Revista Inteligência Competitiva
ISSN: 2236-210X

A PROTEÇÃO DE INFORMAÇÕES E A INTELIGÊNCIA COMPETITIVA: UM ESTUDO SOBRE A PERCEPÇÃO E A SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DO SETOR MOVELEIRO DA SERRA GAÚCHA

Vinicius Zanchet de Lima [1]
Ana Cristina Fachinelli [2]
Fernanda Pauletto D'Arrigo [3]
Deise Taiana de Ávila Dias [4]
Daniela Baggio [5]

RESUMO

Em um cenário competitivo, a informação e o conhecimento podem ser considerados como recursos fundamentais para a vantagem competitiva das organizações. Entretanto o volume de informações disponíveis, proporcionado pela tecnologia pode criar vantagem pelo uso destas informações nos negócios da empresa, mas também pode ser alvo de tentativas de imitação e favorecer a concorrência. Por isso, as empresas vivem um momento de valorização dos segredos comerciais, onde tão importante quanto à coleta de informações e a proteção destas informações. O presente estudo teve por finalidade investigar a percepção dos gestores a segurança da informação em suas organizações, bem como as medidas de proteção adotadas contra a espionagem industrial. Para isso foi realizado uma pesquisa qualitativa exploratória junto aos gestores de pequenas, médias e grandes empresas do setor moveleiro da Serra Gaúcha, no Rio Grande do Sul. Para a análise e interpretação dos dados foi utilizada mapas de associação de ideias. Os resultados indicam que na percepção dos gestores, a proteção das informações da empresa está associada ao porte da empresa**.**

Palavras-chave: Inteligência Competitiva. Proteção de informações. Espionagem industrial.

1 Mestrando em Administração. Universidade de Caxias do Sul. E-mail: vinizanchet@gmail.com
2 Doutora em Ciências da Comunicação e da Informação. Université de Poitiers. E-mail: afachinelli@gmail.com
3 Mestranda em Administração. Universidade de Caxias do Sul. E-mail: fernanda.darrigo@gmail.com
4 Mestre em Administração. Universidade de Caxias do Sul. E-mail: deiset.dias@gmail.com
5 Mestranda em Administração. Universidade do Vale do Rio dos Sinos. E-mail: baggiodaniela@gmail.com

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

1 INTRODUÇÃO

Em meio ao valor do conhecimento na economia global, a informação torna-se fundamental para as organizações alcançarem e manterem a vantagem competitiva em seus negócios. Neste cenário surge a Inteligência Competitiva (IC) como um processo de aquisição, organização e uso da informação no ambiente de negócios (CARUSO; STEFFEN, 1999). O monitoramento do ambiente pode proporcionar às organizações a oportunidade de antecipar as mudanças do mercado, uma vez que estas identifiquem informações que podem ser aproveitadas nos produtos, serviços e na gestão das organizações (CANONGIA, 2004). Entretanto existe uma linha tênue a respeito do limite ético e moral na aquisição destas informações e, muitas vezes o uso de algumas fontes ilícitas acaba configurando casos de espionagem industrial (CRANE, 2005; JONES, 2008).

De acordo com Jones (2008), a espionagem é uma prática mais comum do que se imagina. No mundo corporativo muitas empresas já sofreram espionagem e engana-se quem acredita que apenas grandes empresas se envolvem em casos de espionagem. De acordo com o Sebrae (2013) as pequenas e médias acabam se utilizando de informações sem saber o risco que correm. Diante deste contexto, o objetivo do estudo foi compreender a percepção dos gestores de empresas têm sobre espionagem industrial e quais práticas de prevenção contra espionagem são utilizadas para proteger suas informações.

2 REFERENCIAL TEÓRICO

O presente estudo se situa no campo da Inteligência Competitiva (IC), discutindo a aquisição, uso da informação na perspectiva da espionagem e da contra espionagem industrial.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

2.1 Inteligência Competitiva

Os pioneiros da IC no mundo dos negócios, originários de diversas organizações governamentais de inteligência, encontraram nelas um ambiente favorável às suas aptidões profissionais de inteligência para coletar e processar as informações de forma ética e legal. Os conceitos de inteligência que por muitos anos sustentaram as estratégias militares, agora poderiam ser utilizados para obter significativa vantagem competitiva em seus campos de operação. (GOMES; BRAGA, 2004, PRESCOTT; MILLER, 2002).

O sucesso econômico de um país depende da sua capacidade de aplicar atividades inovadoras que criam uma vantagem competitiva em um ambiente de transformação (VILLELA; MAGACHO, 2009). A IC tem sido reconhecida como uma ferramenta de gestão estratégica que poderia aumentar a vantagem competitiva (CANONGIA, 2004).

A estratégia competitiva envolve o posicionamento de um negócio para maximizar o valor das capacidades que distinguem a organização de seus concorrentes, ou seja, um aspecto central na formulação estratégica é a análise de percepção dos concorrentes (DRUCKER, 1998; PORTER, 2004). Nesse contexto, a transformação dos dados em informação está em conhecimento ou inteligência que são fatores críticos para o sucesso das organizações. A sobrevivência e o crescimento de uma organização muitas vezes dependem das informações precisas e atualizadas que ela tem sobre os seus concorrentes, e um plano para usar essas informações a seu favor (MCGONAGLE; VELLA, 1990; COELHO et al. 2006).

Fitzpatrick e Burke (2003) definem IC como sendo a aquisição de informações relevantes, de uma forma legal e ética sobre o ambiente corporativo. Por sua vez Combs (1992) define como um processo de análise do posicionamento, desempenho, potencialidades e intenções estratégicas dos concorrentes e transforma estas informações em conhecimento estratégico. Para Brody (2008) não existe uma definição única para IC, geralmente é visto como o processo pelo qual as organizações reúnem informações acionáveis sobre os concorrentes e ao ambiente competitivo, e idealmente aplicá-la a seus

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

processos de planejamento e tomada de decisões, a fim de melhorar o desempenho da empresa.

