquisador consiga perceber como eventos passados foram interpretados. Foi utilizada a modalidade de entrevista semiestruturada, a qual tem como característica questionamentos básicos que são apoiados em teorias e hipóteses relacionadas ao tema da pesquisa (MANZINI, 2004).

As questões do roteiro de entrevista foram elaboradas de forma a abordar todas as variáveis que compõem o ciclo do conhecimento e o modelo de fatores que influenciam o compartilhamento de conhecimento buscando identificar a presença ou não delas dentro do contexto das pequenas e médias empresas de base tecnológica desenvolvedoras de soluções em TIC. Também foram incluídas perguntas a respeito do perfil sócio-profissional do entrevistado para ajudar a compreender o fenômeno.

As entrevistas se deram da seguinte forma: foram entrevistados dois indivíduos em cada empresa, sendo os mesmos indicados pelas próprias empresas, as entrevistas eram gravadas em áudio, os entrevistados respondiam oralmente às perguntas feitas pelo

pesquisador, os entrevistados não tiveram contato prévio com as questões, as perguntas eram feitas de acordo com o roteiro de entrevista, mas adaptações foram necessárias no momento da entrevista, como mudança na ordem de algumas questões, necessidade de explicar a pergunta, exclusão de algumas perguntas que foram respondidas antecipadamente em perguntas anteriores, dentre outras necessidades percebidas pelo entrevistador.

Após a realização das entrevistas em cada uma das empresas, foi realizada a transcrição das mesmas e uma avaliação do roteiro de entrevista. Assim, após a primeira entrevista, percebeu-se a necessidade de se adicionar mais categorias no modelo conceitual, criando mais perguntas e desta forma obter mais detalhes dos entrevistados. Tendo em vista essa necessidade, uma adição no modelo conceitual permitiu a criação de uma segunda versão do roteiro de entrevista. Depois da segunda entrevista, foi realizada a avaliação do roteiro de entrevista e o mesmo sofreu algumas alterações, onde algumas perguntas foram justapostas de forma a dar mais coerência. No final, tivemos três versões diferentes do roteiro de entrevista, os quais podem ser vistos nos anexos.

O ciclo de coleta de dados foi finalizado, levando mais tempo e com bem menos entrevistas do que o esperado e planejado inicialmente. Muitos fatores contribuíram para esse atraso e para a falta de participação das empresas, dentre os principais podemos citar a época em que as empresas foram procuradas, sendo os meses de dezembro e janeiro caracterizados por muitos feriados e por ser o período de férias de muitos funcionários. Também contribuiu para a dificuldade em conseguir as entrevistas a falta de consciência das empresas sobre a importância das pesquisas científicas.

4.5 CARACTERIZAÇÃO DA AMOSTRA

Para melhor compreender o fenômeno que está sendo investigado, o roteiro de entrevista continha questões que abordavam características do entrevistado, como idade, curso, instituição e ano de formação e tempo de serviço na empresa. Assim, a amostra de participantes na pesquisa é composta de oito pessoas, sendo apenas uma mulher. A média de idade é de 26 anos, a média de tempo desde que concluíram a formação é de 4,5 anos e o tempo médio trabalhando na empresa atual é de 3,4 anos.

Todos eles trabalham desempenhando funções semelhantes, mas devido à falta de regulamentação da área há uma variedade de denominações para tal função. Eles se denominaram como analistas de sistemas, programadores ou desenvolvedores de *software*. A falta de clareza na definição da função também é reflexo da cultura da área de

desenvolvimento de *software*, onde o indivíduo que desempenha essa função participa de todo o processo do desenvolvimento, sendo exigido um conhecimento amplo por parte dos mesmos.

Outra característica relevante dos entrevistados, pois ajuda a entender o nível de conhecimento em segurança da informação que eles possuem, é o curso de formação. Três deles são formados no IFPB, no curso de Tecnologia em Sistemas para Internet, três deles são formados em Ciência da Computação, um no UNIPÊ e dois na UFCG. Além deles, um tem formação de nível técnico, também no IFPB, e outro é graduado em Gestão de Tecnologia da Informação na UNISEB de Ribeirão Preto – SP, o qual também é um curso de tecnólogo. A diferença entre os cursos de bacharelado e os de tecnologia está na amplitude dos conhecimentos, enquanto que um curso de tecnologia tem duração de três anos e tem como objetivo ser mais focado no mercado de trabalho, o curso de bacharelado tem duração de 4 anos e visa dar uma visão mais ampla de conhecimentos.

O tempo médio de formação é de 4,5 anos devido à contribuição de dois entrevistados que apresentam mais de nove anos de experiência, pois cinco dos entrevistados tem menos de três anos de formação. Não pude verificar se profissionais recém-formados são uma tendência dentre as empresas ou se houve um fator subjetivo na escolha dos mesmos, pois, conforme dito anteriormente, os entrevistados foram escolhidos pelas empresas. O tempo de formação também influencia no tempo do vínculo dos indivíduos com as empresas.

4.6 ANÁLISE DOS DADOS

Um dos aspectos essenciais da pesquisa qualitativa é a variedade de abordagens e métodos (FLICK, 2009) e não existe entre eles um que seja o mais adequado, a escolha é feita de acordo com as necessidades da pesquisa. A análise qualitativa de dados é uma das poucas facetas em que existe uma maneira preferencial de realização, para Merriam (2009) esta maneira é através da realização da análise durante a coleta de dados. Segundo ela, o resultado da pesquisa depende do que é encontrado nos dados, assim a realização da análise durante a coleta dos dados pode evitar que os dados coletados sejam sem foco, repetitivos e superficiais. Ainda segundo Merriam (2009), o objetivo da análise qualitativa é dar sentido aos dados, interpretando o que os indivíduos disseram, é a resposta da questão de pesquisa.

Assim como qualquer tipo de texto, os dados resultantes das entrevistas podem dizer mais do que os autores imaginam. A análise de conteúdo é apenas um método de análise de texto. Ela é uma técnica que produz inferências de um texto dentro de seu contexto social

de forma objetiva (BAUER; GASKELL, 2008). Apesar de sua característica qualitativa, a análise de conteúdo também apresenta aspectos quantitativos em sua natureza, onde a sua unidade de medida é a frequência e a variedade de mensagens, mas o seu foco é na comunicação do significado (MERRIAM, 2009). Embora uma grande parte das análises clássicas do conteúdo culmine em descrições numéricas, tem aumentado a atenção dada a "tipos", "distinções" e "qualidades" no texto antes de qualquer quantificação (BAUER; GASKELL, 2008). Desta forma, a análise de conteúdo será a abordagem de análise utilizada nesta pesquisa.

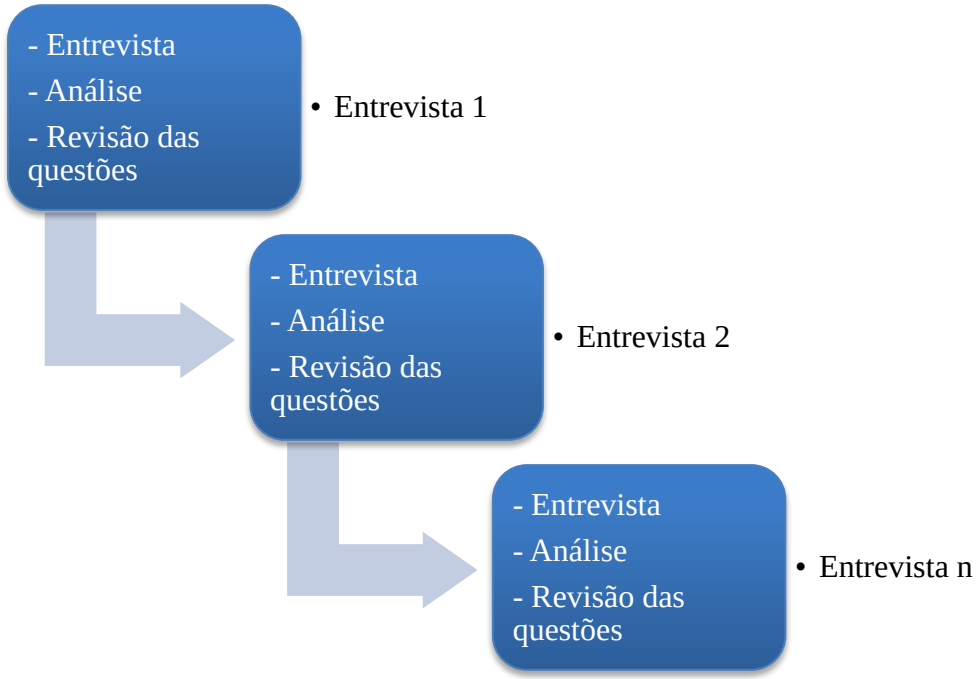
As etapas da análise de conteúdo adotadas nesta pesquisa são explicitadas na Figura 8. A transcrição das entrevistas é a atividade que fornece a amostra de texto a ser analisada. A atividade de codificação e categorização identifica os trechos do texto relevantes de acordo com a teoria que fundamenta a pesquisa, esses trechos são identificados e classificados de acordo com as categorias pré-definidas. Por fim, na atividade de interpretação são produzidas inferências sobre os trechos categorizados e sobre as descrições numéricas resultantes dessa codificação.

Figura 8 – Passos da análise de conteúdo

Fonte: Elaboração própria, 2013

Assim como sugerido por Merriam (2009), a análise dos dados ocorreu concomitantemente com a realização das entrevistas, permitindo verificar se os dados coletados estavam sendo adequados à realização da pesquisa. As atividades foram realizadas conforme Figura 9.

Figura 9 – Processo de coleta de dados



Fonte: Elaboração própria, 2013.

A realização da análise de conteúdo foi apoiada pelo uso do *software* Atlas.TI[3]. O mesmo se caracteriza por ser uma ferramenta que contribui para o aperfeiçoamento das pesquisas que desempenham a análise de dados qualitativos (WALTER; BACH, 2009). A utilização deste *software* dá mais credibilidade ao trabalho, pois possui dentre as suas finalidades a busca, categorização, organização e registro de interpretações (GODOI, MATOS, 2006).

