Inteligência Competitiva e Proteção de Informações: Um Estudo Sobre a Percepção dos Gestores de Empresas do Setor Moveleiro

RESUMO
Atualmente o conhecimento é considerado como o principal ativo das organizações, um fator importante para a vantagem competitiva. Com a valorização dos segredos comerciais e o volume de informações disponíveis, proporcionado pelo advento da tecnologia da informação, gerenciar de maneira eficiente as informações passou a ser um diferencial estratégico. É necessário não apenas coletar as informações, mas sim protegê-las. O estudo teve por finalidade investigar a percepção dos gestores, e as medidas de proteção que as organizações estão adotando contra a espionagem industrial. Para isso foi realizado uma pesquisa qualitativa exploratória junto aos gestores de empresas do setor moveleiro da cidade de Bento Gonçalves- RS. Para a análise e interpretação dos dados foi utilizada mapas de associação de ideias. Os resultados indicam que as variações da pesquisa, na percepção dos gestores e na proteção das informações da empresa estão associadas ao porte da empresa**.**

Palavras-chave: Espionagem industrial. Proteção das informações. Percepção dos gestores.

1 INTRODUÇÃO

Como a informação torna-se importante na economia global, algumas empresas buscam vantagem competitiva por meio da inteligência competitiva. As organizações monitoram o ambiente externo, pois nele concentram-se ameaças e oportunidades. Neste contexto, se justifica a existência de um Sistema de Inteligência Competitiva, o qual monitora e produz conhecimento estratégico relevante sobre sua posição competitiva (BERGERON; HILLER, 2002, PORTER, 1980). As empresas precisam cada vez mais buscar vantagens competitivas através de informações (CANONGIA, 2004), algumas vezes a busca por essas informações acabam passando do limite ético e moral tornando-se espionagem industrial (CRANE, 2005).

Por outro lado a espionagem é uma prática mais comum do que se imagina, no mundo corporativo, muitas empresas já sofreram espionagem sem que elas tenham se dado conta (JONES, 2008). Apesar das empresas grandes estarem envolvidas em casos de espionagem, a maior preocupação é com as pequenas e médias empresas, pois elas representam 99% do total de empresas brasileiras, segundo SEBRAE (2013), algumas delas às vezes nem sabem o risco que correm com o roubo de suas informações (SAMLI; JACOBS, 2003).

Diante desse contexto, o objetivo do estudo foi compreender a percepção que os gestores das empresas têm sobre espionagem industrial e quais práticas de prevenção contra espionagem são utilizadas, para proteger suas informações, nas indústrias do setor moveleiro da cidade de Bento Gonçalves.

Além da introdução, esse estudo está organizado na seguinte ordem, primeiro apresenta fundamentos da inteligência competitiva, espionagem industrial, e as prevenções contra espionagem, segundo momento, apresenta os procedimentos metodológicos adotados para realizar a pesquisa qualitativa, seguidamente apresenta os dados e a análise dos mesmos com base nos questionários aplicados nos gestores das empresas, e por fim apresenta as considerações finais do estudo.

2 INTELIGÊNCIA COMPETITIVA

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). Inteligência Competitiva (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 do concorrente (PORTER, 1986). 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).

Segundo os autores Fitzpatrick e Burke (2003), a definição de inteligência competitiva é a aquisição de informações relevantes, de uma forma legal e ética sobre o ambiente corporativo. Para Brody e Wright (2008) não existe uma definição única para inteligência competitiva, 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 processos de planejamento e tomada de decisões, a fim de melhorar o desempenho da empresa.

Além disso, (IC) é a produção de conhecimento acionável para a melhoria da ação da estratégia corporativa (BERGERON; HILLER, 2002) o mesmo pensamento de Porter (1980) que menciona (IC) como um componente de inteligência de negócios que visa ganhar vantagem estratégica.

Uma pesquisa da American Futures Group consultoria, segundo os autores Xua et al., (2014) indica que 82 % das grandes empresas e mais de 90 % das 500 maiores empresas da Forbes Globais adotaram (IC) para o risco de gestão e decisões.

Malhotra (1993) descreve com base nas necessidades de (IC), que dados relevantes podem ser obtido de forma ética podendo ser através de clientes, materiais promocionais do concorrente, análise de produtos do concorrente, os relatórios anuais do concorrente, feiras e distribuidores. Inteligência Competitiva 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).

3 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, 1955).