Apesar de pequenas variações, a função da IC é entendida pelos vários estudiosos de forma bastante uníssona, como sendo o processo de coleta, análise e distribuição de informações legal e eticamente obtidas, relativas ao entorno competitivo e de comportamento do consumidor com o objetivo de sustentar os processos decisórios nas organizações (FULD, 1995; RODRIGUES; RICCARDI, 2007; PRESCOT; MILLER, 2002; COMBS, 1992).

Além disso, a IC é a produção de conhecimento acionável para a melhoria da ação da estratégia corporativa (PORTER, 2004; BERGERON; HILLER, 2002; COMBS, 1992), um componente de inteligência que visa ganhar vantagem estratégica. Xua et al. (2014) aponta a gestão de informações estratégicas como uma fonte vital para a empresa.

Malhotra (1993) descreve com base nas necessidades da IC, que dados relevantes podem ser obtidos de forma ética podendo ser através de clientes, materiais promocionais dos concorrentes, análises de produtos, relatórios anuais dos concorrentes, feiras e distribuidores. A IC deve ser uma atividade legal e respeitar os códigos de ética, envolvendo a transferência de conhecimentos do ambiente para a organização dentro das regras estabelecidas (ROUACH; SANTI, 2001).

2.2 Espionagem Industrial

A espionagem não é uma atividade moderna ou recente. Considera-se que o primeiro espião industrial tenha sido o homem pré-histórico que desejou saber como os membros da tribo vizinha conseguiam produzir o fogo (SAHELI; GRISI, 2001). Também exemplo de Boulton e Watt em 1776 estavam cientes de que espiões tentaram roubar seus segredos no início à introdução da máquina a vapor (BIRCH, 1995).

A IE é definida como uma tentativa por parte dos governos ou indústrias em adquirir informações classificadas com não públicas (PRESCOTT; MILLER, 2002).

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

Da mesma forma, o Serviço de Inteligência de Segurança Canadense, definiu espionagem econômica como "qualquer ação que pode ser descrita como ilegal clandestina ou coercitiva por um governo estrangeiro, a fim de obter acesso não autorizado há informações com pretensão de obter vantagem econômica" (CSIS / SCRS, 2001). Por sua vez Crane, (2005) define EI como o acesso a informação confidencial sem obter a aprovação por parte do titular da informação.

Cada negócio prospera em informação, seus maiores efeitos são para aperfeiçoar o projeto de produtos ou serviços, para obter o direito de preços na compra de materiais, para recrutar a melhor equipe, e fazer o melhor uso de instrumentos financeiros. A EI é entendida como uma extensão dessa necessidade básica, o uso de métodos secretos para obter informações que se acredita que não pode ser encontrado abertamente (SOMMER,1993)

Não importa qual a atividade ou porte da empresa, todas possuem informações exclusivas, dados que ajudam aumentar as receitas ou lucros. A organização pode ter gasto pouco ou nenhum dinheiro, ou esforço na obtenção das informações pode até mesmo tê-la descoberta por acidente, no entanto são de propriedade particular, e dá-lhe uma vantagem sobre seus concorrentes (KAPERONIS, 1984). Nem todas as empresas estão cientes disso, muitas delas sofrem espionagem sem ter percebido (JONES, 2008).

No atual cenário em que as empresas estão inseridas, em um mercado competitivo e altamente dinâmico no qual a tecnologia influencia os resultados econômicos, faz-se necessário zelar pelo patrimônio, tendo em vista a permanência de suas atividades no mercado. A EI traz alguns elementos negativos para a empresa tais como: multas pesadas, perda de propriedade intelectual e até o declínio dos preços das ações (SCULLY, 2013). É difícil colocar um valor sobre o custo do ataque (JONES, 2008), os custos de uma fuga de informação são altos, podendo ter um maior impacto quando se trata de tecnologia (CRAWFORD; SOBEL, 1982). Após a empresa sofrer espionagem, mesmo que ela consiga impedir a utilização das informações por terceiros, ainda assim o proprietário original pode sofrer danos significativos, mesmo que o uso exclusivo dos ativos é devolvido (BRENNER, 2001)

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

Dentre vários métodos de coleta de informações na espionagem o mais utilizado é o recrutamento de pessoas que tem acesso à informação (empregados, consultores, estudantes, etc.) (CANADIAN SECURITY INTELLIGENCE SERVICE, 2001). No entanto Crane (2005) inclui outros métodos como: arrombamento, fotocópias, recuperação de lixo e de intercepção de comunicações. Littlejohn (1994) menciona que muita da espionagem sofrida pelas empresas se da pela a exposição acidental, geralmente devido à negligência dos funcionários, ignorância ou descuido, por exemplo, deixando os dados confidenciais em sua mesa durante um intervalo de descanso, ou não especificar cláusulas de não divulgação das informações ao assinar acordos estratégicos como o licenciamento ou fusões. Além de todos os velhos métodos estabelecidos, uma das técnicas que está sendo utilizada atualmente são o roubo de laptops e outros computadores (JONES, 2008).

A fronteira entre a pesquisa de informações e a espionagem é incerta, e certamente dependente do ambiente sociocultural em que as unidades econômicas estão inseridas. Um exemplo prático mencionado por Saheli e Grisi (2001), quando olhado para dentro de uma casa onde tem suas janelas escancaradas pode ser deselegante, mas não proibido. Porém se esconder para tentar fotografar as pessoas que estão dentro desta, pode ser considerado invasão de privacidade. Pode-se argumentar, que nem todos os meios de coletas de informações são aceitáveis no contexto competitivo, afinal concorrentes são tipicamente vistos como estando em uma batalha de soma zero (SAHELI; GRISI, 2001).

A diferença entre IC e EI é que, a primeira é a análise, organização e distribuição de informações legalmente disponíveis úteis para o formulador de políticas, no outro lado, a espionagem corporativa é roubar segredos (COSKUN; JACOBS, 2003). Um exemplo citado por Moreira (1999) é que a diferenciação de pesquisa de mercado e a espionagem é considerar que esta última começa quando as informações a serem coletadas sobre os concorrentes não estão disponíveis publicamente, isto é, o concorrente não deseja revelá-las.

Há alguns limites para a coleta de informações, normalmente espera-se a lei para determinar o limite entre a prática aceitável e inaceitável, mas com o rápido avanço das informações e das tecnologias de comunicação, bem como a crescente profissionalização

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

do competitivo setor de inteligência, os limites legais não são sempre claros como se poderia esperar (CRANE, 2005; JONES, 2008).