Através do Atlas.TI, os arquivos com as entrevistas transcritas foram utilizados, trechos considerados importantes foram classificados de acordo com as categorias do modelo teórico. O Atlas.TI foi importante no suporte a classificação e na consulta aos trechos classificados. Tal facilidade em classificar e consultar os trechos permitiu que a análise fosse realizada com mais dinamismo e precisão.

[3] O *software* pode ser obtido no *site*: www.atlasti.com

5 RESULTADOS

Para melhor entender as percepções dos entrevistados acerca do compartilhamento de conhecimento foram incluídas no roteiro de entrevista, questões que buscavam mensurar o entendimento dos indivíduos sobre segurança da informação e política de segurança da informação, além de saber se os mesmos tinham consciência do seu papel e responsabilidade na garantia da segurança dentro da organização.

Ao dizer o que entendiam por segurança da informação, a grande maioria dos entrevistados demonstrou conhecer superficialmente o tema e abordavam, implicitamente, as propriedades de confidencialidade e acessibilidade. De maneira geral, eles definem a segurança da informação relacionando-a com a proteção da informação e com a garantia de que ela só esteja disponível para a pessoa adequada. Assim como podemos verificar nas citações a seguir.

> “Manter os dados importantes, que não sejam fáceis de acesso para as pessoas que não tem permissão pra isso”.
>
> Entrevistado2, Empresa1.

> “Segurança da informação é realmente garantir que a informação, o dado que esteja sendo tratado não chegue a pessoas não autorizadas no objetivo do produto”.
>
> Entrevistado1, Empresa2.

> “É a informação estar nas mãos corretas, na hora certa, qualquer coisa que passe disso é falta de segurança”.
>
> Entrevistado2, Empresa3.

> “Segurança da informação é não deixar que invasores não [*sic*] tenham acesso a informações confidenciais”.
>
> Entrevistado2, Empresa4.

Ao serem consultados a respeito do seu conhecimento sobre política de segurança todos eles apresentaram maior conhecimento sobre o tema, talvez pelo fato do termo “política” ser algo mais genérico e disseminado. Para eles, a política de segurança da

informação seria a formalização das regras e normas definidas pela empresa que os funcionários devem seguir para garantir a segurança da informação. Um erro no entendimento dos indivíduos estava na amplitude da política, acreditando que a política se resume apenas a tecnologia, pois, assim como afirmou Ifinedo (2012), soluções tecnológicas raramente são suficientes para prover total proteção dos recursos organizacionais de TI.

> "Acredito que sejam normas, que sejam regras que devem ser seguidas por todos integrantes em uma empresa".
>
> Entrevistado2, Empresa3.

> "Seria um conjunto de boas práticas de como a segurança da informação vai ser bem executada na empresa".
>
> Entrevistado1, Empresa4.

> "Seria uma série de regras que você teria que adotar ... criadas para que você não cometa falhas".
>
> Entrevistado1, Empresa2.

> "Política de segurança da informação são as normas que vão se adotar para todos os usuários. Que na minha opinião tem que ser bem prático e deixar bem claro".
>
> Entrevistado1, Empresa1.

Nas respostas às questões nas quais se indagava se eles tinham consciência do seu papel e de suas responsabilidades na garantia da segurança, alguns assumiram que não tinham consciência, enquanto alguns disseram ter consciência, mas não apresentaram confiança quanto a isso, outros responderam fugindo do tema. O que realmente pôde ser observado foi que a consciência que os indivíduos têm diz respeito à importância que a informação possui e que há necessidade de protegê-la, embora o conhecimento sobre como proteger seja limitado, se resumindo a alguns procedimentos básicos e a seguir as determinações da gerência. Como alertaram Von Solms e Von Solms (2004), se os indivíduos não possuem conhecimento sobre segurança da informação, eles não têm consciência dos riscos que eles correm nem dos danos que eles podem causar.

> “Não, não tenho”.
>
> Entrevistado1, Empresa2

> “Tenho consciência. Até por que a gente lida com informações que precisam de um pouco mais de segurança. Então, isto está colocado já para o pessoal, mas sem tanta formalidade”.
>
> Entrevistado2, Empresa3.

> “Não é uma questão formal, mas cada um tem consciência do que tem que fazer, do que não pode e também da importância que tem a informação”.
>
> Entrevistado2, Empresa3.

> “A gente não tem uma cartilha definida. Mas todo mundo é consciente do que você faz é registrado, todo mundo sabe que tem que fazer backups, e a questão do segredo do negócio, sabemos que não podemos expor nada que diz respeito apenas a empresa”.
>
> Entrevistado1, Empresa4.

O entendimento que os indivíduos possuem sobre segurança da informação, política de segurança da informação e nível de conscientização sobre papéis e responsabilidades na segurança da informação tem impacto direto no compartilhamento de conhecimento e nas práticas adotadas por eles para garantir a segurança da informação, conforme veremos no decorrer desta análise.

Percebemos que há um déficit de conhecimento sobre segurança da informação entre os indivíduos participantes desta pesquisa. Isto vem desde as suas formações, pois nos cursos superiores na área de TIC não existem disciplinas específicas de segurança da informação, e continua quando os indivíduos ingressam no mercado de trabalho, pois não há uma preocupação das empresas em melhorar o conhecimento dos seus funcionários.

> “Meu conhecimento sobre segurança da informação não é tão profundo.”
>
> Entrevistado2, Empresa3.

> “Meu conhecimento em segurança é muito pouco”.
>
> Entrevistado2, Empresa4.

> “Não é muito comum, o pessoal do desenvolvimento compartilha mais conhecimento sobre regra de negócios”.
>
> Entrevistado2, Empresa2.

> “Não é uma área que eu conheço muito, nem na graduação, nem nas empresas a gente vê muito, então eu nunca tive tanto contato”.
>
> Entrevistado1, Empresa2.

Consequente à falta de conhecimento sobre segurança da informação, os indivíduos entrevistados, em sua grande maioria, demonstraram também desconhecer normas e guias de melhores práticas em segurança da informação. Enquanto os que disseram conhecer, reconheceram ter conhecimento apenas superficial. Assim como está explícito no seu nome, esses guias são coletâneas das melhores práticas que se mostraram eficazes em outras empresas ajudando outras empresas a decidirem quais as estratégias de segurança da informação adotar. Porém, Hone e Eloff (2002) lembram que esses guias descrevem os processos e controles necessários para implementar com sucesso um política de segurança da informação, mas eles não dizem como um política deve ser.

> “Eu já li algumas coisas sobre isso”.
>
> Entrevistado1, Empresa2.

> “A 27001, se não me engano, é o gerenciamento da segurança da informação”.
>
> Entrevistado2, Empresa2.

> “Muito pouco. Já andei lendo sobre as normas de segurança definidas pela ISO”.
>
> Entrevistado2, Empresa2.

> “Eu tenho uma certa base, mas não me aprofundei muito”.
>
> Entrevistado1, Empresa4.

5.1 CICLO DO CONHECIMENTO

Para entendermos o modo como o compartilhamento de conhecimento auxilia os indivíduos na falta de uma política formal de segurança da informação, fazemos uso do modelo do ciclo do conhecimento proposto por Choo (2003), o qual é composto por três modos divididos em 11 categorias, as quais foram utilizadas para classificar trechos das entrevistas.

5.1.1 Criação de significado

O primeiro modo, *criação de significado*, é o modo onde os indivíduos percebem a necessidade de novos conhecimentos. Geralmente, isto ocorre quando há mudanças no ambiente. Um evento citado por todos eles foi um apagão de energia elétrica ocorrido em 26 de outubro de 2012 que atingiu todo o nordeste e causou perda de dados nos servidores das empresas. Mas, como eles mesmos interpretaram, isso não afetou o trabalho deles, pois as mudanças não eram de sua responsabilidade. Este episódio serviu para fortalecer a percepção de que as empresas não estão completamente preparadas para garantir a segurança de sua informação.

As mudanças que foram citadas pelos indivíduos entrevistados e que segundo eles tinham impacto sobre eles foram as que mudanças que diziam respeito aos novos projetos nos quais eles trabalhariam. Os novos projetos possuem suas próprias especificações e clientes, o que representam necessidades diferentes, as quais não necessariamente são novas necessidades de segurança.

> “Quando eu estava de férias, teve um apagão no nordeste inteiro e teve algumas informações que não foram perdidas, mas deu trabalho para recuperar”.
>
> Entrevistado2, Empresa2.

> “Questão de roubo ou invasão, eu desconheço. A questão de perda de informação, no último apagão de energia elétrica que teve, algumas informações que estavam em HDs foram perdidas”.
>
> Entrevistado2, Empresa3.

> “Basicamente, o que aconteceu foi perder dados de um backup”.
>
> Entrevistado1, Empresa4.

> “A gente tem uma reunião onde define as metas da empresa, o que deve ser entregue em forma de história, a história é o que o cliente precisa que a gente vai implementar. Então, a gente como analista de sistemas estima essas histórias, o esforço que vai ser e depois a gente cria uma especificação breve e nela a gente vai prever o que vai ter e após isso a gente começa a fazer a implementação”.
>
> Entrevistado2, Empresa2.

5.1.2 Construção do conhecimento

O segundo modo do ciclo do conhecimento é chamado de *construção do conhecimento*, é nesse modo que o indivíduo adquire novos conhecimentos, inclusive de fontes diferentes, e os internaliza. Além de compartilhar o conhecimento que possui. O conhecimento que trafega nessa fase do ciclo do conhecimento varia entre tácito e explícito, conforme visto no capítulo anterior.

5.1.2.1 Socialização

De acordo com os entrevistados, os indivíduos nas empresas, incluindo eles mesmos, costumam compartilhar o conhecimento que possuem. Embora o compartilhamento de conhecimento seja intenso entre os indivíduos, isso não ocorre quando o conhecimento a ser compartilhado é relativo à segurança da informação.

> “Não é muito comum, o pessoal do desenvolvimento compartilha mais conhecimento sobre regra de negócios. Mas, uma vez ou outra, acontece questões sobre política de segurança”.
>
> Entrevistado2, Empresa2.

> “O objetivo de compartilhar o conhecimento aqui é pra que todos possam melhorar e finalizar as tarefas ou o produto e isso pra empresa é o que importa na verdade.”
>
> Entrevistado1, Empresa2.

