Produção do Conhecimento Sensível na Gestão e Engenharia da Produção Industrial

Renato Batista Pires Junior – eaecrbp@gmail.com
MBA GESTÃO E ENGENHARIA DA PRODUÇÃO INDUSTRIAL – IPOG

Resumo

Este trabalho refere-se aos temas produção do conhecimento sensível na Gestão e Engenharia da Produção Industrial ante a problemática do uso e da obtenção indevida de conhecimentos sensíveis – aqueles os quais, pela importância e necessidade de proteção, exigem medidas especiais de salvaguarda – que sempre foram grande fonte de atenção das organizações sejam elas públicas ou privadas, aplicando técnicas de obtenção de dados negados, por um lado, e neutralização, por outro, compiladas, organizadas e transformadas, respectivamente, nas Atividades de Inteligência e de Contra-Inteligência, presentes em todas as grandes decisões, proporcionando aos Governos Segurança e fornecendo às Empresas Competitividade. Tem este artigo o objetivo principal de sugerir uma referencia de gestão inteligente do conhecimento que prima pela acessibilidade e funcionalidade, apresentar um panorama integrado dos processos de gestão e aplicar técnicas de inteligência com o objetivo de otimizar certos processos. Para isto são apresentados e discutidos alguns conceitos de conhecimento, procedimentos de processos inerentes à gestão do conhecimneto e às tecnologias possíveis de serem aplicadas à gestão do conhecimento organizacional para a produção e proteção do conhecimento sensível. Enfim, podemos dizer que informação custa capital e tempo. Inteligência produz capital e adquire tempo.

Palavras-chave: Conhecimento sensível; inteligência; segurança

1. Introdução

1.1 – Objetivo

Objetivo deste trabalho é comprovar e descrever a importância da metodologia cientifica no universo acadêmico do discente como ferramenta fundamental para trabalho acadêmico, e que este discente com este instrumento poderá conquistar o mundo científico, bem como, construir uma arquitetura inteligente de compreensão e entendimento da gestão e produção do conhecimento sensível e organizacional em unidades de produção industrial, visando discutir as implicações diretas da ineficiência e omissão desta para as organizações dentro de sua estrutura de trabalho proposta, através da história sobre a compreensão das influências de várias teorias do "Conhecimento" estabelecendo parâmetros de avaliação, critérios de verdade, objetivação, metodologia e a relação sujeito e objeto para os vários modos de conhecimentos diante da crise da razão que se instaurou no século XX e que há de se prolongar neste presente século ou no vindouro, através dos desafios da construção de uma ética normativa compatível com as evoluções das descobertas e do conhecimento no campo científico.

1.2 – Método

Este trabalho adotou procedimentos previstos para uma pesquisa de natureza descritiva, teórico-empírica de abordagem qualitativa - (DEMO, 1991), que privilegiou a produção do conhecimento sensível de forma que todos os programas de qualidade total e de melhoria contínua possam promover segurança do patrimônio, controle e resultados para o investidor e consumidor.

1.3 – Resultados

De acordo com a estatística realizada, foi constatada que 27,9% dos funcinários possuem cursos e treinamentos na área de atuação. Predominou a escolaridade do ensino fundamental entre os recursos humanos e ambos os sexos estiveram presentes na mesma proporção. Em geral as empresas adotam critérios para a contratação dos funcionários, sendo o mais freqüente a apresentação pessoal por experiência. A descrição e ética dos colaboradores foi considerada como relevante. A falta de experiência, de responsabilidade e de compromisso nas realizações das atividades, bem como, de formação mínima para a função estão entre as principais dificuldades encontradas pelas organizações.

Neste trabalho, procurei compreender a proteção e segurança do conhecimento sensível, da informação, da qualidade de vida no trabalho, da satisfação, do bem-estar e da condição de vida secular das pessoas. As orientações aqui apresentadas baseiam-se na norma para apresentação de artigo científico, a NBR 6022 de 2003. (FACHIM, 2010)

2. Desenvolvimento

2.1 – Histórico

Historicamente, atividades de Inteligência são de tradição dos círculos militares, tendo sido decisivas em todos os grandes conflitos mundiais, tendo de longo tempo os seus conceitos são aplicados por diversas Organizações, atentas com o crescimento e assédio da concorrência, extravios de informações e em defesa de seu patrimônio e sua longevidade, seja esse físico, eletrônico ou composto por valores intangíveis tais como a credibilidade e confiança de mercado, por exemplo. Sua atual utilização como ferramenta-chave na gestão do conhecimento e organizacional de negócios, assim, representa uma séria ameaça corporativa, sendo registrados continuamente casos de fraudes internas, concorrência desleal e furto de informações, e até o seu uso, com regularidade, pelo Crime Organizado.

As vertentes principais das várias inteligências, são as seguintes:

A Inteligência Clássica (ICla) tem as suas mais antigas e conhecidas aplicações voltadas para a defesa do Estado, aí incluídas, instrumentalmente, as áreas diplomática e militar. Um possível exemplo de aplicação da atividade de Inteligência na diplomacia poderia ser a política externa formulada por John Dulles, ex-ministro das relações exteriores dos EUA ao tempo da chamada Guerra Fria. Talvez, não coincidentemente, John fosse irmão de Allen Dulles, diretor da CIA de 1953 a 1961. . (FRAGA PRETO, 2008)

Já a moderna Inteligência Competitiva (ICom), também chamada Inteligência Empresarial, é operacionalizada com a aplicação dos conhecimentos, técnicas e habilidades desenvolvidos cientificamente desde muito tempo pela Inteligência Clássica. Na ICom estariam incluídos, enquanto objetos de interesse a proteção do conhecimento referente aos empreendimentos científicos, industriais e comerciais, entre outros. (FRAGA PRETO, 2008)

De acordo com o Grande General Napoleão, todo líder tem o direito de ser vencido, mas não o direito de ser surpreendido. (BONAPARTE, 1815).

Conforme escreveu com sapiência Sun Tzu no livro a Arte da Guerra: " Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo e nem a si mesmo, perderá todas as batalhas. (SUN TZU, século IV, A.C.)

Para Fraga (2002), no século XX, durante a Segunda Guerra Mundial, as Forças Armadas dos países envolvidos criaram complicados códigos para transmitir suas mensagens, a fim de que os inimigos não descobrissem seus segredos. Desde que o homem existe, ele produz, mas também esconde conhecimentos. O homem escreve, fala, faz sinais para se comunicar, porém muitas vezes necessita guardar segredo a respeito de diversos assuntos, como, por exemplo, questões políticas, contatos diplomáticos, comunicações militares, produções científicas, atividades comerciais, industriais, financeiras, pandemias, além de seus segredos pessoais.

Segundo Fraga, as mensagens consideradas secretas existem desde a antiguidade e sempre exerceram grande fascínio. Bastou o homem aprender a escrever para que começasse a "esconder" seus escritos. Além disso, onde tem segredo tem quem quer descobrir o segredo. Se desde os primórdios da história existem métodos de esconder informações, dos mais simples aos mais engenhosos, desde a Antiguidade também existem os hackers e crackers que bolaram métodos de decifrar e decodificar . É por isso que dizemos que a Inteligência se subdivide em duas partes: Inteligência e Contra-inteligência.

Inteligência**:** atua por meio da produção de relatórios, contendo conhecimentos sobre fatos e situações que influem ou que podem influir nas decisões e nas ações do governo e sobre a proteção e a segurança da sociedade e do Estado. (FRAGA PRETO, 2008)

Contra-inteligências**:** atua por meio da adoção de medidas que protejam os assuntos sigilosos importantes para o Estado e a sociedade e que impeçam as ações de Inteligência por agentes estrangeiros. (FRAGA PRETO, 2008)

2.2 – Conceito

Conhecimento é a relação que se estabelce entre sujeito que "conhece" ou deseja "conhecer" e o objeto a ser conhecido ou que se dá a conhecer de forma interativa e plena.