Espionagem industrial segundo **(**Annual Reportto Congresson Foreign Economic Collectionand Industrial Espionage, 1995) é definida como “uma tentativa por parte dos governos ou indústria estrangeira em adquirir informações classificadas públicas ou não públicas de empresas norte-americanas.

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 à informação econômica, como informações proprietárias ou tecnologia, para obter vantagem econômica” (CSIS / SCRS, 2001). Segundo o autor Crane, (2005) espionagem industrial é definida como o acesso a informação confidencial sem obter a aprovação por parte do titular da informação.

Para Sommer (1993) 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. Espionagem industrial 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.

Em uma pesquisa feita pela Pricewaterhouse Coopers 84% dos empresários afirmou que a informação sobre os seus concorrentes foi um fator importante no seu próprio crescimento dos lucros. Um terço confirmou que uma economia débil torna tal chamado "inteligência competitiva" mais importante do que nunca. Mas a maioria das pequenas empresas não estão conscientes de que elas têm informações que precisam ser protegidas (WELLNER, 2003).

Kaperonis (1984) menciona que não importa qual a atividade da empresa, ela pode produzir biscoito ou computadores, ambas vão ter suas receitas exclusivas, todos os dados que ajudam a vender produto, ou aumentar as suas receitas ou lucros, poderia ser considerados de sua propriedade. A organização pode ter gasto pouco ou nenhum dinheiro, ou esforço na obtenção da informação pode até mesmo tê-la descoberta por acidente, no entanto ela é particular, e dá-lhe uma vantagem sobre seus concorrentes. Esta informação é comercialmente útil e, portanto, poderia ser considerado como propriedade, isso não são geralmente conhecido mesmo em organizações grandes e pequenas, segundo o autor Jones (2008) as organizações em sua maioria, não sabem que foram espionadas.

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 espionagem industrial traz alguns elementos negativos para a organização como multas pesadas, perda de propriedade intelectual e 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, se o projeto trata de uma combinação de tecnologias e campos de aplicação que é particularmente elevado de interesse quanto à estratégia da organização. (CRAWFORD; SOBEL, 1982).

O autor Brenner (2001) relata que quando uma empresa sofre uma espionagem industrial e mesmo conseguindo 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.

É importante saber como espionagem industrial está comprometida, de modo que os pontos fracos de uma organização não podem ser isolados. O método de coleta mais utilizado é o recrutamento de alguém que tem acesso à informação (empregados, consultores, estudantes, etc.) (CSIS / SCRS, 2001). No entanto o autor Crane (2005) inclui outros métodos, arrombamento, fotocópias, recuperação de lixo e de intercepção de comunicações. Littlejohn (1994) descreve que a categoria mais freqüente é insidiosa, é 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 ao assinar acordos estratégicos como o licenciamento

ou fusões. Além de todos os velhos métodos estabelecidos, uma das técnicas que está sendo utilizado são o roubo de laptops e outros computadores (JONES, 2008).

Razões para a realização da espionagem industrial segundo o autor Sommer (1993).

a) Para ganhos econômicos, ou possivelmente injustos vantagem sobre um concorrente no negócio;
b) Obter material de pesquisa de mercado com o menor custo possível;
c) Para reduzir os custos de pesquisa e desenvolvimento, descobrindo o que já foi alcançado por outros;
d) Para adquirir a nova tecnologia com o menor custo possível;
e) Para evitar o desperdício de recursos de pesquisa e seguir as linhas que outros já encontraram o inútil;
f) Para expandir uma lista de potenciais clientes;
g) Para verificar se está pagando o menor preço possível para a sua matéria-prima;
h) Para obter os dados com os quais pode executar a análise da concorrência.

A fronteira entre a pesquisa de informações e a espionagem é incerta, e certamente dependente do ambiente sócio-cultural em que as unidades econômicas estão inseridas. Um exemplo prático que os autores Sahelie e Grisi (2001) comentam, quando olhado para dentro de uma casa que 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.

A diferença entre inteligência competitiva e espionagem corporativa 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 (SAMLI; JACOBS, 2003).

Uma forma de simples entendimento que o autor Moreira (1999) cita sobre 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 do competitivo setor de inteligência, os limites legais não são sempre claros como se poderia esperar. De fato as questões éticas nos negócios normalmente entram em jogo quando a lei é incapaz para definir tais limites Crane (2005).

Paine (1993) concluiu que 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.