5.1.2.2 Combinação

Ainda dentro do modo de construção do conhecimento, a categoria *combinação*, na qual o indivíduo agrega vários conhecimentos para formar um, esteve presente no momento em que eles citavam as fontes de conhecimento utilizadas por eles além da consulta a outros indivíduos. Podemos assim, constatar que o compartilhamento de informação diretamente com outros indivíduos é a principal fonte de conhecimento, mas que eles costumam complementar com consultas a internet, através de fóruns e sites especializados, além de consultar as documentações originais das ferramentas e tecnologias que eles utilizam.

> “A gente dá preferência a buscar informação nas documentações oficiais”.
>
> Entrevistado2, Empresa3.

> “Pegar conhecimentos pequenos que vão se somando e formando o quebra-cabeça formando um conhecimento geral para a organização, que cresce e melhora a qualidade dos seus produtos e serviços”.
>
> Entrevistado1, Empresa4.

> “Sites mais reconhecidos, pessoas especializadas. As ferramentas de busca ajudam a encontrar tudo”.
>
> Entrevistado1, Empresa4.

5.1.2.3 Internalização

Dentro da área de desenvolvimento de soluções em TIC, a realização de testes é comum, de forma a validar o que foi desenvolvido e buscar por eventuais erros. Esta é a forma mais comum identificada de *internalização* do conhecimento. Em todas as empresas os

indivíduos afirmaram realizar testes, em algumas delas existindo pessoas responsáveis exclusivamente por isso.

> “Temos ambiente de teste, o ambiente de produção fica no cliente, mas o projeto que eu trabalho fica aqui. Tem a equipe de teste, de homologação, de produção e o pessoal que tem algumas bases pra fazer teste e de espelho também”.
>
> Entrevistado1, Empresa2.

> “Antes de fazer uma implantação, a gente realiza testes. Existe uma equipe de testes”.
>
> Entrevistado2, Empresa2.

> “O teste que a gente utiliza é mais o teste de aceitação”.
>
> Entrevistado2, Empresa3.

5.1.3 Tomada de decisão

O modo final do ciclo do conhecimento é a *tomada de decisão.* Neste momento os indivíduos já tiveram acesso ao conhecimento necessário para resolver o seu problema. Eles podem ter acessado mais de uma solução possível, de forma que devem decidir qual conhecimento utilizarão e se vão utilizar esse conhecimento na solução do seu problema.

São vários os critérios utilizados na avaliação das soluções disponíveis, dentre os citados pelos entrevistados estão o próprio conhecimento possuído previamente, a consulta a outras pessoas, o desempenho e a plausibilidade da solução.

> “A primeira coisa que influencia são os meus conhecimentos, o que eu achar... O que eu acho a melhor solução. Depois disso eu vou conversar com outras pessoas eu vou buscar em outras fontes qual seria a melhor solução”.
>
> Entrevistado1, Empresa2.

> “Primeiramente, questão de desempenho. Segundo, opiniões de pessoas mais experientes”.
>
> Entrevistado2, Empresa2.

> “A facilidade. Não adianta resolver o problema, mas ser complicado de aplicar”**.**
>
> Entrevistado1, Empresa4.

As expectativas em relação às soluções escolhidas são baseadas principalmente na eficácia. Poucos esperam que a solução seja a melhor possível e apenas um indivíduo se preocupou com o impacto da solução no cliente.

> ‘Que ela funcione. Que ela resolva o meu problema”.
>
> Entrevistado1, Empresa1.

> “Espera que no final o cliente fique satisfeito com a solução”.
>
> Entrevistado2, Empresa2.

> “Ela tem que resolver o problema da melhor forma”.
>
> Entrevistado2, Empresa3.

> “Espera que resolva o problema”.
>
> Entrevistado2, Empresa4.

5.2 FATORES QUE INFLUENCIAM O COMPARTILHAMENTO

Vários fatores influenciam o compartilhamento de conhecimento, assim, para melhor entendermos o compartilhamento entre os indivíduos usamos como suporte o modelo de fatores que influenciam o compartilhamento proposto por Ipe (2003), o qual foi detalhado anteriormente. A esse modelo adicionamos mais uma categoria, conforme detalhado em capítulos anteriores.

5.2.1 Cultura do ambiente de trabalho

Segundo este modelo, o principal fator, no qual todos os outros estão inseridos, é a cultura do ambiente de trabalho. Segundo Ipe (2003), a cultura influencia os outros fatores de várias formas, ela dita a valoração do conhecimento, os tipos de relacionamentos, as recompensas, encoraja o compartilhamento e define as oportunidades, tanto informais e formais, de compartilhamento. Segundo Cormack (2001), uma cultura de segurança é desejável em qualquer organização, mas essa cultura não se desenvolve por si só.

Ao serem perguntados como era o ambiente na empresa e se gostavam de trabalhar lá, todos deram respostas positivas. Eles ressaltaram o tamanho da equipe como um ponto forte, pois com a equipe pequena e espacialmente próxima, as oportunidades de socialização eram maiores e as pessoas se tornam mais facilmente próximas.

> "O clima é como se fosse uma família. Tem as regras de uma empresa, mas todo mundo tem o respeito com o outro. É respeitada a hierarquia, mas é um clima bem natural."
>
> Entrevistado1, Empresa4.

> "Bem interessante, agradável, descontraído, o pessoal é interessante de trabalhar, é um espaço bem flexível".
>
> Entrevistado2, Empresa3

> "O clima é bem legal. Eu já trabalhei em empresas maiores, onde eu senti que o entrosamento era bem menor. Quanto menor a empresa, maior o entrosamento. Acho que essa é uma empresa de porte médio, onde o pessoal se comunica bastante, inclusive entre setores".
>
> Entrevistado1, Empresa2

> "A empresa tem um ambiente pequeno, e a socialização ajuda a compartilhar a informação".
>
> Entrevistado1, Empresa1

5.2.2 Motivação para compartilhar

A cultura do ambiente exerce forte influência nos outros fatores, as categorias que formam o fator de *motivação para compartilhar* tiveram grande presença nas respostas dos indivíduos. Sendo a categoria *relacionamento com o receptor* a mais frequente. O relacionamento com o receptor tem bastante influência da cultura do ambiente, como afirmado anteriormente, o fato de haver poucos indivíduos nas empresas facilita o fortalecimento dos laços entre eles. O que corrobora com o que dizem Bock *et al* (2005), segundo eles, os indivíduos que acreditam que a sua relação com os outros indivíduos melhoraria com o compartilhar são mais prováveis de compartilhar seu conhecimento.

5.2.2.1 Relacionamento com o receptor

A influência do relacionamento com o receptor fica bem clara quando os indivíduos respondem a pergunta sobre quais eram as pessoas que eles procuravam quando precisavam obter algum conhecimento, nas respostas, majoritariamente, eram apontados os companheiros de equipe de trabalho. Embora eles se limitassem a consultar pessoas dentro da própria organização, a preferência era por consultar aqueles que têm maior reputação.

> “As pessoas que tem mais conhecimento, até porque aqui é quase todo mundo próximo, pois a equipe é pequena”.
>
> Entrevistado1, Empresa3

> “Eu procuro as pessoas de melhor conhecimento”.
>
> Entrevistado2, Empresa3

> “O pessoal mais experiente da organização”.
>
> Entrevistado1, Empresa4

É nesta categoria que um novo elemento passa a ter preponderância, os líderes, chefes ou gerentes, ou seja, uma pessoa no nível hierárquico superior ao dos entrevistados. Os líderes se mostraram a maior fonte de conhecimento relativo à segurança da informação, como os indivíduos não possuíam confiança nem conhecimento suficiente nesta área para que

pudessem compartilhar, os gerentes, pela responsabilidade do cargo, assumiam todas as decisões.

> “Geralmente, os líderes do projeto. Geralmente, ele tem essa função mesmo, de orientar os desenvolvedores, de dizer qual a tecnologia vai ser usada, o que vai ser implementado”.
>
> Entrevistado1, Empresa2

> “Normalmente o que a gente faz é consultar os superiores que estão a mais tempo na empresa e sabem como funciona tudo”.
>
> Entrevistado1, Empresa2.

5.2.2.2 Recompensas por compartilhar

Ainda dentro dos fatores motivadores, a categoria *recompensas por compartilhar* tem destaque por sua frequência. Ao serem perguntados sobre o que os motivaria a compartilhar conhecimento, foi quase unânime como resposta a preocupação com o crescimento da área, segundo eles o compartilhamento contribui para que o conhecimento chegue a mais pessoas. Outra recompensa por compartilhar é que a empresa vai se beneficiar, pois, para eles, se a empresa prosperar, eles também prosperarão.

> “O desenvolvimento melhor do produto, até do trabalho”.
>
> Entrevistado1, Empresa3.

> “Eu estou contribuindo para resolver os problemas da empresa. Tanto com meu aprendizado, quanto o da outra pessoa, eu estou contribuindo para o crescimento da empresa”.
>
> Entrevistado2, Empresa3.

> “O crescimento da organização, pois se a organização cresce eu cresço junto. Melhorando a circulação de informação dentro da empresa, automaticamente está melhorando pra mim”.
>
> Entrevistado1, Empresa4.

Ainda no âmbito da categoria de recompensas, verificamos que para os indivíduos a imagem perante os seus companheiros de trabalho e perante a gerência é muito importante. Para eles, a reputação por ser uma boa fonte de conhecimento é a principal vantagem em compartilhar conhecimentos. Diferente do que afirmou Ipe (2003), que diz que ao perceberem o poder em torno da posse do conhecimento os indivíduos tendem a retê-lo, os indivíduos da entrevista fizeram uso do *poder* relacionado ao conhecimento através da reputação adquirida por quem compartilha, ou seja, quem compartilha mais e melhor é mais bem visto e tem recompensas por isso. Esta situação também ajuda a explicar porque conhecimento sobre segurança da informação é pouco compartilhado, visto que eles conhecem pouco sobre o assunto, uma informação incorreta repassada poderia comprometer sua imagem perante os outros.