Portanto, Conhecimento sensível: se a apropriação é fisica, sensível, o conhecimento é sensível.

Para o objeto do nosso artigo, o conceito de conhecimento sensível "na atividade de inteligência", pode-se afirmar que a informação sensível é aquela perceptível, privilegiada, ou seja, a informação relevante e que é captada pelos sentidos externos (visão, tato, paladar, olfato) e dos sentidos internos (memória, fantasia, imaginação). Dentro do contexto que propomos dissertar, tem o conceito na espionagem industrial do uso e da obtenção indevida de dados negados, conhecimentos sensíveis – aqueles os quais, pela importância e necessidade de proteção, exige medidas especiais de salvaguarda.

Na Grécia Antiga extraimos diversidade nas visões e métodos de conhecimento, como cita Aristóteles – Episteme – A ciência (conhecimento) é fundamentada na Observação (Experiência). Também tem-se o conceito de informação privilegiada, sendo sinônimo de conhecimento restrito a pessoas ou grupos. Normalmente são dados negados para conhecimento público, ficando restrito sua divulgação a terceiros.

A definição usual tem o conhecimento como sendo "crença verdadeira justificada". Existe dificuldade em definir o que realmente é conhecimento, baseado no paradoxo de que o conhecimento reside apenas na mente dos indivíduos e ao mesmo tempo poder ser capturado, armazenado e compartilhado (SPIEGLER, 2002). Essa inconsistência é evidenciada nas definições de conhecimento apresentadas a seguir.

Para Davenport & Prusak (1998), o conhecimento é definido como:

> Uma mistura fluida de experiência condensada, valores, informação contextual e 'insight' experimentado, a qual proporciona uma estrutura para a avaliação e incorporação de novas experiências e informações. Ele tem origem e é aplicado na mente dos conhecedores. Nas organizações, ele costuma estar embutido não só em documentos ou repositórios, mas também em rotinas, processos, práticas e normas organizacionais.

Para Probst (2002), conhecimento é: O conjunto total incluindo cognição e habilidades que os indivíduos utilizam para resolver problemas, compreendendo, teoria e prática, regras do cotidiano e instruções sobre como agir. O conhecimento baseia-se em dados e informações, estando sempre ligado às pessoas, construído por indivíduos e representando suas crenças sobre relacionamentos causais.

Nonaka e Takeuchi (1997) consideram o conhecimento como "um processo dinâmico de justificar a crença pessoal com relação à 'verdade', produzido (ou sustentado) pela informação". Dentro disso, acrescentam um aspecto dinâmico e de certo modo cumulativo à definição usual de conhecimento. Trata-se de uma mistura de valores, experiências, intuição e informação contextual, formando uma estrutura na mente de uma pessoa que a habilita a avaliar e acompanhar novas experiências e informações.

Esta experiência tem base firme no conjunto de atividades desenvolvidas através do tempo, portanto, fundamenta-se em fatos passados, isto é, nos problemas enfrentados, nas decisões tomadas e nos resultados obtidos (DAVENPORT & PRUSAK, 1998).

Reforçando o conceito de Nonaka e Takeuchi, Angeloni (2002) define que conhecimento corresponde ao "agrupamento articulado de informações por meio da legitimação empírica, cognitiva e emocional, não podendo ser considerado apenas como um agrupamento de informações. Significa nesse contexto, compreender todas as dimensões da realidade, captando e expressando essa totalidade de maneira mais ampla e integral".

Segundo Sveiby (1998), a definição de conhecimento depende do contexto e, por isso, seria mais razoável explicá-lo como:

> Uma capacidade humana, de caráter tácito, orientado para a ação, baseado em regras, individual e em constante mutação.
>
> Seu conteúdo é revelado em ações de competência individual, isso porque, na prática, essa se expressa por meio de conhecimento explícito, habilidade, experiência, julgamento de valor e rede social.

Conhecimento é a representação de todas as habilidades, experiências e capacidades praticadas pelo indivíduo ou pela organização, combinando sentimento, inteligência e capacidade de realização em ciclos contínuos de inovação e interpretação (STYHRE, 2001).

Paradoxalmente, Peter Drucker conceitua conhecimento, em sua apresentação no UCB Knowledge Fórum em 1998, através de uma comparação com informação: "O que está nos livros é informação; o que está nos bancos de dados é dado. Conhecimento existe apenas entre as duas orelhas".

O aprender fazendo provoca a internalização. Esse processo cíclico descrito caracteriza a espiral do conhecimento, proposta por Nonaka e Takeuchi, apresentada na figura 1:



Figura 1 - Espiral do conhecimento.

Fonte: Adaptado de NONAKA e TAKEUCHI (1997).

Ampliando a abordagem da espiral apresentada sob a ótica epistemológica, verifica-se que o conhecimento tácito dos indivíduos constitui a base do conhecimento organizacional e que o mesmo conhecimento mobilizado é ampliado "organizacionalmente" através das suas formas de conversão e cristalizado em níveis ontológicos superiores.

Dessa forma, a interação entre o conhecimento tácito e explícito terá uma evolução cada vez maior na medida em que subirem os níveis ontológicos, conforme exibido na figura 2:

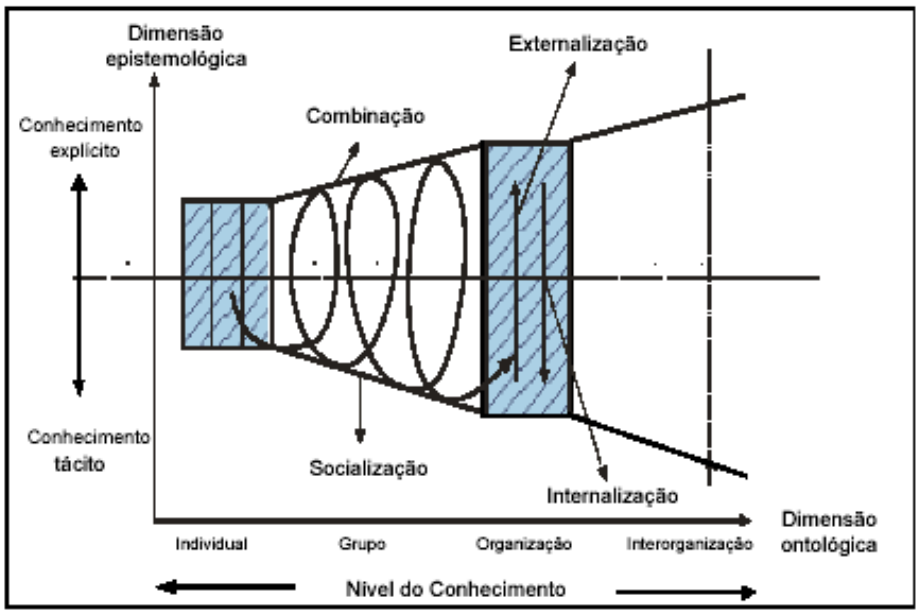


Figura 2 - Espiral de criação do conhecimento organizacional.

Fonte: Adaptado de NONAKA e TAKEUCHI (1997).

2.3 – Fundamento

A lei de combate ao Crime Organizado – Lei 9.034/95, considerando a macrocriminalidade, o autor deste artigo buscou enfatizar a multidisciplinaridade da Gestão do Conhecimento e organizacional dentro da Gestão e Engenharia da Produção Industrial.