5 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" (Society of Competitive Intelligence Professionals, 2007).

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 espionagem industrial se torna mais proveitosa.

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 (SCHULTZ, 1994).

Phillip e Wright (1999) colocam os recursos humanos como sendo uma das principais brechas para espionagem industrial, se o gerente de recursos humanos não compreende a importância da segurança da organização, ele não vai transmitir a mensagem adequada ao pessoal. Além disso, 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. O ponto mais importante para atuação eficaz da contra-espionagem é o desenvolvimento da mentalidade de segurança, para que 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 (GRISI; SAHELI, 2001).

Canadian Security Intelligence Service (CSIS), 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).

Samli e Jacobs (2003) descrevem que o impacto da globalização mundial vem trazendo mercados mundiais mais próximos, 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 regiões e empresas locais 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 espionagem industrial.

O autor Scully (2013) faz um estudo em uma das áreas mais frágeis a roubo de informações atualmente, o espaço cibernético e traz a opção de proteção eficaz onde abrange não apenas a segurança do servidor em repouso de criptografia, mas também incluem robusta criptografia em vôo WAN. Ao fazê-lo, as organizações podem proteger e garantir as informações críticas, estar em conformidade com a privacidade e requisitos regulamentares de confidencialidade, evitar possíveis sanções pecuniárias e exposição pública negativa, e proteger sua reputação valorizada. Isso pode significar que industriais devem ter uma disposição contra-espionagem em suas estratégias, estudos indicam que muitas empresas, no entanto, não têm quaisquer preventivas de estratégias contra-espionagem**.** (SAMLI; JACOBS, 2003).

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 espionagem industrial não pode ser somente esporadicamente, deve ser contínuo, em constante evolução e analise (KAPERONIS, 1984).

Snyder e Crescenzi (2009) relatam que aplicação da lei não provou ser eficazes na redução da freqüência de espionagem econômica. Embora estatutos, têm proporcionado melhorias, 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, prevenção voluntária.

As empresas que trabalham com produto ou serviço podem ser espionadas a qualquer momento, os autores 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 espionagem industrial.

a) Remover todos os computadores, impressoras e aparelhos de fax de áreas de trabalho comuns;
b) Documentos importantes devem ser evitados deixar sobre mesas;
c) Todos os terminais devem ter protetores de tela protegida por senha;
d) Acesso hierárquico deve ser utilizado pelo uso da identificação com código de cores emblemas;
e) Todos os fax e mensagens de internet devem ser protegidos;
f) Todos os antigos R & D e outros documentos sensíveis devem ser desfiado;
g) Contratos empregatícios devem ser sigilosos, eles devem ser abrangentes e atualizados;
h) Estagiários e estudantes pesquisadores de pós-graduação também deve assinar acordos legais;
i) Os funcionários devem ser treinados para reconhecer a diferença entre segredos comerciais e conhecimentos gerais;
j) Documentos de confidencialidade legal devem ser assinados antes de quaisquer dados confidenciais serem compartilhados nas discussões relacionadas ao licenciamento de *joint venture*, ou de pesquisa cooperativa;
k) Os aposentados da empresa não devem ter acesso aos segredos da empresa;
l) Os sistemas de segurança da planta física devem estar em boa forma e os guardas de segurança devem ser bem treinados.

Para um bom programa de proteção contra-espionagem o primeiro passo é conhecer a capacidade de inteligência do adversário, aí sim preocupar-se com a aplicação do programa de segurança, ele é fundamental para impedir que as informações venham cair em mãos dos concorrentes.

5 METODOLOGIA

Quanto aos objetivos, esta pesquisa é de natureza exploratória. De acordo com Vergara (1997), o estudo exploratório é utilizado em área na qual há pouco conhecimento acumulado e sistematizado.

Foram aplicados questionários semi-estruturados, segundo a autora Roesch (1999) utilizam-se questões abertas, que permitem captar a percepção dos participantes da pesquisa. O questionário foi enviado por meio de correio eletrônico. Antecipadamente foi realizado um pré-teste para verificar se as questões eram compreensíveis, se a sequência das questões estava de acordo e se os resultados tinham sentido (ROESCH, 1999).

Quanto ao método, caracteriza-se como uma pesquisa qualitativa. Considera-se que esse método é apropriado 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 espionagem industrial.