De fato as questões éticas nos negócios normalmente entram em jogo quando a lei é incapaz para definir tais limites (CRANE, 2005; FINDER, 2006). Os gestores devem construir compromisso com os códigos e valores éticos, ativamente discutir o que constitui informação questionável, reunir e premiar práticas éticas quando ocorrer. Ao apoiar um sistema competitivo que respeita os princípios da moralidade, apoiará a vitalidade da empresa e a própria vitalidade do sistema competitivo (PAINE, 1993).

2.3 Contra-Espionagem Industrial

O termo contra-espionagem descreve os passos de uma organização para proteger as informações procuradas por coletores de inteligência hostis. Uma das medidas de contra-inteligência mais eficazes é definir as informações secretas relevantes para a empresa e controlar a sua disseminação (CALOF, 1996).

O espaço corporativo está cercado de ameaças que vão desde a sabotagem e espionagem até a guerra de informações, o grande problema é que os gestores possuem um grande conhecimento sobre processo produtivo, mercado, cliente, mas na parte de segurança não possuem conhecimento nenhum, até acham que espionagem não existe, acham que é um tema de guerra fria, com essa falta de percepção e em um ambiente pacífico de competição econômica que a EI se torna mais proveitosa (BEAL, 2005).

A gestão de negócios tem a responsabilidade de forma adequada de proteger os segredos comerciais, através da utilização de práticas de segurança, classificando e controlando documentos sensíveis, restringir a distribuição de informações confidenciais, realizando treinamento em segurança e proporcionando segurança física adequada (SCHUTTZ; COLLISS, 1994).

Os recursos humanos é uma das principais brechas para espionagem industrial. Por isso é de extrema importância que os gestores de recursos humanos compreendam a importância da segurança das informações, ao contrário ele não vai transmitir a mensagem adequada aos colaboradores (PHILLIP; WRIGHT, 1999; BEAL, 2005). Além disso,

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

qualquer programa de segurança da informação, mesmo com o total apoio da alta administração, não pode ser bem sucedido se todos os funcionários não se comprometerem integralmente (PHILLIP; WRIGHT, 1999). Por isso, pessoas altamente qualificadas para auxiliar a organização na definição das medidas de segurança da informação e contra-inteligência deverão ser utilizadas (RODRIGUES; RISCAROLLI; ALMEIDA, 2011). O ponto mais importante para atuação eficaz da contra-espionagem é o desenvolvimento de uma mentalidade de segurança onde saiba a importância da proteção e os riscos das informações no ambiente corporativo (WOOD, 1994).

A contra-espionagem pode ser encarada como uma atitude de defesa passiva, quando tenta simplesmente, proteger as informações estratégicas. Pode ainda ser uma defesa ativa quando tenta desinformar, iludir, enganar, levar o adversário a erro de julgamento, através de planejamento meticuloso (SAHELI ; GRISI, 2001).

O *Canadian Security Intelligence Service* (serviço de Inteligência Canadense) desenvolveu um programa de conscientização em organizações públicas e privadas, para defender o país da espionagem e de outras ameaças contra interesses comerciais. Da mesma forma a estrutura de Contra-Inteligência do *Federal Bureau of Investigation* (FBI), além de exercer sua missão de segurança nacional nos EUA, implementou o programa *Awareneness of National Security Issuesand Response* (ANSIR), com o objetivo de proteger informações governamentais contra ameaças potenciais, bem como reduzir a vulnerabilidade de segurança em organizações Americanas (BALUÉ; NASCIMENTO, 2006).

O impacto da globalização mundial aproxima os mercados mundiais, pois cria um fluxo de tecnologia, fluxo de informação, e os fluxos de capital através do ciberespaço. Estes fluxos não só aumenta a consciência de novos produtos, novos desenvolvimentos, e as novas tecnologias, mas também obriga muitas empresas a se protegerem, quando competem com empresas mundiais, essas empresas não têm os recursos ou algumas vezes, até mesmo a visão para neutralizar as ameaças da globalização assim, elas podem estar propensas a recorrer à EI (COSKUN; JACOBS, 2003).

Scully (2013) faz um estudo em uma das áreas mais frágeis a roubo de informações atualmente: o espaço cibernético. Segundo o autor, grande parte dos dados importantes ou

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva ISSN: 2236-210X

negócio da empresa está armazenado em computadores, por isso as organizações dependem da confiabilidade de seus sistemas baseados em tecnologia da informação, se a confiança nesses dados for destruída, o impacto pode ser comparável à própria destruição da empresa (BEAL, 2005). Isso pode significar que empresas devem ter uma disposição contra-espionagem em suas estratégias, estudos indicam que muitas empresas, no entanto, não têm quaisquer preventivas de estratégias contra-espionagem (COSKUN; JACOBS, 2003; BEAL, 2005).

Cabe a administração de segurança interna e práticas devem prevenir ou minimizar exposições de segurança e garantirá integridade dos dados e sistemas informáticos. A lista não pode ser exaustiva, combater a EI não pode ser somente esporadicamente, deve ser contínuo, em constante evolução e análise (KAPERONIS, 1984).

A aplicação da lei não provou ser eficaz na redução da frequência da espionagem econômica (SNYDER; CRESCENZI, 2009). Os autores mencionam que embora os estatutos têm proporcionado melhorias e recursos legais em casos de roubo de IC, são claramente insuficientes para controlar o florescimento da espionagem industrial, isso realmente deixa apenas uma variável para controlar o problema, a prevenção voluntária.

Shanley e Crabb (1998) descrevem alguns controles internos que podem ser postos em prática na organização e que poderão ser de enorme utilidade para prevenção da EI: (i) remover todos os computadores, impressoras e aparelhos de fax de áreas de trabalho comuns; (ii) documentos importantes devem ser evitados deixar sobre mesas;(iii) todos os terminais devem ter protetores de tela protegida por senha; (iv) acesso hierárquico deve ser utilizado pelo uso da identificação com código de cores emblemas; (v) controle em todas as partes da organização por câmeras de segurança; (vi) estagiários e estudantes pesquisadores de pós-graduação também deve assinar acordos legais.