2.4 – Doutrina

As atividades de Inteligência e de Contra-Inteligência, ambas, contraste de um mesmo universo, dependem da conscientização de todos os elementos da Organização nos procedimentos definidos para proteção de áreas e instalações, documentos e materiais, pessoas, processos e tecnologias, especialmente sistemas de comunicação e informações, eletrônicos ou não. (FRAGA PRETO, 2008)

Uma área especifica para desenvolver e implantar uma cultura de Produção, Aquisição e Proteção do Conhecimento Proprietário Sensível, devendo prevenir e garantir e centralizar todos os programas dispersos por diversos departamentos, tais como Segurança (CSO), Segurança da Informação (CISO), Escritório de Risco (CRO),

Financeiro (CFO), Auditoria Interna, Qualidade, RH, Marketing, respeitando sempre as decisões de esses profissionais em sua atuação, pois à Área de Inteligência compete coletar, analisar e informar tempestivamente aos Gestores, sem, entretanto, possuir qualquer poder de execução, sobretudo e principalmente, Controle de Ativos e Recursos de Informação, Imagem de Mercado e Conformidade Legal ("Compliance").

Desta forma, a Inteligência proporciona a produção do conhecimento para o processo decisório em Governos e em negócios no tempo e na maneira adequados; já a Contra-Inteligência utiliza as medidas ativas e passivas necessárias à proteção das informações de administração, dos processos decisórios, de negócios e seus próprios sistemas e processos de coleta de informações para investimentos e decisões de negócios futuros, por meio de sofisticadas técnicas de falsa informação, desinformação e logro. (FRAGA PRETO, 2008)

2.5 – Segurança Institucional (Controle Interno) na Proteção da Produção do Conhecimento Sensível

Compreende " um conjunto de medidas que visam a prevenir e a obstruir as ações adversas de quaquer natureza que incidam ou possam incidir sobre os Recursos Humanos, a Documentação e o Material, as Comunicações, a Informática e as Áreas e Instalações que configuram a organização", desdobramdo-se nos segmentos a seguir:

- **Segurança dos Recursos Humanos;**
- **Segurança da Documentação e do Material;**
- **Segurança das Comunicações;**
- **Segurança da Informática; e**
- **Segurança das Áreas e das Instalações.**

2.6 – Segurança dos Recursos Humanos

Conjuntos de medidas voltado para os Recursos Humanos, no sentido de assegurar comportamentos adequados às funções desempenhadas, à salvaguarda de conhecimento e de dados de omteresse da instituição, abrangendo também medidas de proteção física dos indivíduos detentores de conhecimentos e de dados que devem ser protegidos e que, em função de sua natureza, requeiram excepcionais cuidados.

2.7 – Segurança da Documentação e do Material

Medidas voltadas para os documentos e os materiais, no sentido de salvaguardar os conhecimentos e os dados de interesse neles contidos, de vez que são alvos de furto, de destruição, de aduteração. Tais procedimentos são acompanhados de medidas de segurança patrimonial e de proteção a incêndios.

2.8 – Segurança das Comunicações

Conjunto de medidas voltado para as comunicações, no sentido de salvaguardar conhecimentos e dados de interesse durante os atos de transmissão e de recepção, abrangendo os cuidados com a telefonia, fax, canais de comunicação, linhas de dados e equipamentos de rádio.

2.9 – Segurança da Informática (TI)

Medidas voltadas para a informática, visando a estabelecer padrões que permitam garantir a segurança e a integridade do " hardware " e do " software " dos sistemas de gerenciamento de banco de dados e dos próprios banco de dados. Este tipo de segurança é implementada por meio de medidas que dizem respeito ao controle de acesso aos bancos de dados, ao uso de senhas e a utilização de redes internas (INTRANET) e externas (INTENET).

2.10 – Segurança das Áreas e das Instalações

Um conjunto de medidas voltado para as necessidades de segurança das áreas e instalações que configuram a organização, para a sua demarcação, classificação e sinalização, objetivando a definição das áreas e instalações a serem preservadas por abrigarem dados e conhecimentos de interesse ou pro serem consideradas vitais para o pleno funcionamento do órgão.

São adotados procedimentos de controle de acesso de visitantes e funcionários, guarda ou vigilância das áreas e instalações, equipamentos de fechamento, circuitos internos de TV e outros ligados à segurança patrimonial armada ou não.

3. Exemplos

3.1 – **Informação privilegiada**

Um funcionário que ocupa um cargo de gerência em uma das empresas que compraram a Ipiranga na segunda-feira (19) (Braskem, Petrobras e Grupo Ultra) está na mira da Comissão de Valores Mobiliários (CVM) como um dos principais suspeitos de ter usado informação privilegiada sobre a venda para ganhar dinheiro no mercado financeiro.

Até agora, quatro acionistas tiveram bloqueado o dinheiro que ganharam vendendo as ações da Ipiranga antes do anúncio do negócio. A iniciativa do bloqueio, fortemente elogiada por quem acompanha o mercado financeiro, nunca havia acontecido antes no Brasil. Só desse acionista foram R$ 295 mil bloqueados pela Justiça. Ao todo, 26 investidores estão sendo investigados.

No Brasil, usar informação privilegiada nunca deu cadeia. O que as empresas fazem para evitar vazamento de informação. Na segunda-feira (19), Petrobras, Braskem e Grupo Ultra anunciaram ao mercado que compraram em conjunto o Grupo Ipiranga, por US$ 4 bilhões.

É o maior negócio fechado no Brasil este ano e um dos maiores do setor químico e petroquímico dos últimos tempos. Na sexta-feira (16), último dia de negócios antes do anúncio, os papéis da Ipiranga chegaram a subir mais de 33% na Bolsa de Valores de São Paulo (Bovespa).

O uso de informação privilegiada no mercado financeiro - ou "insider trading" - é um problema temido pelas empresas que têm suas ações negociadas na bolsa. Deixa nas companhias, na maioria dos casos, feridas financeiras e morais: são crimes que envolvem pessoas que gozam de muita confiança dentro das organizações - funcionários, advogados, consultores - e, por isso, são difíceis de detectar e combater.

Segundo a CVM, uma em cada quatro fusões e aquisições de empresas no Brasil tem vazamento de informação. O G1 preparou um passo-a-passo que vai ajudar você a entender porque, no mundo dos negócios, segredos podem ser tão valiosos. Quem são os "insiders traders"?

A expressão é norte-americana (do inglês, "inside"= dentro e "trader"= negociador), mas já é fortemente usada na linguagem corporativa nacional. Insider é toda pessoa que tem acesso a informação privilegiada nas empresas. São os indivíduos que participam diretamente de operações corporativas importantes.

Em uma transação de fusão entre duas empresas, por exemplo, a estimativa da CVM é de que participem até 200 pessoas, desde as primeiras negociações até o fechamento do negócio.

Podem ser funcionários de alto escalão, executivos de bancos de investimento, advogados, consultores. Até aí, problema nenhum.

A ilegalidade começa quando um "insider" resolve utilizar a informação para negociar ações na bolsa de valores: se a notícia é boa e vai fazer o preço das ações subir, ele compra os papéis da empresa por um preço baixo para vender depois por um valor bem mais alto.

Se o fato é ruim, ele vende os papéis e evita perder dinheiro antes que o mercado tome conhecimento.

3.2 – **Por que informações valem tanto?**

Na hora de comprar uma ação de uma empresa, o investidor vai escolher as que tenham os melhores resultados e perspectivas para o futuro: empresas lucrativas, que liderem o mercado e paguem bons dividendos para seus acionistas entram na lista das mais atrativas.

Para identificar as candidatas mais fortes, é preciso ficar de olho no noticiário: no mercado financeiro, são as informações sobre cada empresa que vão influenciar a decisão final do investidor de definir um preço melhor ou pior para a ação.