Para o tratamento de dados obtidos com os questionários enviados por correio eletrônico, o método utilizado foi o mapa de associação de idéias de Spink e Lima (p. 107, 2000) mencionam que os mapas de associação de idéias:

> Têm o 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.

Vergara (2009) coloca que a utilização de mapas de associação de ideias consiste em uma forma de análise de dados em estado bruto, organizados em colunas que representam as categorias temáticas escolhidas pelo pesquisador. Os dados são apresentados, sem fragmentação, na sequência em que são coletados.

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 pólos 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 de no Brasil 17.500 empresas, segundo dados da revista Panorama Socioeconômico Município de Bento Gonçalves (2013).

A coleta de dados foi realizada nos meses de maio de 2014, utilizando questionários semi-estruturados com questões abertas, que é ideal nas pesquisas qualitativas, enviadas por meio de correspondência eletrônica, para os gestores das empresas (ROESCH, 1999). Foram enviados 80 questionários e 10 respondidos.

Quadro 1- Caracterização dos respondentes e da empresa

Questionário	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	Pequena
3	16	Gerente	Até 19	Pequena
5	4	Gerente Comercial	Até 19	Pequena
5	4	Gerente de vendas	Até 19	Pequena
6	5	Gerente Sócio	Até 19	Pequena
7	19	Diretora Administrativa Financeira	100 a 499	Média
8	12	Supervisor Financeiro	100 a 499	Média
9	3,5	Gerente Comercial	100 a 499	Média
10	13	Gerente Comercial e Exportação	Acima de 500	Grande

Fonte: Elaborado pelo autor.

6 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 (p. 107, 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 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.

Quadro 2- Mapa 1

Mapa:1	Empresas até 19 funcionários					
Perguntas	Percepção dos Gestores					
	Empresa 1	Empresa 2	Empresa 3	Empresa 4	Empresa 5	Empresa 6
1:O que você entende por espionagem industrial?	Roubo das nossas informações restritas.	Roubo de informações.	Seria o roubo de informções que a empresa possui.	Tem como objetivo obter informações confidenciais ou segredos comerciais sem a autorização dos detentores dessa informação, com fim de alcançar uma certa vantagem econômica. Com o tempo, a espionagem industrial tema dado uma definição mais alargada. Por exemplo, tentativas de sabotar uma empresa	Podemos dizer que é invasão de privacidade.	Espionagem sobre informações que a empresa possui.
2:Quais os cuidados que você toma com as informações?	Nenhuma.	Não tem proteção pois a empresa é de pequeno porte.	Tem que tomar cuidados com invasões em seu sistema, e no local de trabalho.	Não costumamos proteger as informações, por acharmos que por ser pequeno porte não há interesse.	Nenhuma.	Somente com informações sobre os valores o restante não tem proteção.
3:Você tem conhecimento das conseqüências que o vazamento de uma informação pode causar para a empresa?	Não.	Não.	Sim.	Não paramos para pensar sobre o assunto.	Não.	Não.
4:Os gestores tem o conhecimento das leis referente à espionagem industrial?	Não.	Não.	Não.	Não.	Não, nem sabia que existia.	Não.
5:Sendo (1) o mínimo e (10) o máximo, na sua percepção, a prevenção da espionagem industrial tem alguma importância para a sua organização?	Nota 5	Nota 7	Nota 7	Nota 8	Nota 5	Nota 6
Proteção das Informações						
Perguntas	Empresa 1	Empresa 2	Empresa 3	Empresa 4	Empresa 5	Empresa 6
6:Existe algum treinamento ou instruções para os colaboradores terem cuidado com as informações?	Não.	Não.	Não.	Não, nenhum treinamento e nem aviso.	Não.	Nenhuma.
7:Existe algum código de ética/conduta que envolva cuidados em relação a informações?	Não.	Não.	Não.	Não utilizamos.	Não.	Não.
8:Os produtos criados pela empresa são patenteados?	Não.	Não.	Não.	Não.	Não.	Não.
Tipos de Proteção						
9:A empresa mantém banco de dados de clientes? Se sim, como a empresa protege esse banco?	Sim, não todos funcionários do administrativo tem acesso	Sim. Mas não protege.	Sim, ele é protegido com um sistema de proteção de dados.	Sim, não é protegido.	Sim, sem proteção.	Sim. Não protege.
10:A empresa possui tecnologia da informação? Possui alguma proteção	Sim, somente pessoas que possuem a senha.	Sim. Somente antivirus.	Sim, temos um servidor com um software.	Sistema e antivirus e é feito Backup diário das informações do sistema.	Sim sistema de cadastro. Segurança somente com senha.	Sim, mas nenhuma proteção.
11:A empresa tem monitoramento por câmeras, 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.
12: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 pelo autor