3 METODOLOGIA

O método de pesquisa utilizado no desenvolvimento da presente pesquisa é baseado nas proposições de Vergara (1997) e Roesch (1999), referente aos estudos de natureza

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

qualitativa, sendo caracterizada como uma pesquisa exploratória. No que tange ao estudo para o tratamento de dados optou-se pelo mapa de associação de idéias (SPINK; LIMA, 2000).

Os estudos exploratórios são utilizados em área na qual há pouco conhecimento acumulado e sistematizado (VERGARA, 1997). A pesquisa qualitativa é considerada apropriada para a avaliação formativa, quando se trata de melhorar a efetividade de um programa ou plano, ou mesmo quando é o caso da proposição de planos (ROESCH, 1999), pois a ênfase do trabalho refere-se saber qual a percepção, preocupação dos gestores e formas de prevenções que as organizações estão tendo com a EI.

O instrumento de coleta de dados (questionário de pesquisa), foi elaborado com questões abertas, que é ideal nas pesquisas qualitativas (ROESCH, 1999). Depois de estruturado o questionário passou por uma validação de conteúdo com três *experts* da área (MALHOTRA; BIRKS; WILLS, 2012). Após esta validação, tal instrumento foi submetido a um pré-teste, para verificar se as questões eram compreensíveis (Roesch, 1999). Posteriormente a coleta de dados foi realizada por meio de correspondência eletrônica, enviando os questionários para os gestores das empresas. Foram enviados um total de 80 questionários obtendo 10 respondidos.

Para a análise foi seguido à indicação de Spink e Lima (2000), utilizando o método mapa de associação de ideias que têm como objetivo de sistematizar o processo de análise das práticas discursivas em busca de aspectos formais da construção lingüística, dos repertórios utilizados nessa construção e da dialógica implícita na produção de sentidos. Constituem instrumentos de visualização que têm duplo objetivo: dar subsídios ao processo de interpretação e facilitar a comunicação dos passos subjacentes ao processo interpretativo (SPINK; LIMA, 2000). Por sua vez, Vergara (2009) menciona que a utilização de mapas de associação de ideias consiste em uma forma de análise de dados em estado bruto, organizados em blocos que representam as categorias temáticas escolhidas pelo pesquisador. Os dados são apresentados, sem fragmentação, na sequência em que são coletados.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

O objeto de estudo, no caso, empresas pertencentes ao ramo moveleiro, justifica-se, pois o setor pesquisado pertence ao Município de Bento Gonçalves, estado do Rio Grande do Sul é considerado um dos maiores polos moveleiro do estado, possuindo 12%, da representatividade do setor no estado, empregando 8.416 mil pessoas. O município possui 300 empresas no setor moveleiro enquanto no estado existem 2.470 e se tratando de Brasil existem 17.500 empresas, segundo dados da revista Panorama Socioeconômico Município de Bento Gonçalves (2013).

Quadro 1- Caracterização dos respondentes e da empresa

Em-presa	Tempo de empresa do respondente (Anos)	Cargo do respondente	Quantidade de funcionário da organização	Porte da empresa segundo critérios SEBRAE
1	4	Gerente comercial	Até 19	Pequena
2	8	Gerente	Até 19	
3	16	Gerente	Até 19	
5	4	Gerente Comercial	Até 19	
5	4	Gerente de vendas	Até 19	
6	5	Gerente Sócio	Até 19	
7	19	Diretora Financeira	100 a 499	Média
8	12	Supervisor Financeiro	100 a 499	
9	3,5	Gerente Comercial	100 a 499	
10	13	Gerente Comercial e Exportação	Acima de 500	Grande

Fonte: Elaborado pelos autores.

4 ANÁLISE DOS DADOS

A análise busca introduzir os dados empíricos existentes e analisá-los por meio do método Mapa de Associação de Ideias, com objetivo de gerar resultados que permitam responder à pergunta inicial do estudo. Conforme Spink e Lima (2000) o método Mapas de Associação de Idéias não é uma técnica fechada, dessa forma inicialmente são escolhidas categorias teóricas, que refletem os objetivos da pesquisa e, o próprio processo de análise

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

pode levar à definição das categorias. Conforme os critérios de escolhas as categorias são: Percepção dos gestores, proteção das informações, tipos de proteção e cada categoria são analisados por mapas que foram divididos pelo do porte da empresa.

4.1 Empresas de Pequeno Porte

Foram entrevistados seis gestores, de empresas com até 19 funcionários, no qual pode se observar que todos os gestores possuem um razoável entendimento sobre EI, mas na questão referente à proteção de suas informações, dos seis gestores entrevistados apenas dois protegem algumas de suas informações, aquelas que em sua visão são as mais importantes. Dois gestores mencionam que por se tratar de uma pequena empresa, não existem informações relevantes que devem ser protegidas, o fato é que a espionagem não são somente em grandes empresas elas acontecem também em pequenas organizações (SCULLY, 2013). Segundo Kaperonis (1984) independente do negócio, quando ele está gerando lucro sempre vai ter alguém querendo obter suas informações para saber como conseguir o mesmo êxito.

Os gestores entrevistados em suas maiorias não têm percepção alguma sob suas informações, apenas 50% deles têm a noção do que pode acontecer com a organização em um possível vazamento de informações. Segundo o autor (SCULLY, 2013) a espionagem pode trazer um grande prejuízo, desde multas pesadas, perda de propriedade intelectual e declínio dos preços das ações, é difícil colocar um valor sobre o custo deste tipo de ataque

(JONES, 2008). Ainda Brenner (2001) complementa que mesmo a empresa conseguindo impedir a utilização das informações roubadas, ela pode sofrer danos significativos.

Todos os gestores entrevistados não têm o conhecimento das leis referente à EI, isso pode dificultar até mesmo nas suas próprias ações de coletas de informações, pode às vezes acabar ultrapassando a linha da coleta legal das informações, e acabar tornando uma espionagem. Os resultados apontam, que para os gestores a prevenção contra-espionagem industrial, não tem importância para a sua empresa.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

Os dados demonstram que nenhuma empresa possui código de ética e conduta com as informações, e não passam instruções para os colaboradores terem cuidado com as informações. Wood, (1994) menciona que para um programa de segurança da informação dar certo precisara do apoio da alta administração.