“A determinação do valor de uma ação está relacionado ao que todo mundo sabe. Por isso, o mercado tem por princípio que prover informações iguais para todo mundo”, diz o advogado Paulo Frank Coelho da Rocha, sócio do escritório Demarest e Almeida. "É importante garantir que esse princípio seja cumprido, para que o mercado financeiro, um dos pilares da economia, continue sendo confiável".

3.3 – **Notícias poderosas.**

Toda notícia que influencie um investidor a comprar ou vender a ação de uma empresa – o chamado fato relevante, como define a CVM - requer cuidados especiais por parte das

empresas.

Por exemplo: a descoberta de um novo poço por uma exploradora de petróleo, a pesquisa de uma farmacêutica que fracassou após anos de investimento ou o lançamento de um aparelho eletrônico que vai revolucionar o mercado são novidades que podem animar ou afastar um acionista potencial da empresa.

É importante que, ara acontecimentos como esses, a empresa mantenha sigilo até que o fato se confirme e, depois disso, divulgue a notícia para todo o mercado financeiro, sem privilegiar ninguém. “

A legislação determina que um fato relevante deve ser divulgado imediatamente, homogeneamente (a todos os meios possíveis) e, de preferência, fora do horário do pregão”, diz o advogado Marcello Klug Vieira, especialista em insider trading.

3.4 – **Segurança Institucional**

É um tema ausente da agenda nacional e tradicionalmente não constitui prioridade das autoridades e dirigentes do poder público. Habitualmente, essa temática ganha evidência quando da ocorrência de contingências de grande proporção, cujos danos e prejuízos ao país expõem deficiências e revelam sérias vulnerabilidades institucionais, ensejando inclusive a devida responsabilização criminal dos envolvidos.

Infelizmente, prevalece em nossa sociedade a subcultura em que os paliativos imperam em detrimento das soluções, potencializando o agravamento do risco à segurança. Nesse mister, a importância da segurança institucional transcende a ação de proteção e salvaguarda, pois afeta diretamente a eficiência de nossas instituições e, em última instância, a própria segurança nacional.

Exemplos lamentáveis não faltam para ilustrar essa realidade no Brasil, como o afundamento, em 2001, na bacia de Campos, da plataforma da Petrobras P-36, maior plataforma marítima de exploração de petróleo do mundo, implicando um prejuízo de US$ 354 milhões e a morte de 11 funcionários.

O relatório da Agência Nacional do Petróleo (ANP) apontou uma série de irregularidades que teriam levado ao acidente, como problemas mecânicos, falta de treinamento, uso indevido de equipamentos, falta de sistema de controle, deficiências no projeto e erros no gerenciamento da P-36

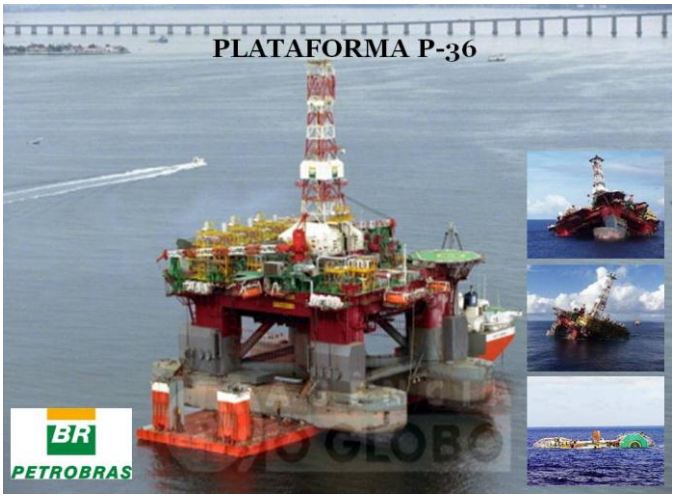


Figura 1: (Plataforma da Petrobras P-36)

Fonte: ANP – Agenica Nacional do Petróleo

Outro trágico exemplo, ocorrido em 2003, foi a explosão que destruiu o foguete brasileiro VLS-1, no Centro de Lançamento de Alcântara/MA, que além dos ingentes prejuízos financeiros não divulgados e do sério comprometimento do estratégico projeto aeroespacial brasileiro, matou 21 técnicos civis. Os relatórios dos ministérios da Defesa, e da Ciência e Tecnologia apresentaram como causas uma série de erros de segurança e manutenção na base.



Figura 2: Explosão do foguete brasileiro VLS-1, no Centro de Lançamento de Alcântara/MA

Fonte: Revsita Veja



(21 técnicos civis falecidos na explosão do foguete brasileiro VLS-1)

Vale dizer que, em ambos os casos, a despeito das inúmeras irregularidades, falhas de segurança e comprometimento à soberania nacional, estranhamente não foram apontados culpados.

Figura 3: Lista de óbitos na explosão do foguete brasileiro VLS-1

Fonte: Revsita Veja

Não nos esqueçamos do maior caso de corrupção da nossa república, que ganhou notoriedade em 2005 como o "escândalo do mensalão". Lembremos que o ensejo de sua descoberta originou-se da corrupção interna dos Correios, desvelada em filmagem clandestina, na qual o chefe do Departamento de Contratação e Administração de Material daquela instituição recebia propina para fraudar processo licitatório daquele órgão.



Figura 4: Flagrante de corrupção nos Correios – PTB-RJ

Fonte: Revsita Veja

(Maurício Marinho, chefe do Departamento de Contratação e Administração de Material dos Correios, é filmado negociando propina com empresários, interessados em participar de licitação nos Correios. No vídeo, Marinho diz ter o respaldo do deputado federal Roberto Jefferson (Figura 4: Flagrante PTB-RJ)).

Sobre esses e outros incontáveis trágicos exemplos nacionais, há um latente aspecto comum e determinante – a ineficiência da segurança institucional dos órgãos públicos e

privados pois a ocorrência de fatos dessa gravidade demonstra a inequívoca falência dessas estruturas.

Na realidade, nossa conjuntura atual delineia um cenário pessimista porquanto a segurança institucional no país, além do diletantismo e despreparo profissional com a qual é exercida, é muitas vezes divorciada de sua destinação, seja para a consecução de interesses escusos de nossas autoridades, ou aquiescendo passivamente irregularidades internas. Foi o que assistimos em 2008 no festival de clandestinidades protagonizadas pela Agência Brasileira de Inteligência (ABIN), na Operação "Satiagraha", que levou o Presidente da República a afastar o seu Diretor-Geral e toda a cúpula da agência; na operação "Caixa de Pandora", em 2010, em que o governador do Distrito Federal (DF) era o principal articulador de um enorme esquema de corrupção, conhecido como "mensalão do DEM", cuja gravidade levou o Procurador-Geral da República a solicitar intervenção federal no DF; e na operação "Mãos Limpas", que prendeu o governador do Amapá e toda a cúpula do seu governo, envolvidos em desvios de recursos do estado.

A verdade é que sistemas de segurança, inteligência, ouvidorias, controladorias, corregedorias e todas as demais estruturas de segurança institucional (controle interno) só são eficientes e plenamente confiáveis se submetidos a rigoroso controle externo, sob a égide dos princípios constitucionais da publicidade e transparência; pois são estruturas especialmente vulneráveis à corrupção. Portanto, os responsáveis por essas atividades devem ser igualmente investigados pelo poder público, particularmente quando da ocorrência de contingências, sofrendo a devida responsabilização funcional; pois a ineficiência, em todas as suas formas de manifestação, constitui a maior ameaça à segurança institucional. Caso contrário, o país continuará a assistir à destruição do seu já combalido sistema imunológico, ante a inação e passividade da sociedade brasileira.