Foram entrevistados seis gestores, de empresas com ate 19 funcionários, no qual pode se observar que todos os gestores possuem um razoável entendimento sobre espionagem industrial, mas na questão de como eles protegem 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 é somente em grandes empresas ela acontece também em pequenas organizações (SCULLY, 2013). Segundo o autor 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 com o vazamento das 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 do ataque (Jones, 2008). Ainda o autor 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 espionagem industrial, 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.

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

Segundo o autor (SOMMER, 1993), existem algumas razões para a realização da espionagem industrial e uma delas é roubar informações dos concorrentes sobre seus clientes para aumentar sua lista de clientes, pode ser verificado na pesquisa que todas as empresas possuem banco de dados de clientes e apenas uma tem proteção desses dados.

Em um mundo globalizado onde a tecnologia da informação é essencial para as empresas, o autor Scully (2013) menciona que o espaço cibernético é uma das áreas mais frágeis a roubo de informações atualmente, 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.

Os autores 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 normas de segurança em visitas na empresa, apenas três possuem normas de segurança, o restante não tem nenhuma proteção.

Quadro 3- Mapa 2

Mapa:2	Empresas de 100 a 499 funcionários		
Perguntas	**Percepção dos Gestores**		
	Empresa 1	**Empresa 2**	**Empresa 3**
1:O que você entende por espionagem industrial?	Pessoas que se infiltram na empresa para espionar e furtar informações sigilosas de propriedade industrial para repasse a terceiros.	Roubo de algo pertencente a empresa.	Favorecimento alheio podendo ser por parte de alguns concorrente, para uso próprio e\ou terceiros, de informações obtidas ilicitamente.
2: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.
2:Você tem conhecimento das conseqüências 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. Só o passivo trabalhista desconhecido que hoje as empresas estão sujeitas, já não valerias mais a pena, montarmos um negócio.	Algumas sim.	Algumas.
3: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.
4:Sendo (1) o mínimo e (10) o máximo, na sua percepção, a prevenção da espionagem industrial tem alguma importância para a sua organização?	Nota 7	Nota 8	Nota 9
	Proteção das Informações		
Perguntas	**Empresa 1**	**Empresa 2**	**Empresa 3**
5:Existe algum treinamento ou instruções para os colaboradores terem cuidado com as informações?	Sim, para a contratação já é feita uma boa triagem, são utilizadas entrevistas com psicólogas organizacionais, as quais buscam informações e fazem testes para avaliar os princípios, o caráter, entre outras questões, buscando identificar futuros problemas. 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.
6:Existe algum código de ética/conduta que envolva cuidados em relação a informações?	Nada assinado, somente verbal.	Sim.	Sim.
7:Os produtos criados pela empresa são patenteados?	Alguns sim, outros não.	Algumas.	Sim. O objetivo principal é garantir.
	Tipos de Proteção		
Perguntas	**Empresa 1**	**Empresa 2**	**Empresa 3**
8: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 de uso.	Sim, somente pessoas autorizadas tem acesso.	Sim, protegemos com senhas.
9:A empresa possui tecnologia da informação? Possui alguma proteção	Sim, a empresa tem perfil para controle e acesso das informações personalizadas, ou seja, cada funcionário acessa somente as informações pertinentes as suas funções, com senhas individualizadas.	Sim, existe proteção através de senhas e antivírus	Sim.
10: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 espeícificas, com senhas individualizadas, em qualquer momento e as imagens gravadas por um bom tempo.	Sim, inclusive na parte administrativa.	Sim.
11: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 são acompanhadas e podem circular somente em áreas autorizadas.	Sim.

Fonte: Elaborado pelo autor.

Foram entrevistados três gestores de empresas até 499 funcionários, conforme no mapa 1 todos os gestores possuem algum conhecimento sobre espionagem industrial, 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 sabem as conseqüências que o vazamento das informações podem causar, conseqüentemente os gestores levam em consideração a importância da prevenção da espionagem industrial na organização.

Outro fator em comum entre os dois mapas analisados, é que todos os gestores não têm conhecimento sobre as leis referentes à espionagem industrial.

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.