> "A impressão que a pessoa tem perante as outras passa muita coisa. Mesmo ela não sabendo nada, mas se ela passa a impressão de que sabe, que ajuda, o povo vê diferente. Infelizmente, o ser humano é assim. Mas, se ela passa o conhecimento e realmente ela tem conteúdo, com certeza ela vai ter uma boa impressão".
>
> Entrevistado1, Empresa2.

> "É importante também, querendo ou não é importante, porque é o resultado do seu trabalho, se você realmente está fazendo um trabalho bem feito, a gente busca sempre isso, se a gente está sendo reconhecido por ter conhecimento, isso é interessante, por que a gente passa a ser bem visto na empresa e as pessoas podem se espelhar em você pra seguir o mesmo caminho ela sempre vai pensar dessa forma".
>
> Entrevistado2, Empresa2.

> "Ele é recompensado na questão da reputação, além de estar aprendendo".
>
> Entrevistado2, Empresa3.

> "A pessoa fica mais bem vista. Se ele contribui para a empresa crescer".

Entrevistado2, Empresa4.

5.2.2.3 Reciprocidade

Ao responder se compartilhariam informações mesmo que os outros não compartilhassem, todos eles disseram que compartilhariam mesmo assim. Embora, ao citar os motivos que o fazem compartilhar, a possibilidade de receber conhecimento posteriormente vindo dos seus colegas se mostrou um fator de motivação bastante importante. Há esse pequeno conflito nos discursos, quando se trata da categoria *reciprocidade*.

> "Sim, com certeza. Até com pessoas que você não tem contato, assim, se surgir uma dúvida, que ele precise entrar em contato com você, aí vai surgir a oportunidade pra você conhecer mais alguém e ter bons relacionamentos dentro da empresa. Até, um dia, eu posso precisar deles pra outra coisa também. Pra um compartilhamento de informação e com certeza ele vai me passar".
>
> Entrevistado1, Empresa2.

> "Sem dúvida. Com certeza. Compartilharia independentemente da atitude deles"**.**
>
> Entrevistado1, Empresa2.

5.2.2.4 Segurança psicológica

Outro fator importante na motivação do compartilhamento é a *segurança psicológica*, ela significa que o indivíduo tem confiança no seu conhecimento, que ele sabe que a recepção por parte dos indivíduos vai ser positiva e que tem consciência que a empresa, na figura dos gerentes, apoia e valoriza o compartilhamento de conhecimento. Tudo isso torna o ambiente propício ao compartilhamento.

Assim como foi previamente relatado, percebeu-se nas entrevistas que o clima da organização contribui bastante para o compartilhamento de informação, visto que as equipes são bem unidas e receptivas ao compartilhamento e há apoio da gerência, que incentiva o compartilhamento entre os indivíduos, mas o pouco conhecimento sobre segurança da informação continua sendo um entrave também na segurança psicológica.

> “O ambiente é muito tranquilo, o pessoal é muito amigo. A gente não tem um padrão muito rígido, muito engessado. A coisa é mais informal, mais amizade. Mantendo sempre a responsabilidade com os trabalhos que a gente tem”.
>
> Entrevistado1, Empresa1.

> “Gosto, o ambiente é legal, todos quando eu cheguei aqui a gente não sabia muito sistema, pois o sistema é grande, mas as pessoas daqui ajudam você, tem descontração”.
>
> Entrevistado2, Empresa2.

> “Sim, encoraja sim. E como aqui temos desenvolvedores muito experientes e alguns poucos experientes, a empresa organiza aulas para os experientes passarem o seu conhecimento”.
>
> Entrevistado2, Empresa3.

> “O clima é como se fosse uma família. Tem as regras de uma empresa, mas todo mundo tem o respeito com o outro. É respeitada a hierarquia, mas é um clima bem natural”.
>
> Entrevistado1, Empresa4.

> “Mais pelo fato de permitir o diálogo, não tem nenhuma ferramenta para isso”.
>
> Entrevistado1, Empresa3.

5.2.3 Oportunidade de compartilhamento

A *oportunidade de compartilhamento* é outro fator influenciador de compartilhamento da informação, essas oportunidades podem ser tanto formais quanto informais. Ambos os tipos de oportunidade foram identificados nas entrevistas, sem diferenciar qual o mais importante. Dentre os canais de aprendizado relacionais foram citadas as conversas informais, o incentivo que a empresa fornece para que os indivíduos consultem seus companheiros e a observação.

> “A gente encoraja isto. A gente já teve problema de esperar de um projeto andar, mas o indivíduo ficou nessa de tentar resolver sozinho e não andar, não progredir. Então a gente incentiva a, se tiver uma dúvida, os outros membros não terão problema em ajudar”.
>
> Entrevistado1, Empresa1.

> “Se reunir, a relação entre as pessoas daqui, acho faz se unir mais pra poder disseminar o conhecimento melhor. Então, acho que em conversas informais realmente são passadas informações”.
>
> Entrevistado1, Empresa2.

> “Se eu sou novo num determinado assunto do nosso produto, então eu tento observar como as pessoas que já trabalham nisso descobrem coisas novas, que compartilham informação e tento fazer do mesmo jeito, eu tento absorver o que realmente importa. Então, com certeza é importante”.
>
> Entrevistado1, Empresa1.

As oportunidades de compartilhamento com propósito foram mais citadas do que os relacionais, dentre elas foram identificadas reuniões de equipe, documentação do trabalho, algumas tentativas de utilização de fórum e *wikis*, mas foi notada a ausência de treinamentos. Em ambos os tipos de oportunidade não houve a preocupação com o conhecimento relativo a segurança da informação.

> “A gente incentiva a uma pessoa que conseguiu algo que ninguém escreveu ainda, a escrever, a fazer palestra”.
>
> Entrevistado1, Empresa1.

> “Uma coisa que a gente usa muito em desenvolvimento, é a questão do reuso. A questão do que é mais fácil de explicar, se é mais fácil de passar a solução pra outra pessoa”.
>
> Entrevistado2, Empresa1.

> “A gente utiliza o scrum, e todos os dias tem reuniões entre cada projeto, cada grupo de projeto e cada um fala pro outro o que está fazendo, quais suas dúvidas e quais seus problemas, e quais as soluções. Isso, acho bem legal, mas isso é de acordo com a metodologia”.
>
> Entrevistado1, Empresa2.

> “Tem vários aspectos que a empresa fornece: existem os documentos, que são compartilhados por todos”.
>
> Entrevistado2, Empresa2.

> “Nós temos um sistema interno para compartilhamento de informação. Com fórum, com wiki e temos reuniões esporádicas”.
>
> Entrevistado1, Empresa3.

> “Tudo documentado. Documentação e especificação a gente cadastra e joga no svn, tanto a documentação do usuário, que é de praxe, e tudo o que a gente faz em relação à implementação a gente coloca no [x]. Que é uma forma de gerenciar o trabalho da gente”.
>
> Entrevistado2, Empresa2.

> “Não conheço nenhum treinamento aqui relacionado a isso”.
>
> Entrevistado1, Empresa2.

5.2.4 Natureza do conhecimento

O último fator do modelo de Ipe (2003) é a natureza do conhecimento, o valor do conhecimento e a forma na qual ele se apresenta, tácito ou explícito, tem impacto sobre o compartilhamento. O fato de, na categoria anterior, os canais com propósito serem mais frequentes se justifica por que a maioria desses canais trata de conhecimento explícito, através da documentação, utilização de fóruns etc. O conhecimento tácito, mais difícil de ser compartilhado, é transmitido nos canais relacionais, através de conversas, de ajuda na resolução de problemas, entre outras maneiras. Da mesma forma, o valor do conhecimento foi abordado juntamente com as categorias de recompensas por compartilhar e poder. É

justamente por perceberem o valor que o conhecimento tem, que a principal recompensa pelo compartilhamento é reputação.

6 CONCLUSÕES

Com as entrevistas pôde-se traçar um perfil dos indivíduos que trabalham em empresas que desenvolvem soluções em TIC, além de identificar algumas características destas empresas. Essa análise foi feita através das percepções dos próprios entrevistados. Desta forma foi possível compreender como as empresas tratam a segurança da informação no seu dia-a-dia e como os indivíduos se comportam neste contexto.

Inicialmente percebeu-se que as empresas não tem uma preocupação de nível profissional com a segurança da informação, o que é destacado como sendo algo alarmante. Elas se mostram limitadas ao focar a segurança apenas nas propriedades de acessibilidade e confidencialidade, ou seja, proteger a informação do acesso por pessoas indevidas e garantir que as pessoas autorizadas tenham acesso à informação.

As empresas não se mostram preparadas para enfrentar problemas de segurança a nível mais amplo, como ocorreu no caso das perdas de informação devido ao apagão, um evento fora do comum, mas previsível. Elas falham em não formalizar a segurança da informação, criando uma política de segurança da informação que possa guiar o comportamento de seus funcionários. Também falham em não prover aos seus funcionários o conhecimento necessário para eles desenvolverem seus trabalhos conscientes de garantir a segurança da informação.

Desta forma, a segurança da informação dentro das empresas ocorre de forma informal. Os funcionários desenvolvem seus trabalhos preocupados apenas com as questões relativas às regras de negócio. Seguem as normas básicas determinadas pelas empresas e ignoram a necessidade de haver cuidados em diversos comportamentos e ações executadas dentro da empresa.

Dentro das empresas foi verificado que existe uma forte atividade de compartilhamento de conhecimento entre os indivíduos. Eles consideram seus companheiros como a principal fonte de conhecimento no momento que precisam tirar dúvidas ou resolver problemas. Toda essa cultura de compartilhamento de conhecimento é apoiada pelas empresas, que a vê como uma forma de contribuir para a produtividade dos seus funcionários.

Os indivíduos se mostraram entusiastas do compartilhamento de conhecimento, revelando serem preocupados com a disseminação do conhecimento, buscando apoiar o crescimento da área e melhorar a produtividade da empresa. Embora, eles compartilhem pensando em futuramente, quando precisarem, possam recorrer aos outros indivíduos. Eles

também valorizam muito a imagem que possui o indivíduo que compartilha, ou seja, a reputação perante os companheiros e perante a gerência.

Um fato claro, percebido nas respostas dos entrevistados, é que eles possuem pouco conhecimento sobre segurança da informação. Isso é consequência da formação universitária que não aborda esta área e da falta de interesse das empresas no assunto. E isto é umas das causas principais de não haver, no meio de tanto compartilhamento de conhecimento, o compartilhamento de conhecimento relativo à segurança da informação.