A genealogia dessa problemática demonstra a inépcia generalizada das autoridades públicas nacionais sobre a temática da segurança institucional, cujo exercício é caracterizado pelo empirismo e práticas viciosas. Muitas são as dificuldades e equívocos existentes a serem vencidos nessa seara, visando à implementação de uma segurança institucional eficiente. Nesse sentido, inicialmente há que se rever os fundamentos sobre os quais são edificadas essas estruturas, a começar pela melhor compreensão do que é segurança institucional e sua aplicação.

A segurança que é majoritariamente praticada em nossas instituições e organizações é extremamente limitada, restringindo-se quase que exclusivamente a procedimentos de implantação de barreiras, controles de acesso, vigilância patrimonial e esforços envidados junto ao público interno no sentido de se criar e aprimorar uma mentalidade preventiva de segurança. Em que pese serem estas medidas relevantes e pertinentes ao caso em testilha, segurança institucional é uma temática muito mais abrangente e totalizante. Contudo, essa compreensão só é alcançada quando se responde à pergunta fundamental: *"O que é segurança institucional?"* Evidentemente, que essa questão suscitará inúmeras respostas que, diferentes entre si, demonstrarão o entendimento controverso dessa atividade, explicando o porquê da diversidade de suas práticas

institucionais, desvelando um de seus problemas cruciais - a falta de uma doutrina oficial sobre segurança institucional, no país. (André Soares)

Destarte, se o principal propósito é a implementação de uma segurança eficiente, voltada para a proteção e salvaguarda do poder público nacional, devemos então saber o que o estado brasileiro entende por segurança. Esse contexto nos remete inevitavelmente à concepção e significado de "segurança nacionaL", cuja doutrina foi lançada ao olvido com o término do regime militar no Brasil, pela grande rejeição social à denominada Lei de Segurança Nacional, que vigorou nesse período.

Nesse mister, nosso diploma legal em vigor que trata dessa temática é o Decreto nº 5.484, de 30 de junho de 2005, que aprova a Política de Defesa Nacional. Nele, o estado brasileiro conceitua Segurança como sendo "a condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais".

Por importante, vale destacar dois fundamentos ressaltados nesse diploma legal, quanto à concepção de segurança pelo estado, que são a "preservação da soberania e da integridade territorial; referente a pressões e ameaças de qualquer natureza".

Isto significa que a segurança nacional implica a preservação de sua soberania, ante a qualquer tipo de ameaças. Desta forma, por analogia do referido decreto, podemos deduzir que segurança institucional é"a condição que permite à instituição pública a preservação de sua autonomia e o cumprimento de sua missão constitucional, livre de pressões e ameaças de qualquer natureza".

Portanto, a segurança institucional visa à completa proteção e salvaguarda do poder público e privado, em toda a sua dimensão e espectro de atuação, contra qualquer tipo de ameaças.

Para cumprir plenamente sua destinação e atividade-fim a segurança institucional deve estruturar-se fundamentalmente em quatro áreas de atuação, a saber: governança corporativa, medidas ativas, medidas preventivas e medidas reativas.

A governança corporativa comanda a gestão organizacional, constituindo o seu centro decisor e irradiador da segurança institucional. É sua atribuição e competência a elaboração do Planejamento Estratégico, no qual a segurança institucional deve estar inserida, com sua respectiva concepção doutrinária própria. Nesse mister, vale ressaltar os equívocos doutrinários generalizados verificados no emprego das atividades de segurança institucional, da denominada atividade de inteligência, e da contra-inteligência. Conquanto sejam atividades afins quanto à salvaguarda institucional, há diferenças significativas quanto aos seus empregos, que devem estar claramente explícitos e delimitados no referido Planejamento Estratégico institucional.

A partir dele, a governança corporativa deve realizar o planejamento da segurança institucional propriamente dito, atentando para a importância da obtenção do equilíbrio entre segurança e o funcionamento eficaz da organização; evitar medidas de segurança excessivas; e o estabelecimento dos devidos controles institucionais, empregando para

isso a gestão da informação e do conhecimento, bem como a tecnologia da informação. Para obtenção da plenitude da salvaguarda institucional, as ações de segurança devem alcançar as diversas atividades estruturais organizacionais, desdobrando-se nos seguintes segmentos:

- Segurança da informação, referente à Política Nacional de Segurança da Informação; regida pelo Decreto no 3.505, de 13 de junho de 2000, que "Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal";
- Segurança das Operações, relacionada à sua atividade-fim;
- Segurança Logística, relacionada à sua atividade-meio;
- Segurança Econômica, relacionada à sua previsão e execução orçamentária; e
- Segurança Administrativa, relacionada ao seu funcionamento eficaz.

Por fim, a governança corporativa é responsável pelas ações de fiscalização e auditoria das atividades de segurança institucional, primando pela sua eficiência e evitando sua perigosa degenerescência.

Para esse mister, devem ser aplicados os preceitos constitucionais da publicidade e transparência, bem como implementado o controle externo das atividades de segurança, inteligência, ouvidorias, controladorias, corregedorias e todas as demais estruturas de segurança institucional.

A governança corporativa deve, ainda, estruturar o sistema de informações da organização, no qual o sistema de segurança institucional será parte integrante, visando ao assessoramento do processo decisório.

As medidas preventivas são de natureza passiva e podem ser classificadas em: ações de comando, direção e chefia; e segurança orgânica. As ações de comando, direção e chefia se referem à forma de exercício da condução institucional, por aqueles investidos dessa responsabilidade funcional, os quais devem ser selecionados não apenas por critérios técnicos e profissionais, mas também e principalmente por atributos morais e de liderança. Nesse contexto, as ações de comando, direção e chefia, constituem especiais medidas preventivas de segurança institucional, quando regidas rigorosamente pelos princípios do exemplo, da ética e da justiça; porquanto repercutem favoravelmente junto ao público interno, fortalecendo o seu sentimento psicossocial e o espírito de corpo institucional, proporcionando especial imunidade a todo tipo de ameaças à segurança. (André Soares)

A segurança orgânica é afeta exclusivamente à proteção da Informação organizacional produzida e sob sua custódia. É desenvolvida com medidas nas áreas de Segurança do Pessoal; Segurança da Documentação e material; Segurança das áreas e instalações, comumente chamada de Segurança Patrimonial; Segurança das Comunicações; e Segurança da Informática, ou meios informatizados. A segurança orgânica é parte integrante da Segurança da Informação, anteriormente referida como balizadora da Política Nacional de Informação, sendo esta muito mais abrangente. Vale registrar que a

segurança orgânica constitui muitas vezes a única expressão de segurança existente em órgãos públicos que, desconhecendo sua aplicação restrita, erroneamente acreditam ser ela capaz de proporcionar a devida segurança institucional. (André Soares)

As medidas reativas referem-se à ação imediata quando da ocorrência de eventuais contingências institucionais e são implementadas por meio da execução de planos de contingência, sindicâncias, inquéritos e demais medidas de apuração internas que se fizerem necessárias. Em relação aos planos de contingência, estes são planejamentos produzidos em função do levantamento dos riscos e vulnerabilidades institucionais e da avaliação do comprometimento que suas eventuais ocorrências possam impactar à organização. Dessa forma são estabelecidos níveis de prioridade e elaboradas as respectivas ações a realizar em caso de suas ocorrências, bem como os procedimentos necessários para a manutenção do funcionamento institucional em condições mínimas de eficiência. Todavia, a realidade geral em nossas instituições é de pendência quanto à conclusão desses planejamentos, os quais muitas vezes sequer são iniciados. Contudo, o desafio subseqüente à elaboração dos planos de contingência é ainda maior, pois demanda as suas permanentes atualizações e, principalmente, a condução dos respectivos treinamentos com todo o público interno; sem os quais tais planejamentos,por melhores que supostamente possam parecer, se não tiverem sido verificados operacionalmente, não terão qualquer efetividade quando de seu acionamento numa eventual situação real.