Conforme os autores Shanley e Crabb (1998) uma das medidas mencionadas por eles é o monitoramento por câmeras, em todas as áreas da organização, e as três empresas pesquisadas possuem essa medida de proteção, e inclusive uma das empresas tem acesso online.

Na questão de normas de segurança para visitação, todas as empresas são bem rigorosas, estão preocupadas com o acesso de pessoas estranhas em suas áreas físicas

Quadro 4- Mapa 3

Mapa:3	Empresa acima de 500 funcionários
Percepção dos Gestores	
Perguntas	**Empresa 1**
1:O que você entende por espionagem industrial?	Informações que concorrentes captam de nossa base e produção de maneira não autorizada.
2: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.
3:Você tem conhecimento das conseqüências que o vazamento de uma informação pode causar para a empresa?	Não.
4:Os gestores têm o conhecimento das leis referente à espionagem industrial?	Não.
5:Sendo (1) o mínimo e (10) o máximo, na sua percepção, a prevenção da espionagem industrial tem alguma importância para a sua organização?	Nota:8
Proteção das Informações	
Perguntas	**Empresa 1**
6: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.
7:Existe algum código de ética/conduta que envolva cuidados em relação a informações?	Sim.
8:Os produtos criados pela empresa são patenteados?	A grande maioria sim.
Tipos de Proteção	
Perguntas	**Empresa 1**
9: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.
10:A empresa possui tecnologia da informação? Possui alguma proteção	Sim, TI e proteção.
11: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.
12:Existe alguma norma de segurança quando pessoas visitam a empresa?	Sim, áreas restritas para fotografar e áreas administrativas.

Fonte: Elaborado pelo autor.

Foi entrevistado apenas um gestor de uma empresa com mais de 500 funcionários, e verificou-se que ele tem entendimento sobre espionagem industrial. Verificou-se semelhança com outros gestores dos mapas anteriores, o gestor também possui cuidados com suas informações, outro fator igual ao mapa 2 é que em sua percepção é importante a 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.

Na contratação dos colaboradores a empresa oferece treinamento, instruções mostrando que a empresa tem código de ética e conduta com as informações.

Na questão dos tipos de segurança a empresa tem um grande cuidado com o banco de dados, possuindo 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, como: visitas somente em áreas restritas e fotografar somente em local permitido.

Através da análise dos dados podemos verificar que todos os gestores possuem um entendimento razoável sobre espionagem industrial, 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, podendo concluir que os gestores das empresas de pequeno porte não estão tendo a percepção da importância da proteção das informações.

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.

Todas as empresas pesquisadas possuem tecnologia de informação, e apenas uma das empresas não tem nenhuma proteção sobre a (TI), 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 visitação as empresas, 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 à empresa.

CONSIDERAÇÕS FINAIS

O estudo foi realizado com o objetivo de verificar a percepção dos gestores das empresas do setor moveleiro no município de Bento Gonçalves- RS sobre espionagem industrial, e quais medidas de proteção estão tomando contra a espionagem.

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 entrevistados não tem a percepção da importância da prevenção do roubo das informações e conseqüentemente não tomam medidas de prevenção do roubo das mesmas. 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 melhorias.

Referências

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

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

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

BIRCH, A**.** Observadores Estrangeiros da Indústria do Ferro britânica durante o século XVIII. *Journal of História Econômica,* v.15, pp 23-33, 1995.

BRENNER, S. Há uma coisa como ' Crime Virtual'? *The California Criminal Law Review*, v. 4, p 11, 2001.

BRODY, R. WRIGHT**,** S. Issues in Defining Competitive Intelligence: An Exploration *Journal of Competitive Intelligence and Management*, v. 4, p 3, 2008.

CANONGIA, C; PEREIRA, M.N.F.; MENDES, C.U.S., ANTUNES, A.M.S. Mapeamento de Inteligência Compe- tiva (IC) e de Gestão do Conhecimento (GC) no Setor Saúde. R. Eletr. Bibliotecon. Ci. Inf., Florianópolis, n. esp., 1º sem. 204. p. 78 – 95, 204.

Centro da Indústria Comércio e Serviço de Bento Gonçalves. *Revista Panorama Socioeconômico Bento Gonçalves,* Rio Grande do Sul, Brasil, 42º ed. 2013.

CRANE, A. In the company of spies: When Competitive Intelligence Gathering becomes Industrial Espionagem. *Business Horizons*, v.48, pp 233–240,2005.