Segundo Sommer (1993), existem algumas razões para a realização da EI e uma delas é roubar informações dos concorrentes sobre seus clientes, para aumentar sua lista de clientes, no entanto pode ser verificado na pesquisa que todas as empresas possuem banco de dados de clientes e que apenas uma delas tem proteção desses dados.

O espaço cibernético atualmente é uma das áreas mais frágeis a roubo de informações (SCULLY, 2013), no entanto, verificou-se que todas as empresas pesquisadas possuem tecnologia da informação, e de alguma maneira fazem a proteção desses dados, apenas uma não tem proteção nenhuma.

Shanley e Crabb (1998) descrevem que uma das proteções básicas que uma empresa deve ter é o monitoramento por câmeras em sua área física, podemos verificar que algumas empresas pesquisadas possuem monitoramento por câmeras em toda sua área de produção e inclusive algumas na parte administrativa, somente duas empresas das seis pesquisadas não possuem monitoramento por câmeras.

Na questão referente à segurança de visitas de pessoas estranhas nas dependências da empresa, apenas três possuem normas de segurança, o restante não tem nenhuma proteção.

Quadro 1: Mapa associação de ideias - PEQUENAS EMPRESAS

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

	Mapa associação de ideias - PEQUENAS EMPRESAS	E1	E2	E3	E4	E5	E6
PERCEPÇÃO DOS GESTORES	Quais os cuidados que você toma com as informações?	Nenhuma.	Não tem proteção pois a empresa é pequena	Cuidados com invasões do sistema.	Acharmos que por ser pequeno porte não há necessidade	Nenhuma.	Protegemos somente informações sobre os valores.
	Você tem conhecimento das consequências que o vazamento de uma informação pode causar para a empresa?	Não	Não	Sim	Não paramos para pensar sobre o assunto.	Não	Não
	Os gestores têm o conhecimento das leis referente à espionagem industrial?	Não	Não	Não	Não	Não	Não
	Sendo (1) o mínimo e (10) o máximo, na sua percepção, a prevenção da espionagem industrial tem alguma importância para a sua organização?	5	7	7	8	5	6
PROTEÇÃO DA INFOR-MAÇÃO	Existe algum treinamento ou instruções para os colaboradores terem cuidado com as informações?	Não.	Não.	Não.	Não.	Não.	Nenhuma.
	Existe algum código de ética/conduta que envolva cuidados em relação a informações?	Não.	Não.	Não.	Não.	Não.	Não.
	Os produtos criados pela empresa são patenteados?	Não.	Não.	Não.	Não.	Não.	Não.
TIPO DE PROTEÇÃO	A empresa mantém banco de dados de clientes? Se sim, como a empresa protege esse banco?	Sim. Nem todos os funcionários do administrativo tem acesso.	Sim. Mas não protege.	Sim, ele é protegido com um sistema de proteção de dados.	Mantemos um banco de dados, mas não é protegido.	Sim, sem proteção.	Sim. Não protegemos.
	A empresa possui tecnologia da informação? Possui alguma proteção?	Sim, somente pessoas que possuem a senha.	Sim. Somente antivírus.	Sim, temos um servidor com um software.	Sistema e antivírus e é feito *Backup* diário das informações do sistema.	Sim sistema de cadastro. Segurança somente com senha.	Sim, mas nenhuma proteção.
	A empresa tem monitoramento por câmaras, ou por outros meios eletrônicos em toda a sua área industrial inclusive na parte administrativa?	Sim em toda a empresa.	Somente área externa	Não.	Sim, a empresa é totalmente monitorada.	Não.	Sim, somente na parte industrial.
	Existe alguma norma de segurança quando pessoas visitam a empresa?	Não	Não	Sim	Sim, somente convidados e com procedências.	Não	Sim, somente na parte industrial.

Fonte: Elaborado pelos autores.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

4.2 EMPRESAS DE MÉDIO PORTE

Foram entrevistados três gestores de empresas até 499 funcionários, conforme no mapa 1 todos os gestores possuem algum conhecimento sobre EI, já na questão de proteção que os gestores têm sobre as informações ao contrário do mapa 1, todos os gestores entrevistados no mapa 2 possuem proteção sob suas informações e ainda sabem as consequências que o vazamento das informações podem causar, consequentemente os gestores levam em consideração a importância da prevenção da EI na organização.

Outro fator em comum entre os dois mapas analisados, é que todos os gestores não têm conhecimento sobre as leis referentes à EI. Os dados demonstram que todas as empresas pesquisadas possuem código de ética e conduta em relação às informações, mas apenas uma das três empresas oferece treinamento e instruções para os colaboradores terem cuidado com as informações.

Todas as empresas têm bancos de dados de clientes e tecnologia da informação com total proteção. Também possuem monitoramento por câmaras de segurança, inclusive uma das empresas tem acesso online. Shanley e Crabb (1998) mencionam que uma das medidas que podem amenizar o roubo de informações é o monitoramento por câmeras, em todas as áreas da empresa.

Na questão de normas de segurança para visitação, todas as empresas são bem rigorosas e estão preocupadas com o acesso de pessoas estranhas em suas áreas físicas, portanto possuem algum tipo de norma e segurança nesta área.