As medidas ativas são de natureza ofensiva, no sentido de se antecipar às eventuais ameaças e agentes adversos à instituição. Todavia, sua viabilidade demanda possuir a devida capacidade de investigação, que muitas instituições abdicam exercer. Desta forma, mesmo com uma satisfatória segurança estruturada em bases preventivas, sem as referidas medidas de natureza ofensiva, tais organizações ficam permanentemente à mercê da ação de forças antagônicas desconhecidas. Portanto, a implementação de medidas ativas de segurança complementam todo o ciclo de segurança institucional, exercendo também importante papel como elemento dissuasório, inibidor de ameaças. As referidas medidas ativas podem ser realizadas em várias vertentes, destacando-se, dentre elas: a investigação e as operações de inteligência; a constituição de força de emprego; e o emprego da comunicação, por meio da propaganda e contrapropaganda.

Entenda-se por capacidade de investigação a possibilidade de emprego operacional de meios e recursos técnicos científicos para análise de provas, materiais e evidências, no sentido de perscrutar a verdade dos fatos, em bases objetivas e com alta credibilidade, reconhecidamente comprovada. Conquanto tal aparato seja próprio das estruturas policiais, vale considerar, em função das peculiaridades institucionais, a viabilidade de possuí-los, ou de solicitá-los a esses órgãos de investigação, em função de suas necessidades de segurança institucional.

Vale dizer que a incapacidade institucional de realizar investigações dessa natureza representa evidente vulnerabilidade orgânica que, se identificada por agentes adversos, potencializa o risco de ameaças institucionais.

As operações de inteligência estão afetas à denominada atividade de inteligência, cuja doutrina de emprego deve constar do referido Planejamento Estratégico, integrada ao

planejamento de segurança institucional, conforme anteriormente descrito. Contudo, destaca-se que esta é uma seara controversa e polêmica no país, cuja inépcia generalizada de nossas autoridades e dirigentes tem causado prejuízos ao melhor emprego das atividades de segurança e inteligência, pelo diletantismo com que ambas são exercidas. Nesse mister, em apertada síntese, ressalta-se que "operações de inteligência" nada mais são que uma forma diferenciada de investigação, caracterizada pelo emprego do sigilo operacional, o qual constitui sua atividade-fim. Todavia, seu emprego envolve elevado potencial de risco, exigindo adequada estrutura em recursos de material e pessoal, cujo capital humano devidamente qualificado nessa atividade técnica-especializada é extremamente raro no país.

Portanto, o emprego das operações de inteligência só deve ser realizado em condições plenamente satisfatórias, sem o que constitui inclusive risco à segurança institucional. Todavia, constituem instrumento valioso, indispensável e insubstituível, tanto no assessoramento do processo decisório quanto na ação contra forças adversas.

A constituição de força de emprego representa o contingente em pessoal especializado para atuação na fiscalização interna, segurança ostensiva, exercendo papel de polícia no âmbito institucional. Essa atividade pode ser realizada com pessoal orgânico da instituição, ou de empresa idônea contratada para serviço terceirizado, destacando-se por importante a necessidade de rigoroso controle de contra-inteligência sobre seus integrantes.

"Nós ganhamos a guerra da revolução e perdemos a guerra da comunicação" *é o* 'mea culpa'***(*** Palestra de André Soares no "***1º Congresso Brasileiro de Gestão do Ministério Público - Governança institucional",*** patrocinado pelo Conselho Nacional do Ministério Público (CNMP).**)** veladamente assumido pelas mais nobres autoridades da Inteligência do Brasil, que comprova não apenas a importância da comunicação, mas principalmente o seu grande poder. Nesse sentido, o seu emprego é de grande valia para a segurança institucional, particularmente no contexto da propaganda e contrapropaganda que, atuando na expressão psicossocial, visam à obtenção de comportamentos predeterminados pelos diversos públicos de interesse. Por meio do emprego especializado da comunicação poder-se-á constituir um "exército invisível" e numeroso de colaboradores, no país e no exterior, indo ao encontro dos propósitos institucionais e conseqüentemente proporcionando a desejada segurança.

Por fim, lembremos que o principal e mais importante fator, não apenas para a consecução da segurança da organização, mas em todo o seu contexto institucional, são os seus recursos humanos.

Assim, a segurança institucional deve atentar para a segurança do pessoal, desde o processo seletivo, passando pelo desempenho da função, até a fase do desligamento de seus integrantes; emprestando especial atenção ao recrutamento de capital humano das áreas institucionais consideradas críticas, que são aquelas onde são desenvolvidas atividades vitais e sensíveis para a instituição, organização pública ou privada. Dentre elas, estão indubitavelmente os setores de segurança e inteligência; que, por serem

atividades técnicas e especializadas, exigem pessoal altamente qualificado, submetido a permanente treinamento e reavaliação profissional. Nesse mister, por importante, vale ressaltar a necessidade da adoção de medidas especiais de segurança, voltadas notadamente para o recrutamento do capital humano dos seus cargos de direção e chefia, que devem ser ocupados por pessoal devidamente qualificado e estritamente orgânico da referida instituição. Tal assertiva é importante doutrina consolidada nas melhores práticas de segurança institucional, com inúmeros exemplos de graves contingências ocorridas no Brasil, decorrentes do seu descumprimento. Portanto, contrariar esse preceito fundamental de segurança institucional é já comprometê-la.

O anunciado futuro promissor do Brasil de ascensão ao seleto grupo das principais potências mundiais requer a devida contrapartida quanto à garantia da segurança nacional e sua soberania, a qual é estruturada a partir da salvaguarda do poder público, representado por nossas instituições sejam elas públicas ou privadas. Protegê-las é muito mais que superar ameaças; é consolidar a sua própria eficiência e fortalecer a segurança do estado e da sociedade brasileira.

4. Aplicação na Engenharia da Produção Industrial

A Inovação sem fronteiras

As companhias inovadoras não se definem mais pela capacidade de criar novos produtos apenas dentro de seus laboratórios - e sim por abrir suas portas e formar eficientes redes de colaboração. Uma equipe de 200 pesquisadores — quase todos com mestrado ou doutorado — trabalha no centro de pesquisas da sede da fabricante de cosméticos Natura, em Cajamar, na Grande São Paulo. O time de cientistas mais do que dobrou de tamanho nos últimos três anos — e os investimentos da empresa em pesquisa alcançaram 110 milhões de reais em 2007, equivalentes a 2,5% de seu faturamento total. Mesmo com esse aumento de orçamento e de pessoal, a Natura não seria capaz de desenvolver sozinha os mais de quase 200 produtos que lançará no mercado neste ano.

Hoje, a pesquisa de quase metade das 120 novas tecnologias em estudo pela empresa está nas mãos de uma rede de parceiros que vem se multiplicando rapidamente e já representa um grupo de quase uma centena de universidades e companhias dentro e fora do país. Graças a essa cadeia, coordenada pela química paulistana Sônia Torucci, gestora de redes de inovação da Natura, o tempo médio de desenvolvimento de novos produtos da empresa caiu de cinco para dois anos.

A meta de Sônia é fazer com que parceiros brasileiros, franceses, alemães e americanos supram a metade da necessidade de inovação da empresa até 2010. Num movimento simbólico, em meados de 2009 o laboratório da Natura deverá deixar o prédio da sede em Cajamar e passará a funcionar em Campinas, no interior de São Paulo, próximo de universidades e empresas com as quais a fabricante mantém parceria. “Minha tarefa é mapear e me aproximar cada vez mais de parceiros com competência para vencer os nossos desafios tecnológicos”, diz Sônia.