A segurança da informação é um tema que pode ser considerado crítico dentro das organizações, qualquer compartilhamento impreciso e errado poderia gerar consequências que trariam sérios impactos negativos à organização. Então, para evitar que sua imagem fosse abalada, conscientes do pouco conhecimento que possuem e dos riscos, eles não se sentem confiantes em compartilhar conhecimento quando o assunto é segurança da informação.

Para suprir as necessidades de conhecimento sobre segurança da informação, os indivíduos recorrem aos gerentes ou líderes de equipe. São eles os responsáveis pelas decisões do que deve ser feito, adotado ou compartilhado. Desta forma, os indivíduos conseguem o conhecimento que precisam e se eximem do peso de compartilhar conhecimento que pode levar a manchas na sua reputação.

Assim, entende-se que as empresas não tem uma preocupação com a segurança da informação, deixando que ela seja feita informalmente. O compartilhamento de conhecimento entre os indivíduos é natural e constante, exceto quando o conhecimento é relativo à segurança da informação. Pois, os indivíduos que fazem parte dessas empresas não apresentam conhecimento adequado sobre segurança da informação. Eles deixam a responsabilidade de decisões sobre segurança nas mãos dos líderes de equipe.

6.1 LIMITAÇÕES E ESTUDOS FUTUROS

A presente pesquisa tem algumas limitações que impedem que os resultados sejam estendidos a todas as empresas de desenvolvimento de soluções em TIC. A primeira e principal limitação desta pesquisa foi a quantidade de indivíduos entrevistados e de empresas participantes. As empresas existentes na região carecem de maior publicidade, muitas delas não têm websites nem não fazem propagandas, dificultando que as mesmas sejam encontradas.

Tentando contornar esse problema, escolhemos como critério de seleção as empresas participantes do Farol Digital. Uma iniciativa, que principalmente, torna as empresas acessíveis. Mas, mesmo tendo o website do Farol Digital como fonte agregadora de informações sobre as empresas, tais informações de contato muitas vezes não eram completas ou estavam desatualizadas.

Dentre as empresas com as quais foi possível estabelecer contato, a maioria delas não demonstrou interesse de participação na pesquisa. Esse desinteresse pode ter vários motivos, como indisponibilidade de tempo, mas podemos inferir que o desconhecimento sobre a pesquisa científica contribui para esse desinteresse.

Além da limitação de quantidade de pessoas participante, a presente pesquisa tem caráter exploratório, ficando como sugestão para que futuros estudos aprofundem os estudos aqui iniciados, além de ampliar a amostra da pesquisa.

Esta pesquisa teve como entrevistados os funcionários das empresas que não ocupam cargos de gerência. Como dentre os achados da pesquisa verificou-se que os gerentes e líderes de equipe exercem uma influência consideravelmente grande na garantia da segurança da informação nas empresas, também sugerimos que em estudos posteriores seja investigado a real influência dos gerentes e líderes, além de averiguar o conhecimento que eles têm sobre segurança da informação.

REFERÊNCIAS

AIRC. Attack Intelligence Research Center Annual Threat Report: 2008 Overview and 2009 Predictions. Attack Intelligence Research Center, Alladin Knowledge Systems, Belcamp, MD. Disponível em: <http://www.aladdin.com/pdf/airc/AIRC-Annual-Threat-Report2008.pdf> . Acessado em: 8 mar 2012.

ALAVI, M.; LEIDNER, D. E. Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. **MIS Quarterly**, v. 25, n. 1, p.107-136, 2001.

ANDERSON, E.; CHOOBINEH, J. Enterprise Information Security Strategies. **Computers & Security**, v. 27, p. 22-29, 2008.

ANDREWS, K. M.; DELAHAYE, B. L. Influences on knowledge processes on organisational learning: The psychosocial filter. **Journal of Management Studies**, v. 37, n. 6, p.797-809, 2000.

BARRET, M.; CAPPLEMAN, S.; SHOIB, G.; WALSHAM, G. Learning in Knowledge Communities: Managing Technology and Context. **European Management Journal**, v. 22, n.1, p. 1-11, 2004.

BASKERVILLE, R.; SIPONEN, M. An Information Security Meta-Policy for Emergent Organizations. **Logistics Information Management**, v. 15, n. 5/6, p. 337-346, 2002.

BAUER, M. W.; GASKELL, G. Pesquisa qualitativa com texto, imagem e som: um manual prático. 7. Ed. Petrópolis: Vozes, 2008.

BLAKLEY, B.; McDERMOTT, E.; GEER, D. Information Security is Information Risk Management. **Procedures of ACM Workshop on New Security Paradigms**, 2001.

BOCK, G;. LEE, J.; ZMUD, R. Behavioral Intention Formation in Knowledge Sharing: Examining the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate, **MIS Quarterly**, v. 29, n.1, p. 87-111, 2005.

BOSS, S. R.; KIRSCH, L. J. The Last Line of Defense: Motivating Employees to Follow Corporate Security Guideliness. **Proceedings of the 28th International Conference on Information Systems**, Montreal, 2007.

BROWN, J. S.; DUGUID, P. Organizational Learning and Communities-of-Practice: Toward a Unified View of Working, Learning, and Innovation. **Organization Science**, v. 2, n. 1, p. 40-57, 1991.

BROWN, R.B.; WOODLAND, M. J. Managing knowledge wisely: A case study in organizational behavior. **Journal of Applied Management Studies**, v. 8, n. 2, p. 175-198, 1999.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness. **MIS Quarterly**, v. 34, n. 3, p. 523-548, 2010.

BURRELL, G.; MORGAN, G. Sociological paradigms and organizational analysis: elements of the sociology of corporate life. Ashgate Publishing Limited, Aldershot, England, 1979.

CAVUSOGLU, H.; CAVUSOGLU, H.; RAGHUNATHAN, S. Economics of IT Security Management: Four Improvements to Current Security Practices. **Communications of the Association for Information Systems**, v. 14, p. 65-75, 2004.

CHOO, C. W. A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. São Paulo: Ed. Senac São Paulo, 2006.

CHOO, K. R. The cyber threat landscape: Challenges and future research directions. **Computers & Security**, v. 30, p. 719-731, 2011.

CHOOBINEH, J.; DHILLON, G.; GRIMAILA, M. R.; REES, J. Management of Information Security: Challenges and Research Directions. **Communications of the Association for Information System**, v. 20, p. 958-971, 2007.

COAKES, E. Knowledge Management: A Primer. **Communications of the Association for Information Systems**, v. 14, p. 406-489, 2004.

COHEN, W. M.; LEVINTHAL, D. A. Absorptive Capacity: A New Perspective on Learning and Innovation. **Administrative Science Quarterly**, v. 35, n. 1, Special Issue: Technology, Organizations, and Innovation, p. 128-152, 1990.

CONNER, F. W.; COVIELLO, A.W. Information Security Governance: A Call to Action. National Cyber Security Partnership Corporate Governance Task Force Report. 2004.

CONSTANT, D.; KIESLER, S.; SPROULL, L. What's Mine Is Ours, or Is It? A Study of Attitudes about Information Sharing. **Information System Research**, v. 5, n. 4, p. 400-421, 1994.

CORMACK, A. Do we need a security culture? **VINE,** v. 31, n. 2, p. 8 -10, 2001.

CORTÊS, M. R.; PINHO, M.; FERNANDES, A. C.; SMOLKA, R. B.; BARRETO, A. L. C. M. Cooperação Em Empresas De Base Tecnológica: uma primeira avaliação baseada numa pesquisa abrangente. **São Paulo Em Perspectiva**, v. 19, n. 1, p. 85-94, 2005.

COX, A.; CONNNOLY, S. Raising information security awareness in the academic setting. **VINE 123**, 2001.

D`ARCY, J.; HOVAV, A.; GALLETA, D. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach**. Information Systems Research** 20(1), p. 79–98, 2009.

DAVENPORT, T. H.; DELONG, D. W.; BEERS, M. C. Sucessful Management Knowledge Projects. **Sloan Management Review**, 1998.

DAVENPORT, T.; PRUSAK, L. Conhecimento empresarial. Rio de Janeiro: Campus, 1998.

DAVISON, R. M.; OU, C. X. J.; MARTINSONS, M. G. Information Technology to Support Informal Knowledge Sharing. **Information Systems Journal**. 2012.

DELONG, D. W.; FAHEY, L. Diagnosing cultural barriers to knowledge management. **Academy of Management Executive**, v. 14, n. 4, p. 113-127, 2000.

DLAMINI, M. T.; ELOFF, J. H. P.; ELOFF, M. M. Information Security: The moving target. **Computers & Security**, 28, p. 189-198, 2009.

DOHERTY, N. F.; FULFORD, H. Aligning the information security policy with the strategic information systems plan. **Computers & Security**, 23, p. 55-63. 2006.

DRUCKER, P.F. The new society of organizations, **Harvard Business Review**, V. 95, n. 5, p. 95-105, 1992.

FAUCHER, J. B. P. L.; EVERETT, A. M.; LAWSON, R. Reconstituting knowledge management. **Journal of Knowledge Management**, v. 12, n. 3, p. 3-16, 2010.

FLICK, U. Introdução à pesquisa qualitativa. Métodos de Pesquisa. 3. ed. Porto Alegre: Artmed, 2009.

GERBER, M.; VON SOLMS, R. Management of risk in the information age. **Computers & Security**, v. 24, p. 16-30, 2001.

GODOI, C.; MATTOS, P. Entrevista qualitativa: instrumento de pesquisa e evento dialógico. In: GODOI, Cristiane; BANDEIRA-DE-MELO, Rodrigo; SILVA, Anielson (organizadores). Pesquisa qualitativa em estudos organizacionais: paradigmas, estratégias e métodos. São Paulo: Saraiva, 2006.

GORDON, L. A.; LOEB, M.P. The economics of information security investment. **ACM Transactions on Information and System Security**, v. 5, n. 4, p. 438–457, 2002.

GRANT, R. M. Prospering in Dynamically-Competitive Environments: Organizational Capability as Knowledge Integration. **Organization Science**, v. 7, n. 4, p. 375-387, 1996.