Quadro 2: Mapa de associação de ideias - MÉDIAS EMPRESAS

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

	Mapa de associação de ideias - MÉDIAS EMPRESAS	E7	E8	E9
PERCEPÇÃO DOS GESTORES	Quais os cuidados que você toma com as informações?	Controles específicos e senhas para o acesso a determinadas informações, assim como o controle de rastreamento de acessos.	Existe algumas informações que são restritas.	Algumas informações temos cuidados.
	Você tem conhecimento das consequências que o vazamento de uma informação pode causar para a empresa?	Olha se pensarmos assim realmente não teríamos mais nem empresa, pois tudo é um risco.	Algumas sim.	Algumas.
	Os gestores têm o conhecimento das leis referente à espionagem industrial?	Temos pouco conhecimento referente estas leis, isto não é o nosso foco,	Não	Sim
	Sendo (1) o mínimo e (10) o máximo, na sua percepção, a prevenção da espionagem industrial tem alguma importância para a sua organização?	7	8	9
PROTEÇÃO DA INFOR-MAÇÃO	Existe algum treinamento ou instruções para os colaboradores terem cuidado com as informações?	Sim. Na contratação já é feita uma triagem, são utilizadas entrevistas com psicólogas para buscar informações para avaliar os princípios, o caráter. As pessoas que entram passam pela integração, onde além do treinamento são passados os valores pelo qual a empresa norteia suas ações, assim como o perfil de comportamento que se espera de cada um, suas obrigações, seus direitos e também o cuidado como uso das informações que são pertinentes a empresa.	Não.	Sim.
	Existe algum código de ética/conduta que envolva cuidados em relação a informações?	Nada assinado, apenas verbal	SIM	SIM
	Os produtos criados pela empresa são patenteados?	Alguns sim, outros não.	Algumas.	Sim.
TIPO DE PROTEÇÃO	A empresa mantém banco de dados de clientes? Se sim, como a empresa protege esse banco?	Sim temos banco de dados de clientes, caso contrário não teríamos como trabalhar. Proteção através de restrições de uso e senhas individuais.	Sim, somente pessoas autorizadas tem acesso.	Sim, protegemos com senhas.
	A empresa possui tecnologia da informação? Possui alguma proteção?	Sim, a empresa tem perfil para controle e acesso das informações personalizadas.	Sim, existe proteção através de senhas e antivírus.	Sim.
	A empresa tem monitoramento por câmaras, ou por outros meios eletrônicos em toda a sua área industrial inclusive na parte administrativa?	A empresa possui monitoramento por câmaras na área industrial e também na área administrativa, as quais podem ser acessadas online, por pessoas específicas, com senhas individualizadas, em qualquer momento e as imagens gravadas por um bom tempo.	Sim, inclusive na parte administrativa.	Sim.
	Existe alguma norma de segurança quando pessoas visitam a empresa?	Todas as visitas monitoras e acompanhadas. Também solicitamos dados prévios das pessoas que nos visitam para a busca de informações.	Sim , somente em áreas autorizadas.	Sim.

Fonte: Elaborado pelos autores

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

4.3 EMPRESAS DE GRANDE PORTE

Foi entrevistado apenas um gestor de uma empresa com mais de 500 funcionários, e verificou-se que ele tem entendimento sobre espionagem industrial. Também identificou-se semelhança com os gestores dos mapas anteriores, o gestor também possui cuidados com suas informações, outro fator igual ao mapa 2 refere-se ao entendimento da importância da proteção das informações da organização.Um ponto negativo em comum aos outros mapas é que o gestor não tem entendimento das leis sobre espionagem industrial, conforme mostra o Quadro 3.

Quadro 3: Mapa de associação de ideias - GRANDE EMPRESA

		E10
PERCEPÇÃO DOS GESTORES	Quais os cuidados que você toma com as informações?	A empresa possui um código de ética e conduta contrato de confiabilidade, restrições ao acesso de informações a pessoas não autorizadas, restrições ao envio e copia de documentos.
	Você tem conhecimento das consequências que o vazamento de uma informação pode causar para a empresa?	Não
	Os gestores têm o conhecimento das leis referente à espionagem industrial?	Não
	Sendo (1) o mínimo e (10) o máximo, na sua percepção, a prevenção da espionagem industrial tem alguma importância para a sua organização?	8
PROTEÇÃO DA INFOR-MAÇÃO	Existe algum treinamento ou instruções para os colaboradores terem cuidado com as informações?	No momento da contratação sim, código de ética e conduta, a melhorar.
	Existe algum código de ética/conduta que envolva cuidados em relação a informações?	Sim
	Os produtos criados pela empresa são patenteados?	A maior parte sim
TIPO DE PROTEÇÃO	A empresa mantém banco de dados de clientes? Se sim, como a empresa protege esse banco?	Possui, acesso restrito a um numero limitado de pessoas e monitoramento deste acesso.
	A empresa possui tecnologia da informação? Possui alguma proteção?	Sim, TI e proteção.
	A empresa tem monitoramento por câmaras, ou por outros meios eletrônicos em toda a sua área industrial inclusive na parte administrativa?	Possui mas não em todos os cantos, mas tem sim na área administrativa.
	Existe alguma norma de segurança quando pessoas visitam a empresa?	Sim, áreas restritas para fotografar e áreas administrativas.

Fonte: Elaborado pelos autores.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

Percebe-se que na contratação dos colaboradores a empresa oferece treinamento, instruções mostrando que a empresa tem código de ética e conduta com as informações. Na questão referente aos tipos de segurança, a empresa tem um grande cuidado com os bancos de dados, possui acesso restrito há um numero limitado de pessoas, possui também proteção no sistema da tecnologia de informação e monitoramento por câmeras, incluindo a área administrativa, mas em alguns pontos da empresa não possui monitoramento.

E por fim a empresa possui normas de segurança em visitas, tais como: visitas somente em áreas restritas e fotografar somente em local permitido.

5 DISCUSSÃO E CONSIDERAÇÕS FINAIS

Através da análise dos dados podemos verificar que todos os gestores possuem um entendimento razoável sobre EI, e a grande maioria deles protegem suas informações. Mas se compararmos por mapas, podemos verificar que o mapa 1 somente dois gestores protegem suas informações, nos mapas 2 e 3 onde foram analisadas empresas de médio e grande porte, todos os gestores tem proteção de suas informações. Outra comparação que podemos fazer é sobre a nota que os gestores deram perante sua percepção sobre a importância da proteção das informações, observou-se grande diferença em comparação aos mapas, onde o mapa 1 em média foi 6.3, já o mapa 2 e 3 a média foi 8.0, pode-se verificar que quanto maior o porte da empresa maior a média de percepção do gestor.

Um fator negativo de muita importância, que passa despercebido pelos gestores, é o conhecimento das leis sobre espionagem industrial, nenhum gestor possui o conhecimento. Outro ponto que chamou a atenção é que todas as empresas do mapa 1 não possuem código de ética e moral, e muito menos treinamento e instruções para os colaboradores terem cuidados com as informações.