A lógica de abrir as portas dos laboratórios adotada pela Natura subverte o conceito tradicional das companhias inovadoras. Desde os primórdios da Revolução Industrial, as empresas criaram um modelo segundo o qual apenas quem detinha a capacidade de inovar dentro de casa — e de manter a sete chaves o próprio segredo industrial — poderia superar os concorrentes. A crescente necessidade de encurtar ciclos de inovação, porém, vem forçando as empresas dos mais diversos ramos a migrar para o conceito batizado de inovação aberta.

O modelo está mudando a maneira como algumas das empresas mais inovadoras do mundo, como Apple, IBM e *Procter&Gamble*, concebem novos produtos. O princípio consiste em captar cérebros que estão fora da companhia para acelerar o lançamento de produtos. "Uma empresa insular que acha que tem todas as respostas está perdendo tempo. Estamos na era da companhia aberta e colaborativa. Trata-se de uma mudança radical", diz *Alan G. Lafley*, presidente mundial da *Procter&Gamble* em seu recém-lançado livro O Jogo da Liderança.

Entusiasta do conceito, *Lafley* vem transformando a centenária *Procter&Gamble* num dos melhores modelos mundiais de inovação aberta. Hoje, mais da metade das iniciativas da P&G em pesquisa e desenvolvimento envolve pelo menos um parceiro externo — há uma década eram raros os forasteiros que conseguiam entrar nos laboratórios da companhia espalhados por países como *Estados Unidos, China, Índia e Japão*.

Trata-se de uma mudança na maneira como os mais de 138 000 funcionários vêem a própria corporação — uma imagem desenhada há mais de um século desde que os empreendedores *James Procter e William Gamble* inventaram a primeira fórmula de sabão em pó. "Tínhamos orgulho de inventar sozinhos nossos próprios produtos", disse a EXAME Jeff Weedman, vice-presidente de desenvolvimento de negócios externos da Procter&Gamble, de seu escritório em *Cincinnati*. "Tivemos de quebrar a resistência ao que não era inventado por nós e entender que reproduzir as inovações de terceiros com sucesso também é motivo de orgulho."

O argumento mais convincente de *Weedman* — e de qualquer outra empresa envolvida com inovação aberta — é o resultado. Quando o veterano *Lafley* assumiu a presidência, em 2000, havia evidências de sobra apontando que o antigo modelo de auto-suficiência da *P&G* se tornara ineficaz. Naquela época, apenas 20% dos lançamentos da companhia atingiam as metas de retorno de investimento. As vendas estavam estagnadas e as ações caíram à metade de seu valor num período de apenas um ano.

Uma das primeiras medidas de *Lafley* foi determinar que metade das inovações da companhia deveria estar relacionada a parceiros externos até 2008. (A meta foi superada antes do previsto, no ano passado.) O movimento garantiu que a empresa ganhasse agilidade na pesquisa e conseguisse identificar melhor as oportunidades de mercado. Hoje, 50% dos lançamentos atingem suas metas de retorno de investimento. A mudança se reflete no resultado financeiro: nos últimos seis anos, o faturamento da *P&G* dobrou, alcançando 76 bilhões de dólares em 2007, e as ações valorizaram 150%.

Um dos grandes benefícios desse modelo de inovação é que as empresas conseguem dividir os riscos e custos do processo de inovação. Uma das empresas que aprenderam essa lição foi a americana *IBM*. Em 2000, a *IBM* anunciou investimentos de 5 bilhões de dólares para desenvolver o negócio de chips para grandes servidores. Na época, a opção da empresa foi encarar quase toda a pesquisa sozinha.Os altos investimentos e os longos ciclos de maturação desse negócio fizeram com que a divisão registrasse prejuízos de mais de 1 bilhão de dólares até 2003. Dois anos depois desse fiasco, a IBM anunciou a formação de um "ecossistema de inovação" para o desenvolvimento de novas tecnologias de chips. Fazem parte do grupo nove parceiros, entre eles *Sony*, Toshiba e um centro de pesquisa da universidade de Albany, nos Estados Unidos. Juntos, os parceiros investiram 1 bilhão de dólares no projeto e formaram uma rede de 250 pesquisadores. Ao adotar esse modelo, a divisão de chips da IBM passou a dar lucro (a empresa não revela de quanto).

Abrir as portas representa um desafio tão ou mais complexo que inovar dentro de casa. É preciso identificar e contratar os melhores cérebros mundo afora e buscar uma forma de integrá-los às necessidades da empresa. Há basicamente dois jeitos de fazer isso: peregrinar pessoalmente em busca de parceiros e usar a internet como uma espécie de radar virtual. A Natura decidiu por uma combinação dos dois.

A equipe de Sônia tem passado boa parte do tempo no que chama de road shows, em empresas e universidades espalhadas pelo Brasil para apresentar os tipos de parceria que busca. (Em 2007, ela já visitou mais de 40 parceiros em potencial no país, como o laboratório Fleury e a Universidade de Brasília.) "É uma novidade até mesmo para mim, que cresci inovando num modelo mais tradicional e fechado", diz ela, que trabalhou no laboratório da gigante de bens de consumo Unilever, em Londres, nos anos 90. Um dos casos mais recentes de parceria para inovação da Natura envolve a fabricante paulista de extratos vegetais Citroflora e a Universidade Federal de Santa Catarina.

A parceria resultou no lançamento mais importante da empresa no ano passado, o Chronos com flavanóides de passiflora. Uma das formas encontradas pela Natura para se aproximar de seus parceiros é o portal Natura Campus, inaugurado em 2003, que apresenta uma lista das áreas de interesse da companhia e abre espaço para que pesquisadores postem suas idéias. Em 2003, a Natura recebeu 15 projetos de parceria. Hoje, existe mais de uma centena de projetos na fila.

O diálogo virtual ganha proporções gigantescas para uma companhia como a *P&G*, com atuação em mais de 180 países. Seus executivos estimam que conseguem articular cerca de 1,5 milhão de pesquisadores pela internet — um time virtual quase 200 vezes maior que a equipe de 8 500 pesquisadores que trabalha hoje em seus laboratórios.

O principal radar para captar as idéias desses pesquisadores é o portal *Develop and Connect*, criado em 2003 (outras gigantes de bens de consumo, como Nestlé e Unilever, decidiram seguir o modelo e criaram portais semelhantes). Hoje, a rede é tão ativa que cerca de 29% das questões submetidas pela companhia encontram alguma solução em apenas três semanas. Foi

assim que a *Procter* conseguiu resolver em menos de um ano uma questão que teria levado pelo menos o dobro do tempo para ser resolvida internamente: uma solução para estampar imagens nas batatas fritas da marca Pringles. A resposta para o dilema estava numa pequena padaria em *Bolonha*, na *Itália*. O dono, pesquisador de uma universidade local que tinha desenvolvido uma técnica eficiente de imprimir imagens em bolos e outros doces, ajudou os pesquisadores da P&G a adaptar o sistema para batatas fritas. A novidade, lançada em 2004, fez com que as vendas de Pringles crescessem a um ritmo acima de dois dígitos percentuais no decorrer dos dois anos seguintes. Algumas dessas redes ganharam vida própria e tornaram a internet uma grande arena para o compartilhamento de problemas e de soluções de diversas companhias. Um dos casos mais relevantes é o do InnoCentive, criado pelos pesquisadores do laboratório farmacêutico americano *Eli Lilly* quase por acaso. No final de 2001, seus cientistas se viram com uma questão difícil: desenvolver rapidamente uma matéria-prima para colocar um produto no mercado. Para resolvê-la, decidiram lançar um desafio na internet — a solução foi dada por um cientista aposentado, que recebeu 25 000 dólares pela idéia.