GRANT, R. M. Toward A Knowledge-Based Theory of the Firm. **Strategic Management Journal**, v. 17, p. 109-122, 1996.

GRAY, D. E. Pesquisa no mundo real. 2.ed. Porto Alegre: Penso, 2012.

GUPTA, A. K.; GOVINDARAJAN, V.. Knowledge Flows Within Multinational Corporations. **Strategic Management Journal**, v. 21, p. 473-496, 2000.

HANISCH, B.; LINDNER, F.; MUELLER, A.; WALD, A. Knowledge management in project environments. **Journal of Knowledge Management**, v. 13, n. 4, p. 148-160, 2009.

HARLOW, J. Security policy - an individual view. **VINE**, v. 31, n. 2, p.17-22, 2001.

HENDRIKS, P. Why Share Knowledge? The Influence of ICT on the Motivation for Knowledge Sharing. **Knowledge and Process Management**, v. 6, n. 2, p. 91–100, 1999.

HONE, K.; ELOFF, J. H. P. Information security policy: what do international information security standards say? **Computers & Security**, v. 21, n. 5, p. 402-409, 2002.

HSU, C.; LEE, J.; STRAUB. D. W. Institutional Influences on IS Security Innovations. **Information Systems Research**. Articles in Advance, p. 1–22, 2012.

IFINEDO, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. **Computers & Security**, v. 31, n. 1, p. 83-95, 2012.

IPE, M. Knowledge Sharing in Organizations: A Conceptual Framework. **Human Resource Development Review**, v. 2, n. 4, 2003.

ISO/IEC 17799. Information technology - Security techniques - Code of practice for information security management, 2005.

JARVENPAA, S.L; STAPLES, D.S. Exploring perceptions of organizational ownership of information and expertise. **Journal of Management Information Systems**, v. 18, n. 1, p.151–183, 2001.

JASIMUDDIN, S. M. A holistic view of knowledge management strategy. **Journal of Knowledge Management**, v. 12, n. 2, p. 57-66, 2008.

JISC - JOINT INFORMATION SYSTEMS COMMITTEE. Developing an Information Security Policy . Publicado em: 16 Mar 2001. Disponível em: <http://www.jisc.ac.uk/aboutus/howjiscworks/committees/subcommittees/pastcommittees/jcas/jcaspaperssecurity.aspx> Acessado em: 20 fev 2012.

KARJALAINEN, M.; SIPONEN, M. Toward a New Meta-Theory for Designing Information Systems (IS) Security training Approaches. **Journal of the Association for Information Systems**. Vol. 12, Issue 8, p. 518-555, 2011.

KARYDA, M.; KIOUNTOUZIS, E.; KOKOLAKIS, S. Information systems security policies: a contextual perspective. **Computers & Security**, 24(3), p. 246–260, 2005.

KOGUT,B.; ZANDER, U. Knowledge of The Firm, Combinative Capabilities, and The Replication Of Technology. **Organization Science**, v. 3, n. 3, p. 383-397, 1992.

LANE, P. J.; LUBATKIN, M. Relative Absorptive Capacity And Interorganizational Learning. **Strategic Management Journal**, v. 19, p. 461–477, 1998.

LOWENDAHL, B. R.; REVANG, O.; FOSSTENLOKKEN, S. M. . Knowledge and value creation in professional service firms: A framework for analysis. **Human Relations**, v. 54, n. 7, p. 911- 931, 2001.

MACFARLANE, R.; BUCHANAN, W.; EKONOMOU, E.; UTHMANI, O.; FAN, L.; LO, O. Formal security policy implementations in network firewalls, **Computers & Security**, v. 31, p. 253-370, 2012.

MACHADO, S. A.; PIZYSIEZNIG, J.; CARVALHO, M. M.; RABECHINI, R. MPEs de Base Tecnológica: conceituação, formas de financiamento e análise de casos brasileiros, 2001.

MACHLUP, F. Semantic quirks in studies of information. In: MACHLUP, F.; MANSFIELD, U. (Ed.). The study of information: Interdisciplinary messages New York, NY: Wiley, p. 641-671, 1983.

MADIGAN, E.M.; PETRULICH, C.; MOTUK, K., The cost of non-compliance: when policies fail. ACM. Baltimore, MD, USA, p. 47-51, 2004.

MANZINI, E. J. A entrevista na pesquisa social. Didática, São Paulo, v. 26/27, p. 149-158, 1991.

MARCH, J. G. Exploration and Exploitation in Organizational Learning, **Organization Science**, v. 2, n. 1, p. 71–87, 1991.

MARTINSONS, M. G.; WESTWOOD, R. I. Management information systems in the Chinese business culture: An explanatory theory. **Information & Management**, v. 32, n. 5, p. 215-228, 1997.

MCDERMOTT, R. Learning Accross Teams: The Role of Communities of Practice in Team Organizations. **Knowledge Management Review**, 1999.

MCLEAN, K. Information security awareness – Selling the cause. Proceedings of the IFIP TC11, Eighth International Conference on Information Security: IT Security: The Need for International Cooperation, p. 179-193, 1992.

MERRIAM, S. B. Qualitative Research: a guide to design and implementation. San Francisco: Jossey-Bass, 2009.

MITNICK, K. D.; SIMON. W, L. **The Art Of Deception: Controlling The Human Element Of Security**. Wiley Publishing. Indianapolis, 2002.

NAHAPIET, J.; GHOSHAL,S. Social capital, intellectual capital, and the organizational advantage**. The Academy of Management Review**, v. 23, n.2, 1998.

NONAKA, I. A Dynamic Theory of Organizational Knowledge Creation. **Organization Science**, v. 5, n.1, p. 14-37, 1994.

O'REILLY, C.; PONDY, L. Organizational Communications. 1980. In Kerr, S. (ed.) Organizational Behavior. Columbus: Grid. OFEK, SARVARY, 2001.

PAN, S. L.; SCARBROUGH, H. Knowledge management in practice: An exploratory case study. Technology Analysis & Strategic Management, v. 11, n. 3, 1999.

POLANYI, M. Personal Knowledge, London, Routledge and Kegan Paul. 1962.

POLANYI, M. The tacit dimension. New York: Doubleday Anchor. 1967.

POLANYI, M. Meaning, The University of Chicago Press, Chicago, IL. 1975.

PUHAKAINEN, P.; SIPONEN, M. Improving employees' compliance through information systems security training: An action research study. MisQuarterly, 34(4), p. 757-778, 2010.

RANDEREE, E. Knowledge management: securing the future. **Journal of Knowledge Management**, v. 10, n. 4, p. 145-156, 2006.

RANSBOTHAM, S.; MITRA, S. Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. **Information Systems Research**, v. 20, n. 1, p. 121–139, 2009.

ROOS, J.; VON KROGH, G. Figuring Out Your Competence Configuration. **European Management Journal**, v. 10, n. 4, p. 422-42, 1992.

ROUSE, M. **Framework**. Publicado em: Setembro de 2005. Disponível em: <http://whatis.techtarget.com/definition/framework>. Acessado em: 29 de setembro de 2012.

SAMBAMURTHY, V.; SUBRAMANI, M. Special Issue On Information Technologies And Knowledge Management. **MIS Quarterly**, v. 29, n. 1, p. 1-7, 2005.

SAMPIERI, R.; COLLADO, C.; LUCIO, P. **Metodología de la investigacíon**. México: McGraw-Hill, 1991.

SIEMSEN, E.; ROTH, A. V.; BALASUBRAMANIAN, S.; ANAND, G. The influence of psychological safety and confidence in knowledge on employee knowledge sharing. **Manufacturing & Service Operations Management**, v. 11, n. 3, ,p. 429-447, 2009.

SIPONEN, M. T.; PAHNILA, S.; MAHMOOD, A. Employees‘ adherence to information security policies: An empirical study**. Proceedings of the IFIP SEC2007**, p. 14-16, 2007.

SIPONEN, M.; WILLISON, R. Information security management standards: Problems and solutions. **Information & Management**, 46, p. 267–270. 2009.

SIPONEN, M.; BASKERVILLE, R.; HEIKKA, J. A Design Theory for Secure Information Systems Design Methods. **Journal of the Association for Information Systems**, v. 7, n. 11, p. 725-770, 2006.

SONG, J.; ALMEIDA, P.; WU, G. Learning-by-Hiring: When Is Mobility More Likely to Facilitate Interfirm Knowledge Transfer? **Management Science**, v. 49, n. 4, p. 351–365, 2003.

SPENDER, J. C. Making knowledge the basis of a dynamic theory of the firm, **Strategic Management Journal**, Special Issue, v. 17, p. 45-62, 1996.

SPENDER, J. C.; GRANT, R. Knowledge and the firm: overview. **Strategic Management Journal**, Special Issue, v. 17, p. 5-9, 1996.

STANTON,J. R.; STAM, K. R.; MASTRANGELO, P.; JOLTON, J. Analysis of end user security behaviors. **Computers & Security**, v. 24, p. 124-133, 2005.

STENMARK, D. Leveraging Tacit Organisational Knowledge. **Journal of Management Information Systems**, v. 17, n. 3, p. 9-24, 2001.

STEVENSON, W. B.; GILLY, M. C. Information Processing and Problem Solving: The Migration of Problems Through Formal Positions and Networks of Ties. **Academy of Management Journal**, v. 34, p. 918-928, 1991.

STOREY, D. J.; TETHER, B. S. New technology-based firms in the European Union: an introduction. **Research Policy**, v. 26, p. 933–946, 1998.

STRAUB, D. W. Effective IS security: An empirical study. **Information Systems Research** v. 1, n. 3, p; 255- 276, 1990.

SYMANTEC. Symantec Internet Security Threat Report:Trends for 2008, Symantec Corporation, Cupertino, CA. Disponível em: <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiv_04-2009.en-us.pdf> Acessado em: 8 mar 2012.

TAMPOE, M. Motivating knowledge workers - the challenge for the 1990s. In: Myers, P.S. (ed.), Knowledge Management and Organizational Design, Boston, MA, Butterworth-Heinemann, p. 179–190, 1996.

TRURAN, W. R. Pathways for knowledge: How companies learn through people. **Engineering Management Journal**, v. 10, n. 4, 1998.