Em comum é que todas as empresas têm banco de dados, mas comparando os mapas pode ser verificado que quatro das seis empresas do mapa 1 não possui proteção sobre esses dados, as do mapa 2 e 3 todas possuem proteção.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

Todas as empresas pesquisadas possuem tecnologia de informação, e apenas uma das empresas não tem nenhuma proteção sobre a tecnologia da informação, ainda foi identificado que todas as empresas possuem câmeras de monitoramentos, algumas somente em alguns pontos da empresa e outras em todos os departamentos incluindo a parte administrativa. Referente à questão de segurança em visitações na empresa, apenas três empresas do mapa 1 possui normas de segurança o restante não possui, nos mapas 2 e 3 todas tem normas de segurança na visitação.

De maneira geral, os resultados encontrados apontam que o porte das empresas tem uma grande influência na percepção dos gestores sobre a importância da proteção das informações e nas próprias práticas de proteção, nas empresas maiores a percepção e proteção dos gestores perante as informações é maior. Dois dos gestores entrevistados do mapa 1 demonstraram que por se tratar de empresa de pequeno porte não há necessidade de proteção das informações, justificam que não existe procura por informações em empresas de pequeno porte.

Um ponto importante para que a contra-espionagem seja eficaz é o desenvolvimento da mentalidade de segurança dos gestores, para que saiba a importância da proteção e os riscos das informações no ambiente corporativo, conforme os dados apresentados os gestores das pequenas empresas não estão observando a importância da proteção das informações no mundo atual, pois elas podem ser um grande diferencial competitivo para a empresa, independente do tamanho do negócio ou atividade, sempre vai ter informações que seus concorrentes estão interessados em adquiri-las.

Outro resultado encontrado foi, quando os gestores possuem um entendimento sobre a importância das informações, ele acaba percebendo que é preciso ter uma melhor proteção dessas informações e que ela é importante para a empresa.

A partir da pesquisa realizada foi possível identificar que os gestores de pequenas empresas entrevistadas não tem a percepção da importância da prevenção do roubo das informações e consequentemente não tomam medidas de prevenção do roubo das mesmas.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

Já as empresas de médio porte e grande porte os gestores tem a percepção da importância da proteção das informações e estão tomando medidas de prevenção, mas em alguns aspectos ainda necessitam de algumas melhorias.

PROTECTION OF INFORMATION AND COMPETITIVE INTELLIGENCE: A STUDY ON THE PERCEPTION AND INFORMATION SECURITY IN FURNITURE SECTOR COMPANIES GAÚCHA SERRA

ABSTRACT

In a competitive scenario, knowledge and information can be considered as key resources for competitive advantage of organizations. Nevertheless the volume of information available provided by technology can create advantage for use of the information in business although it can also be the target of imitation attempts and promote competitors. Therefore, companies are experiencing a moment of valuation of trade secrets where, as important as the collection of information, is the protection of this information. This study aimed to investigate the perception of manager's information security in organizations and the protective measures taken against industrial espionage. To reach the aim, was conducted an qualitative exploratory research with managers of small, medium and large companies in the furniture industry of Serra Gaucha, in Rio Grande do Sul. For data analysis was used maps association of ideas technique. The results indicate that according to the perception of managers the protections of corporate information are associated with the size of the company.

Palavras-chave: Competitive Intelligence. Protection of information. Industrial espionage.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

REFERÊNCIAS

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 1995. Disponível em: <http://fas.org/irp/ops/ci/docs/fecie_fy00.pdf>. Acesso em: 11 jun. 2014.

BALUÉ G. I; NASCIMENTO O. S. M. Proteção do Conhecimento: Uma Questão de Contra-Inteligência de Estado. **Revista Brasileira de Inteligência**. v. 2, n. 3, 2006.

BEAL, A. Segurança da Informação: **princípios e melhores práticas para a proteção dos ativos de informação nas organizações** – São Paulo: Atlas, 2005.

BERGERON, P. E; HILLER, C. A. Inteligência Competitiva, **Revisão Anual de Informações Ciência e Tecnologia**. v. 36, p. 353-390, 2002.

BIRCH, A. Foreign observers of the british iron industry during the eighteenth century. **Journal of Economic History**. v. 15, p. 23-33, 1995.

BRENNER, S. W. 'Is there such a thing as 'Virtual Crime'? **California Criminal Law Review**, v. 4, p. 105-111, 2001.

BRODY, R. Issues in defining competitive intelligence: an exploration. **Journal of Competitive Intelligence and Management**, v. 4, p. 3-16, 2008.

CALOF, L. **What's your competitive intelligence quotient**, unpublished Conference Report, p. 4-7 1996.

CANADIAN SECURITY And INTELLIGENCE COMMUNITY: **Her Majesty the Queen in Right of Canada**, 2001. Disponível em: https://www.csis-scrs.gc.ca/index-en.php. Acesso em: 23 out. 2014.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

CANONGIA, C; PEREIRA, M. N. F.; MENDES, C. U. S.; ANTUNES, A. M. S. Mapeamento de inteligência competitiva e de gestão do conhecimento no setor saúde. Encontros Bibli: **Revista Eletrônica de Biblioteconomia e Ciência da Informação**. p. 78-95, 2004.

CARUSO, C. A. A.; STEFFEN, F. D. **Segurança em Informática e de Informações** – São Paulo: Editora SENAC São Paulo, 1999.

COELHO, G. M.; DOU, H.; QUONIAM, L.; SILVA, C. H. Ensino e pesquisa no campo da inteligência competitiva no Brasil e a cooperação francobrasileira. **Revista Hispana de La Inteligencia Competitiva-Puzzle**, n. 23, p. 12-19, 2006.

COMBS, R. E. The competitive intelligence handbook. **Metuchen: Scarecrow**, 1992.

CRANE, A. In the company of spies: when competitive intelligence gathering becomes industrial espionage. **Business Horizons**, v. 48, n. 3, p. 233–240, 2005.

CRAWFORD, V; SOBEL, J. **Strategic Information Transmission Econometrica**, v. 50, p. 1431–1451, 1982.

DRUCKER, R **The coming of new organization**. Harvard Business Review, p. 45-53, 1988.