Hoje, o *InnoCentive* é um portal independente, reunindo mais de 30 grandes empresas americanas e um grupo de 140 000 pesquisadores em 175 países. Uma das companhias que aderiram ao portal é a fabricante de *aeronaves Boeing*. Sua estréia no *InnoCentive* aconteceu em 2004, quando a empresa desenvolvia um novo modelo de aeronave, o 767 (paralelamente, formou um ecossistema com seus principais fornecedores para que eles ajudassem na concepção do produto).

Houve um duplo benefício — financeiro e estratégico. A Boeing conseguiu economizar 600 milhões de dólares em pesquisa e diminuiu o tempo final para a montagem do avião — de um mês para apenas três dias — graças a sugestões de forasteiros. A própria P&G estimulou a criação de outras três redes — *NineSigma, yet2.com e YourEncore.com* — que hoje são abertas a qualquer empresa. "Nesses ambientes, as companhias podem aproveitar os mercados globais emergentes e desenvolver produtos e serviços muito mais rápido e com mais eficiência do que era possível no passado", escreveram os consultores americanos *Don Tapscott* e *Anthony Willians* no livro *Wikinomics*, lançado em 2007.

Os riscos da inovação aberta ainda são pouco conhecidos — até porque são poucas as grandes empresas que mergulharam no modelo e boa parte das experiências em massa ainda é *recente. Um dos perigos mais evidentes, porém, é o vazamento de informações confidenciais*. Como garantir que um segredo industrial compartilhado com diversos parceiros não acabe nas mãos de um concorrente? A saída escolhida pelas empresas que apostam na inovação aberta é fazer contratos draconianos com seus fornecedores, exigindo sigilo absoluto (a quebra de contrato implica multas pesadas).

Outra precaução é deixar claro qual será o cálculo para a remuneração do trabalho dos parceiros — que pode ser desde royalties vinculados à venda do produto final até simples compra da tecnologia desenvolvida. O maior desafio está no convívio entre as várias partes durante o desenvolvimento. "Qualquer relacionamento terá altos e baixos, mas se fizermos nosso trabalho escolhendo parceiros com cultura semelhante à nossa, os problemas podem se

resolver mais facilmente", afirma Weedman, da Procter&Gamble. "Mais arriscado do que entrar no novo modelo é ficar de fora."

5. Conclusão

No cenário do desenvolvemento industrial e econômico atual, o Conhecimento passou a ser o maior diferencial competitivo entre países, empresas e profissionais. Dominar a tecnologia, os processos e o saber científico torna-se, cada vez mais, a chave do progresso e o principal valor das instituições e organizações públicas e privadas. Proteger o Conhecimento tornou-se, assim, uma necessidade das organizações e uma questão de segurança institucional (controle interno) e pessoal para o desenvolvimento de uma cultura da proteção do conhecimento. Com a inovação tecnológica industrial estamos escolhendo para o mercado consumidor um antagonismo cultural do "Modis Vivendis" – modos de vida – do sujeito em relação a demanda de consumo sem se importar com as origens do objeto e sua aplicabilidade social.
Diante da pluralidade de ofertas e um consumidor exigente, surge dentro do contexto da produção industrial o profissional da engenharia da produção industrial, na medida que as empresas de serviços usam, cada vez mais, a tecnologia e a segurança da informação como parte de uma estratégia competitiva, contratam, cada vez mais, pessoal com uma orientação técnica, ética profissional, sigilo industrial, dedicando-se à concepção, inovação, melhoria continua e implementação de sistemas que envolvem pessoas, materiais, informações, equipamentos, energia, ambiente e com a preservação do meio ambiente. As empresas de serviços aperceberam-se que a utilização inteligente da tecnologia pode ajudá-las a reduzir custos de operação e aumentar a lucratividade. O mercado mundial de trabalho está se dividindo, cada vez mais, em três: os países pós-industriais, que produzem sobretudo idéias, informações, serviços, estética e símbolos; os países industrializados, que produzem bens materiais; e os países pré-industriais, que estão condenados ao simples consumo de produtos provenientes do exterior. (PAULESKY, 2002)

Sendo assim, as nações produtoras de conhecimento possuirão uma significativa vantagem frente àquelas que o consomem, necessitando os países pré-industrializados ou industrializados desenvolver mecanismos que facilitem a produção e a disseminação do conhecimento como fator de sobrevivência e desenvolvimento sócio-econômico. Nesse foco, Peter Druker, já propunha a constituição de uma base de conhecimento na sociedade, contendo conhecimentos em rápida mudança o que possibilitaria uma ampla diversidade de aplicações sobre o conhecimento armazenado. Essa proposta reflete diretamente no modo de construir e administrar uma organização inovadora e suas competências, por meio da previsão e aceitação do novo, transformando suas idéias em tecnologia, produtos e processos (DRUKER, 1976).

A economia mundial vive um momento bastante delicado. A extinção das barreiras econômicas provocadas pelo fenômeno da globalização, aliada ao extremamente rápido avanço da tecnologia, faz com que os operadores das macro e microeconomia tenham que reavaliar periodicamente suas ações e decisões perante o mercado.

No Brasil percebe-se o despertar das empresas para a necessidade de gerir o conhecimento corporativo, porém poucas iniciativas concretas no sentido de reconhecer e utilizar o conhecimento para agregar vantagens competitivas são identificadas.

Enfim, o surgimento de modelos de gestão de conhecimento, como o proposto neste trabalho, e sua implementação nas organizações, aliado à definição de políticas organizacionais e governamentais que promovam a cultura da gestão do conhecimento e a formação de trabalhadores do conhecimento, tornarão a empresa brasileira mais forte, reconhecida e atuante no mercado globalizado, conseqüentemente incrementando a economia nacional, o que possibilitará maiores investimentos sociais, gerando um país menos desigual e mais justo.

Referências :

BAND, Willian A., **Competências Críticas**, São Paulo: Editora Campus, 1994.
DAVENPORT, T. H.; PRUSAK, L. **Conhecimento empresarial**. Rio de Janeiro: Campus, 1998.
DEMO, Pedro. **Metodologia Científica em Ciências Sociais**. São Paulo: Cortez, 1991.
DRUKER, Peter, **Teoria da Adminsitração** , 1976
EXAME, **A inovação sem fronteira**, eEd. Abril, 2008
FACHIM, Odília. **Fundamentos de Metodologia.** São Paulo: Saraiva, 2001.
FRAGA PRETO, Hugo César. **Segurança Pública Inteligente.** Goiás – Goiânia: Kelps, 2008.
LAFLEY, Alan G., CHARAN, Ram, **O Jogo da Liderança,** São Paulo: Editora Campus, 2008. 188p.
NONAKA e TAKEUCHI**, A criação do conhecimento Organizacional, SP,** Editora Era da Informação, 2005
PAULESKY, Jordan Juliani, **Gestão Inteligente do Conhecimento**, 2002, Florianópolis,SC
PEREIRA DAS NEVES, Lúcia Maria Bastos, **Napoleão Bonaparte**, Ed. Alameda, 2008, 1ª edição
PROBST, Gilbert et al. **Os elementos construtivos do sucesso.** São Paulo: Bookman, 2002.
RICH, Eliane; KNIGHT, Kevin. **Inteligência Artificial**. ed. São Paulo: Makron Books, 1993.
SENGE, Peter M. **A quinta disciplina: arte e prática da organização de aprendizagem.** ed São Paulo: Circulo do Livro, Best Seller, 1998. 443p.
STYHRE, A., **A Inteligência Competitiva aplicada nas Organizações do Conhecimento**, Ed. Silabo, 2001
SUN, Tzu, **A arte da guerra**, século IV, A.C., L&PM Pocket
SVEIBY, K., ***The new organizational wealth***:. *San Francisco*, CA: Berrett Koehler, 1998
TAPSCOTT, Don e WILLIANS, Anthony, ***WIKINOMICS***, SãoPaulo, Ed. Nova Fronteira, 2007