TUOMI, I. Data is more than knowledge: implications of the reversed knowledge hierarchy for knowledge management and organization memory. **Journal of Management Information Systems**, v. 16, n. 3, p. 103-117, 1999.

VALERIO, A.; VALERIO, D. M. Gestão De Pessoas Altamente Qualificadas Em Pequenas Empresas De Base. **Revista De Administração Mackenzie**, v. 7, n. 3, p. 131-147, 2006.

VON SOLMS, B. Information Security: A Multidimensional Discipline. **Computers & Security**, n. 20, p. 504-508, 2001.

VON SOLMS, B; VON SOLMS, R. The 10 deadly sins of information security management. **Computers & Security**, n. 23, v. 5, p. 371-376, 2004.

VON SOLMS, S. H. Information Security Governance - Compliance management vs operational management. **Computers & Security**, 24, p. 443-447, 2005.

WALTER, S. A.; BACH, T. M. Adeus papel, marca-textos, tesoura e cola: Inovando o processo de análise de conteúdo por meio do ATLAS.TI. Disponível em: <http://www.ead.fea.usp.br/semead/12semead/resultado/trabalhosPDF /820.pdf>. Acesso em 23 de setembro de 2012.

WARKENTIN, M.; WILLISON, R. Behavioral and Policy Issues in Information Systems Security: The Insider Threat. **European Journal of Information Systems**, p. 101-105. 2009.

WESTHEAD, P. R&D inputs. and outputs. of technology based firms located on and off Science Parks. **R&D Management**, v. 27, n. 1, 1997.

WHITMAN, M. E.; TOWNSEND, A. M.; ALBERTS, R. J.; KHOSROWPOUR, M. (ed) Information systems security and the need for policy. Information Security Management: Global Challenges in the New Millennium. Idea Group Publishing, Hershey, PA, 9–18. 2001.

YLI-RENKO, H.; AUTIO, E.; SAPIENZA, H. J. Social Capital, Knowledge Acquisition, And Knowledge Exploitation In Young Technology-Based Firms. **Strategic Management Journal**, v. 22, p. 587–613, 2001.

APÊNDICE A - PRIMEIRA VERSÃO DO ROTEIRO DE ENTREVISTA.

QUESTÕES SOBRE O ENTREVISTADO E A EMPRESA	
1. SEXO	M / F
2. IDADE	
3. FORMAÇÃO (CURSO E ANO)	
4. INSTITUIÇÃO DE FORMAÇÃO	
5. HÁ QUANTO TEMPO TRABALHA NA ORGANIZAÇÃO?	
6. QUAL A SUA FUNÇÃO?	
7. O QUE VOCÊ ACHA DO CLIMA DA ORGANIZAÇÃO?	
8. GOSTA DO TRABALHO?	
9. O TRABALHO É EM EQUIPE OU INDIVIDUAL?	
EXISTE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DEFINIDA FORMALMENTE NA EMPRESA?	
SEGURANÇA DA INFORMAÇÃO (AVALIAR O CONHECIMENTO DO ENTREVISTADO SOBRE SEGURANÇA DA INFORMAÇÃO)	
10. O QUE VOCÊ ENTENDE POR SEGURANÇA DA INFORMAÇÃO?	

11. VOCÊ TEM CONHECIMENTO SOBRE GUIAS DE MELHORES PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO? (CASO SIM, PEDIR PRA CITAR)	
12. VOCÊ TEM CONHECIMENTO SOBRE TÉCNICAS E MÉTODOS DE SEGURANÇA PARA DESENVOLVIMENTO DE SOFTWARES?	
13. O QUE VOCÊ ENTENDE POR POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO?	
14. VOCÊ TEM CONSCIÊNCIA DO SEU PAPEL E DE SUAS RESPONSABILIDADES PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO?	
CRIAÇÃO DE SIGNIFICADO (INTERPRETAÇÃO, SELEÇÃO, RETENÇÃO)	
15. JÁ HOUVE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO? (Invasão, roubo, acidente que levou a perda de informação).	INTERPRETAÇÃO
16. ALGUMA SITUAÇÃO TROUXE A NECESSIDADE DE MUDANÇAS NA SEGURANÇA DA INFORMAÇÃO?	INTERPRETAÇÃO
17. O QUE FOI NECESSÁRIO MUDAR?	SELEÇÃO
18. QUE AÇÕES FORAM TOMADAS?	SELEÇÃO
19. ESSAS AÇÕES SÃO DOCUMENTADAS DE FORMA QUE POSSAM SER CONSULTADAS DEPOIS?	RETENÇÃO
CONSTRUÇÃO DO CONHECIMENTO (SOCIALIZAÇÃO, EXTERIORIZAÇÃO, COMBINAÇÃO E INTERNALIZAÇÃO)	

20. VOCÊ CONSULTA OUTRAS PESSOAS, INCLUSIVE DE OUTRAS EMPRESAS, QUANDO PRECISA RESOLVER UM PROBLEMA RELATIVO A SEGURANÇA DA INFORMAÇÃO?	SOCIALIZAÇÃO
21. QUAIS PESSOAS VOCÊ CONSULTA?	SOCIALIZAÇÃO
22. QUAIS OS MEIOS UTILIZADOS PARA CONSULTAR?	SOCIALIZAÇÃO
23. A ORGANIZAÇÃO PROVÊ TREINAMENTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO?	SOCIALIZAÇÃO
24. VOCÊ OBSERVA O TRABALHO DE OUTRAS PESSOAS PARA APRENDER?	SOCIALIZAÇÃO
25. VOCÊ COMPARTILHA O CONHECIMENTO SOBRE SEGURANÇA DA INFORMAÇÃO QUE POSSUI?	EXTERIORIZAÇÃO
26. QUAIS FATORES TE MOTIVAM A COMPARTILHAR E QUAIS TE IMPEDEM DE COMPARTILHAR?	EXTERIORIZAÇÃO
27. AS PESSOAS DA EMPRESA COMPARTILHAM SUAS EXPERIÊNCIAS SOBRE SEGURANÇA DA INFORMAÇÃO COM O RESTO DA EQUIPE?	EXTERIORIZAÇÃO
28. A EMPRESA ENCORAJA E FACILITA O COMPARTILHAMENTO DE INFORMAÇÃO?	EXTERIORIZAÇÃO
29. QUAIS FATORES INTERFEREM NO COMPARTILHAMENTO DAS INFORMAÇÕES?	EXTERIORIZAÇÃO
30. OS INDIVÍDUOS NA ORGANIZAÇÃO EXPÕEM SUAS NECESSIDADES EM CONVERSAS PROCURANDO RECEBER AJUDA?	EXTERIORIZAÇÃO

31. OS INDIVÍDUOS QUE COMPARTILHAM SEUS CONHECIMENTOS SÃO RECOMPENSADOS POR ISSO?	EXTERIORIZAÇÃO
32. A EMPRESA FORNECE MEIOS PARA APOIAR O COMPARTILHAMENTO DE INFORMAÇÃO?	EXTERIORIZAÇÃO
33. QUAIS OUTROS FONTES DE CONHECIMENTO VOCÊ UTILIZA?	COMBINAÇÃO
34. AS POSSÍVEIS SOLUÇÕES SÃO TESTADAS OU SIMULADAS ANTES DE SEREM APLICADAS?	INTERNALIZAÇÃO
TOMADA DE DECISÃO	
35. O QUE INFLUENCIA A SUA DECISÃO DE ESCOLHA DO CONHECIMENTO A SER UTILIZADO NA SOLUÇÃO DO SEU PROBLEMA?	
36. COMO VOCÊ AVALIA SE A SUA ESCOLHA CONSEGUIRÁ RESOLVER O SEU PROBLEMA?	
37. O QUE VOCÊ ESPERA DA SOLUÇÃO SELECIONADA PARA SER APLICADA?	

APÊNDICE B - SEGUNDA VERSÃO DO ROTEIRO DE ENTREVISTA.

1. IDADE
2. FORMAÇÃO (INSTITUIÇÃO, CURSO E ANO)
3. HÁ QUANTO TEMPO TRABALHA NA ORGANIZAÇÃO?
4. QUAL A SUA FUNÇÃO?
5. O QUE VOCÊ ACHA DO CLIMA DA ORGANIZAÇÃO?
6. GOSTA DO TRABALHO?
SEGURANÇA DA INFORMAÇÃO
7. O QUE VOCÊ ENTENDE POR SEGURANÇA DA INFORMAÇÃO?
8. VOCÊ TEM CONHECIMENTO SOBRE GUIAS DE MELHORES PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO? (CASO SIM, PEDIR PRA CITAR)
9. VOCÊ TEM CONHECIMENTO SOBRE TÉCNICAS E MÉTODOS DE SEGURANÇA PARA DESENVOLVIMENTO DE SOFTWARES?
10. O QUE VOCÊ ENTENDE POR POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO?
11. VOCÊ TEM CONSCIÊNCIA DO SEU PAPEL E DE SUAS RESPONSABILIDADES PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO?
12. A EMPRESA NÃO POSSUI UMA POLÍTICA DE SEGURANÇA FORMALIZADA, ENTÃO COMO A EQUIPE DE FUNCIONÁRIOS PROCEDE PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO?
13. HÁ UM CONSENSO SOBRE COMO PROCEDER OU CADA INDIVÍDUO AGE DE ACORDO COM O SEU CONHECIMENTO?
14. SENDO A SEGURANÇA DA INFORMAÇÃO UM PONTO CRÍTICO NAS ORGANIZAÇÕES, ONDE UMA FALHA PODE GERAR GRANDES

CONSEQUÊNCIAS, VOCÊ SE SENTE CONFIANTE EM COMPARTILHAR CONHECIMENTO SOBRE ESSE TEMA?
15. JÁ HOUVE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO? (Invasão, roubo, acidente que levou a perda de informação).
16. ALGUMA SITUAÇÃO TROUXE A NECESSIDADE DE MUDANÇAS NA SEGURANÇA DA INFORMAÇÃO? O QUE FOI NECESSÁRIO MUDAR? QUE AÇÕES FORAM TOMADAS?
17. É REALIZADA A DOCUMENTAÇÃO DO TRABALHO?
18. VOCÊ CONSULTA OUTRAS PESSOAS, INCLUSIVE DE OUTRAS EMPRESAS, QUANDO PRECISA RESOLVER UM PROBLEMA RELATIVO A SEGURANÇA DA INFORMAÇÃO?
19. QUEM SÃO ESSAS PESSOAS QUE VOCÊ CONSULTA?
20. VOCÊ PROCURA PRIMEIRAMENTE INDIVÍDUOS QUE SEJAM MAIS PRÓXIMOS A VOCÊ OU INDIVÍDUOS QUE TENHAM A MELHOR REPUTAÇÃO?
21. VOCÊ CONTINUARIA COMPARTILHANDO O SEU CONHECIMENTO COM INDIVÍDUOS QUE SE RECUSAM OU NÃO COMPARTILHAM CONHECIMENTO ESPONTANEAMENTE?
22. PRA VOCÊ, É IMPORTANTE SER RECONHECIDO PELOS SEUS COLEGAS DE TRABALHO POR SEU CONHECIMENTO?
23. COMPARTILHAR O CONHECIMENTO É UMA FORMA DE MELHORAR O SEU RELACIONAMENTO COM COLEGAS DE TRABALHO E/OU AMIGOS?