FITZPATRICK, W. M; BURKE D. R.Competitive intelligence, corporate security and the virtual organization. **Advances in Competitiveness Research**, v. 11, n. 1, 2003.

FINDER, J. **The Myth of the Corporate Spy**. Forbes, v. 177, n. 12-15, p. 36, 2006.

FONTES, E. **Segurança da Informação**: o usuário faz a diferença - São Paulo: Saraiva, 2006.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

FULD, L. M. **The new competitor intelligence**: the complete resource for finding, analyzing and using information about your competitor. New York, John Wiley & Sons, 1995.

GIACOMELLO, C. P.; GEHLEN, E.; LARENTIS, F.; MATTIA, M., B. Revista Panorama Socioeconômico Bento Gonçalves-RS, 42. ed.2013.

GOMES, E.; BRAGA, F. **Inteligência competitiva**. Como transformar informação em um negócio lucrativo. 2. ed. Rio de Janeiro: Elsevier, 2004.

JONES, A. Industrial espionage in a hi-tech world. **Computer Fraud & Security**, v. 1, p. 7-13, 2008.

KAPERONIS, I. Industrial Espionage, **Computers and Security**, n. 3 v. 2, p. 117-121, 1984.

LITTLEJOHN, R. The Target Company**, Security Management**, v. 38, p. 134-41, 1994.

MALHOTRA, N. K.; BIRKS, D.; WILLS, P. **Marketing research**: applied approach. 4 th edition. New York: Pearson, 2012.

MALHOTRA, Y. An analogy to a competitive intelligence program: **Role of Measurement in Organizational Research**, 1993. Disponível em: <http://www.brint.com/papers/compint>. Acesso em: 18 jan. 2015.

McGONAGLE, J.; VELLA C. M. **Outsmarting the Competition**. Naperville (Il): Sourcebooks, 1990.

MOREIRA, J. M. A **Ética Empresarial no Brasil**. São Paulo: Pioneira, 1999.

PAINE, L. S. Corporate policy and the ethics of competitor intelligence gathering. **Ethics in Marketing**, p. 260–279, 1993.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

PRESCOTT, J. E.; MILLER, S. H. **Inteligência competitiva na prática**. Rio de Janeiro: Campus, 2002.

PHILLIP, C; WRIGHT, G. R. Industrial espionage and competitive intelligence. **Journal of Workplace Learning**, v. 11, p. 53-59, 1999.

PORTER, M. E. **Estratégia competitiva**: técnicas para análise de indústrias e da concorrência. Rio de Janeiro: Elsevier, 2004.

ROESCH, S. M. A. **Projetos de Estágios e de Pesquisa em Administração**. São Paulo, Editora Atlas, 1999.

RODRIGUES, L. C.; RICCARDI, R. Inteligência competitiva: para negócios e organizações. Maringá, PR: **Unicorpore**, 2007.

RODRIGUES L. C.; RISCAROLLI, V.; ALMEIDA, M. I. R. Inteligência competitiva no Brasil: um panorama do status e função organizacional. **Revista Inteligência Competitiva**. v. 1, n. 1, p. 63-85, 2011.

ROUACH, D; SANTI, P. Competitive intelligence adds value: five intelligence attitudes. **European Management Journal**, v. 19, n. 5, p. 552-559, 2001.

COSKUN, S. A.; JACOBS, L. Counteracting global industrial espionage: a damage control strategy. **Business and Society Review**, n. 108, v. 1, p. 95-113, 2003.

SEBRAE Observatório Internacional Sebrae. **Site institucional**. Disponível em: <http://ois.sebrae.com.br/pais/brasil/>. Acesso em: 25 maio 2014.

SCHUTTZ, A. B; COLLISS, M. M**.** The ethics of business intelligence. **Journal of Business Ethicsv**. n. 4, p. 305-314, 1994.

SCULLY, P. Under lock and key: protecting the network from attack. **Network Security**, n. 7, p. 12-15, 2013.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

SHANLEY, A; CRABB, C. Corporate espionage: no longer a hidden threat. **Chemial Engineering**. n. 105 v. 13, P. 82-96, 1998.

SNYDER, H; CRESCENZI A. Intellectual capital and economic espionage: new crimes and new protections. **Journal of Financial Crime**. v. 16, p. 245-254, 2009.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. Disponível em: http:// http://fas.org/sgp/othergov/indust. Acesso em: 11 de jun. 2014.

SOMMER, P. Computer and Industrial Espionage. **Queen Elizabeth II Conference**, London, 1993.

SPINK, M. J. P. e LIMA, H. Rigor e visibilidade: a explicitação dos passos da interpretação. In: SPINK, Mary Jane P. (org.). **Práticas discursivas e produção de sentidos no cotidiano**: aproximações teóricas e metodológicas. São Paulo: Cortez, 2000.

SAHELI, S; GRISI, C. C. H. Espionagem e ética no sistema de inteligência competitiva. In: **SEMEAD** - SEMINÁRIO EM ADMINISTRAÇÃO, 5., São Paulo: FEA-USP, 2001.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. São Paulo; Atlas, 1997.

VERGARA, S C. **Métodos de pesquisa em administração**. 3. Ed. São Paulo: Atlas, 2009.

VILLELA, T. N.; MAGACHO, L. A. M. Abordagem histórica do sistema nacional de inovação e o papel da incubadoras de empresas na interação de agentes deste sistema. **XIX Seminário Nacional de Parque Tecnológicos e Incubadoras de Empresas**. Florianópolis, SC, 26-30, 2009.

WELLNER, A. S. Spy vs. Spy. **Academic Search Premier**, v. 25, 2003.

WOOD, C. C. Fifty Ways to Secure Dial-up Connections. **Computer & Security**, v. 13, p. 209-15, 1994.

Recebido em: 05/10/2015Aprovado em:01/03/2016

Revista Inteligência Competitiva
ISSN: 2236-210X

XUA, K; LIAO, S; LI, J; SONG, Y; Salesperson competitive intelligence and performance: the role of product knowledge and sales force automation usage. **Industrial Marketing Management**, v. 43, p. 136-145, 2014.

Recebido em: 05/10/2015Aprovado em:01/03/2016