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

CSIS/SCRS Economic Security: Acesso 11 de junho 2014, 1996, http://www.csisscrs.gc.ca/eng/backgrnd/back6e.html.

FITZPATRICK, W. M; BURKE D. R.Competitive Intelligence, Corporate Security and the Virtual Organization. *Advances in Competitiveness Research*, v.11, No. 1 2003.

JONES, A. Industrial Espionage in a Hi-tech World**.** *Computer Fraud & Security*, Jan 2008.v. 1, pp7-13, 2008.

KACETL, J .Business Ethics for Students of Management. *Procedia - Social and Behavioral Sciences* .pp 875– 879, 2014.

KAPERONIS, I. Industrial Espionage. *Elsevier Science Publishers* B.V. North-Holland, Computers & Security.pp 117-121, 1984.

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

MALHOTRA, Y. An Analogy to a Competitive Intelligence Program: Role of Measurement in Organizational Research: 1993, Acesso 18 de julho 2014, http://www.brint.com/papers/ compint.htm.

MCGONAGLE, J.J. & VELLA, C.M. Outsmarting the Competition: Practical Approaches to Finding and Using Competitive Information**.** 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. Ethics in Marketing, pp. 260–279, 1993.

PHILLIP, C; WRIGHT, G. Roy.Industrial Espionage and Competitive Intelligence. *Journal of Workplace Learning*, v. 11, pp53 – 59, 1999.

PORTER, M. E. Competitive strategy: Techniques of Analyzing Industries and Com-petitors. New York: The Free Press. 1980.

PORTER, M. E. Estratégia Competitiva: Técnicas para Análise de Indústrias e da Concorrência. 7 ed. Rio de Janeiro: Campus, 1986.

REVISTA PANORAMA SOCIOECONÔMICO BENTO GONÇALVES-RS, 42 edição. GIACOMELLO, Cíntia P.; GEHLEN, Enio; LARENTIS, Fabiano; MATTIA, Mônica, B. 2013.

ROESCH, S. M. A. Projetos de Estágios e de Pesquisa em Administração. editora Atlas s.a São Paulo, 1999.

ROUACH,D; SANTI, P.Competitive Intelligence Adds Value:Five Intelligence Attitudes; *European Management Journal*, Published by Elsevier Science v. 19, n. 5, pp 552–559, 2001.

SAMLI, A. C;JACOBS , L.Industrial Espionage: A Damage Control Strategy Center for Business Ethics at Bentley College. *Published by BalckwellPublishing Business and Society Review* , 2003.

SEBRAE.Observatório Internacional Sebrae: Acesso 25 de maio 2014. http://ois.sebrae.com.br/pais/brasil/.

SCHUTTZ, A. B; COLLISS, M. M**.** Theethics of Business Intelligence Journal of Business Ethicsv. 13, Issue 4, pp 305-314, 1994.

SCULLY, P.Under lock and key: Protecting the Network From Attack.pp 12-15, 2013.

SHANLEY, A; CRABB, C. Corporate Espionage: No Longer a Hidden Threat, Chemial Engineering. pp 82-96, 1998.

SNYDER, H; CRESCENZI A**.** Intellectual Capital and Economic Espionage: New Crimes and new Protections. *Journal of Financial Crime*.v. 16 pp245-254, 2009.

Society of Competitive Intelligence Professionals: 2007, Acesso 20 de maio de 2014, Frequently asked questions. http://www.scip.org/2_faq.php.

SOMMER, P. Computer and Industrial Espionage.This paper accompanies a presentation made at Compsec 93 on 2 1 October 1993 at the Queen Elizabeth II Conference Centre, 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.

SUMAIA, S; GRISI, C. C. H. Espionagem e Ética no Sistema de Inteligência competitiva 2001. www.ead.fea.usp.br/semead/5semead/Mkt.htm acesso 03 maio 2014.

The Canadian Security and Intelligence Community: Her Majesty the Queen in Right of Canada, 2001:Acesso 23 de junho de 2014.
http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/csis-scrs/pdf/si-eng.pdf.

VERGARA, S. C. Projetos e Relatórios de Pesquisa em Administração, Editora Atlas São Paulo 1997.

VERGARA, S C. Métodos de Pesquisa em Administração. 3ª 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, Brasil, 26-30 outubro de 2009.

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

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

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, January, pp 136-145, 2014.