24. QUAIS OS MEIOS UTILIZADOS PARA CONSULTAR?
25. A ORGANIZAÇÃO PROVÊ TREINAMENTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO?
26. VOCÊ OBSERVA O TRABALHO DE OUTRAS PESSOAS PARA APRENDER?
27. VOCÊ COMPARTILHA O CONHECIMENTO SOBRE SEGURANÇA DA INFORMAÇÃO QUE POSSUI?
28. QUAIS FATORES TE MOTIVAM A COMPARTILHAR E QUAIS TE IMPEDEM DE COMPARTILHAR?
29. AS PESSOAS DA EMPRESA COMPARTILHAM SUAS EXPERIÊNCIAS SOBRE SEGURANÇA DA INFORMAÇÃO COM O RESTO DA EQUIPE?
30. VOCÊ ACREDITA QUE AS PESSOAS QUE COMPARTILHAM CONHECIMENTO NA EMPRESA TEM MELHOR REPUTAÇÃO ENTRE OS COLEGAS?
31. A EMPRESA ENCORAJA E FACILITA O COMPARTILHAMENTO DE INFORMAÇÃO?
32. QUAIS FATORES INTERFEREM NO COMPARTILHAMENTO DAS INFORMAÇÕES?
33. OS INDIVÍDUOS NA ORGANIZAÇÃO EXPÕEM SUAS NECESSIDADES EM CONVERSAS PROCURANDO RECEBER AJUDA?
34. OS INDIVÍDUOS QUE COMPARTILHAM SEUS CONHECIMENTOS SÃO RECOMPENSADOS POR ISSO?
35. VOCÊ ACREDITA QUE AS PESSOAS QUE COMPARTILHAM CONHECIMENTO NA EMPRESA TEM MELHOR REPUTAÇÃO PERANTE A GERÊNCIA?
36. QUAL A VANTAGEM QUE VOCÊ TEM POR COMPARTILHAR O SEU CONHECIMENTO?
37. A EMPRESA FORNECE MEIOS PARA APOIAR O COMPARTILHAMENTO DE

INFORMAÇÃO?
38. QUAL A VANTAGEM QUE A ORGANIZAÇÃO TEM AO HAVER COMPARTILHAMENTO DE CONHECIMENTO ENTRE OS SEUS FUNCIONÁRIOS?
39. QUAIS OUTROS FONTES DE CONHECIMENTO VOCÊ UTILIZA?
40. AS POSSÍVEIS SOLUÇÕES SÃO TESTADAS OU SIMULADAS ANTES DE SEREM APLICADAS?
41. O QUE INFLUENCIA A SUA DECISÃO DE ESCOLHA DO CONHECIMENTO A SER UTILIZADO NA SOLUÇÃO DO SEU PROBLEMA?
42. COMO VOCÊ AVALIA SE A SUA ESCOLHA CONSEGUIRÁ RESOLVER O SEU PROBLEMA?
43. O QUE VOCÊ ESPERA DA SOLUÇÃO SELECIONADA PARA SER APLICADA?

APÊNDICE C - TERCEIRA VERSÃO DO ROTEIRO DE ENTREVISTA.

1. IDADE
2. FORMAÇÃO (INSTITUIÇÃO, CURSO E ANO)
3. HÁ QUANTO TEMPO TRABALHA NA ORGANIZAÇÃO?
4. QUAL A SUA FUNÇÃO?
5. O QUE VOCÊ ACHA DO CLIMA DA ORGANIZAÇÃO?
6. GOSTA DO TRABALHO?
SEGURANÇA DA INFORMAÇÃO
7. O QUE VOCÊ ENTENDE POR SEGURANÇA DA INFORMAÇÃO?
8. VOCÊ TEM CONHECIMENTO SOBRE GUIAS DE MELHORES PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO? (CASO SIM, PEDIR PRA CITAR)
9. VOCÊ TEM CONHECIMENTO SOBRE TÉCNICAS E MÉTODOS DE SEGURANÇA PARA DESENVOLVIMENTO DE SOFTWARES?
10. O QUE VOCÊ ENTENDE POR POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO?
11. VOCÊ TEM CONSCIÊNCIA DO SEU PAPEL E DE SUAS RESPONSABILIDADES PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO?
12. A EMPRESA NÃO POSSUI UMA POLÍTICA DE SEGURANÇA FORMALIZADA, ENTÃO COMO A EQUIPE DE FUNCIONÁRIOS PROCEDE PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO?
13. HÁ UM CONSENSO SOBRE COMO PROCEDER OU CADA INDIVÍDUO AGE DE ACORDO COM O SEU CONHECIMENTO?

14. SENDO A SEGURANÇA DA INFORMAÇÃO UM PONTO CRÍTICO NAS ORGANIZAÇÕES, ONDE UMA FALHA PODE GERAR GRANDES CONSEQUÊNCIAS, VOCÊ SE SENTE CONFIANTE EM COMPARTILHAR CONHECIMENTO SOBRE ESSE TEMA?
15. JÁ HOUVE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO? (Invasão, roubo, acidente que levou a perda de informação).
16. ALGUMA SITUAÇÃO TROUXE A NECESSIDADE DE MUDANÇAS NA SEGURANÇA DA INFORMAÇÃO? O QUE FOI NECESSÁRIO MUDAR? QUE AÇÕES FORAM TOMADAS?
17. É REALIZADA A DOCUMENTAÇÃO DO TRABALHO?
18. VOCÊ CONSULTA OUTRAS PESSOAS, INCLUSIVE DE OUTRAS EMPRESAS, QUANDO PRECISA RESOLVER UM PROBLEMA RELATIVO A SEGURANÇA DA INFORMAÇÃO?
19. QUEM SÃO ESSAS PESSOAS QUE VOCÊ CONSULTA?
20. VOCÊ PROCURA PRIMEIRAMENTE INDIVÍDUOS QUE SEJAM MAIS PRÓXIMOS A VOCÊ OU INDIVÍDUOS QUE TENHAM A MELHOR REPUTAÇÃO?
21. VOCÊ CONTINUARIA COMPARTILHANDO O SEU CONHECIMENTO COM INDIVÍDUOS QUE SE RECUSAM OU NÃO COMPARTILHAM CONHECIMENTO ESPONTANEAMENTE?
22. PRA VOCÊ, É IMPORTANTE SER RECONHECIDO PELOS SEUS COLEGAS DE TRABALHO POR SEU CONHECIMENTO?
23. COMPARTILHAR O CONHECIMENTO É UMA FORMA DE MELHORAR O SEU RELACIONAMENTO COM COLEGAS DE TRABALHO E/OU AMIGOS?
24. QUAIS OS MEIOS UTILIZADOS PARA CONSULTAR?

25. A ORGANIZAÇÃO PROVÊ TREINAMENTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO?
26. VOCÊ OBSERVA O TRABALHO DE OUTRAS PESSOAS PARA APRENDER?
27. QUAIS FATORES TE MOTIVAM A COMPARTILHAR E QUAIS TE IMPEDEM DE COMPARTILHAR?
28. VOCÊ ACREDITA QUE AS PESSOAS QUE COMPARTILHAM CONHECIMENTO NA EMPRESA TEM MELHOR REPUTAÇÃO ENTRE OS COLEGAS?
29. A EMPRESA ENCORAJA E FACILITA O COMPARTILHAMENTO DE INFORMAÇÃO? A EMPRESA FORNECE MEIOS PARA APOIAR O COMPARTILHAMENTO DE INFORMAÇÃO?
30. OS INDIVÍDUOS NA ORGANIZAÇÃO EXPÕEM SUAS NECESSIDADES EM CONVERSAS PROCURANDO RECEBER AJUDA?
31. OS INDIVÍDUOS QUE COMPARTILHAM SEUS CONHECIMENTOS SÃO RECOMPENSADOS POR ISSO?
32. VOCÊ ACREDITA QUE AS PESSOAS QUE COMPARTILHAM CONHECIMENTO NA EMPRESA TEM MELHOR REPUTAÇÃO PERANTE A GERÊNCIA?
33. QUAL A VANTAGEM QUE VOCÊ TEM POR COMPARTILHAR O SEU CONHECIMENTO?
34. QUAL A VANTAGEM QUE A ORGANIZAÇÃO TEM AO HAVER COMPARTILHAMENTO DE CONHECIMENTO ENTRE OS SEUS FUNCIONÁRIOS?
35. QUAIS OUTROS FONTES DE CONHECIMENTO VOCÊ UTILIZA?
36. AS POSSÍVEIS SOLUÇÕES SÃO TESTADAS OU SIMULADAS ANTES DE SEREM APLICADAS?

37. O QUE INFLUENCIA A SUA DECISÃO DE ESCOLHA DO CONHECIMENTO A SER UTILIZADO NA SOLUÇÃO DO SEU PROBLEMA?
38. COMO VOCÊ AVALIA SE A SUA ESCOLHA CONSEGUIRÁ RESOLVER O SEU PROBLEMA?
39. O QUE VOCÊ ESPERA DA SOLUÇÃO SELECIONADA PARA SER APLICADA?