Reuna

PROPOSIÇÃO DE UM MÉTODO DE PROTEÇÃO DE NEGÓCIOS UTILIZANDO PREMISSAS DE CONTRA-INTELIGÊNCIA E GESTÃO DE RISCOS

PROPOSE A METHOD OF BUSINESS PROTECTION BASED ON ASSUMPTIONS OF COUNTER-INTELLIGENCE AND RISK MANAGEMENT

Rilu Dani Cosme Silva
Universidade Católica de Brasília - Brasil
Endereço: W5 Norte, Brasília - DF, CEP 70790-160, Brasil. Fone: 55 (61) 3448-7134
Email: rilu_dani@yahoo.com.br - Lattes: http://lattes.cnpq.br/6503742453111578

Submissão: 24 ago 2013 **Aprovação**: 20 jan 2013. **Última revisão:** 10 mar 2014 **Publicação**: 25 mar 2014. **Sistema de avaliação**: *Double blind review*. Centro Universitário UNA, Belo Horizonte -MG, Brasil. Editor geral Prof. Dr. Mário Teixeira Reis Neto, Co editora Profª. Dra. Wanyr Romero Ferreira

Este artigo encontra-se disponível no endereço eletrônico:
http://revistas.una.br/index.php/reuna/article/view/73

Resumo

Este artigo objetiva propor um modelo que analisa processos e funções no atendimento às premissas de Contrainteligência e Gestão de Riscos. Tal proposição considera um método de proteção de negócios organizacionais. As áreas de conhecimento utilizadas neste estudo são: Contrainteligência e Gestão de Riscos. Será apresentada uma revisão de literatura com os conceitos relacionados aos temas citados, fundamentando a proposta de um método visando à implantação de contramedidas. Para delimitar o escopo de proteção é proposto um método de avaliação de riscos em uma abordagem para minimizar ameaças potenciais que envolvem o modelo de processos da Segurança em Operações. Conceito este que busca convergir e proteger conhecimentos organizacionais considerados como sensíveis às organizações.

Palavras-chave: Contra-inteligência. Gestão de riscos.

Abstract

This article aims to propose a model that analyses processes and functions related with Counter intelligence and Risk Management premises. Theses are the knowledge areas considered in the study: Counterintelligence and Risk Management. There will be presented a literature revision with the refereed concepts, objecting to achieve the proposition of a method which aims the implementation of counter measures. To delimitate the protection scope is proposed one method of risk valuation in one approach to minimize threats that involves the Security Operation's process model. This concept searches to converge and protect organizational knowledge recognized as sensitive to the organizations.

Keywords: Counterintelligence. Risk Management.

1. Introdução

Um espectro de incerteza e insegurança permeia o ambiente profissional, quando o assunto é proteção de vantagens competitivas de uma organização. Talvez essa percepção seja a consequência de uma realidade que motiva a competição extrema, na qual se encontram as nossas organizações privadas. Vantagens competitivas organizacionais podem, em sua maioria, traduzir-se pelo simples fato de organizações possuírem algum tipo de informação ou ativo que possa ser considerado um diferencial em seu modelo de gestão.

No que concerne especificamente ao âmbito organizacional, não basta somente investir em ações e técnicas relacionadas ao estabelecimento de tais vantagens competitivas. Conforme afirma a Associação Brasileira de Inteligência Competitiva (ABRAIC), torna-se fundamental, também, a aplicação de técnicas e ferramentas para a manutenção dessas vantagens, incluindo a proteção do chamado conhecimento sensível, ou vantagens competitivas para os fins deste artigo.

Percebe-se que as necessidades de segurança em um ambiente organizacional tornam-se válidas somente após a ocorrência de determinado incidente. As possíveis perdas organizacionais são diversas, desde o vazamento de informações sigilosas ao colapso de infraestruturas que sustentam a viabilidade de determinados negócios. Dos vários entendimentos sobre como manter protegidas tais informações, um se sobressai, o de que evitemos ao máximo precisar utilizar contramedidas para a proteção de conhecimento sensível no ambiente organizacional. Isso devido à sua complexidade e à possibilidade de obtermos resultados imprevistos. Todavia, no instante em que tais ações são necessárias, elas devem estar implementadas e aptas para a proteção e defesa da organização.

Tendo em vista esse cenário, as seguintes questões tornam-se pertinentes à pesquisa:

- Como identificar de maneira sistemática o escopo de diferenciais competitivos em ambientes organizacionais?
- O que precisa mudar nas organizações com vistas à manutenção de tais vantagens competitivas?
- Existem mecanismos de proteção que podem ser implementados em ambientes organizacionais com vistas a amenizar essa insegurança?

Portanto o objetivo deste artigo é propor um método para identificar mecanismos de proteção no ambiente organizacional em convergência com conceitos relacionados à Contrainteligência (CI). E utilizar uma sistemática de Gestão de Riscos (GR) para a identificação e avaliação de riscos, como proposição para delimitar o que precisa ser protegido no ambiente organizacional.

2. Contrainteligência

No seu sentido mais amplo, contrainteligencia (CI) pode ser entendida como sendo o conjunto de ações que objetivam identificar e neutralizar as ações de espionagem. Pela perspectiva civil, conforme a ABRAIC (2008), tais ações buscam detectar o

invasor, neutralizar sua atuação, recuperar, ou mesmo contra-atacar por meio da produção de desinformação. As definições de contrainteligencia são oriundas do contexto militar e de segurança de estado. Os métodos de contrainteligência foram desenvolvidos e adaptados a partir de técnicas aplicadas de proteção.

A CI pela perspectiva militar do Exército dos EUA, é definida como um esforço multidisciplinar que contempla a Contrainteligência Humana (C-HUMINT), a Contrainteligência de Sinais (C-SIGINT) e a Contrainteligência de Imagens (C-IMINT), desenvolvidas contra todo processo de coleta de origem externa. A força da CI em conjunto com outros ativos de inteligência devem possuir a capacidade em detectar todos os aspectos da coleta de inteligência e atividades relacionadas que se propõem a ameaçar a Segurança em Operações, de Pessoal e de Material. Através de sua capacidade analítica, a CI provê recomendações, as quais, se implementadas, irão resultar em negação de informação às eventuais ameaças.

Conforme Gleghorn (2003, p. 19), de acordo com manual de contra-inteligência do Exército Americano e o manual dos Fuzileiros Navais Americanos, MCWP 2-14, existem essencialmente quatro funções, nas quais a contra-inteligência é fundamentada e opera, sendo: coleta, investigação, análise e operações. Enquanto essas quatro funções são derivadas especificamente do FM 34-60 e MCWP 2-14, os demais organismos de força nacional e o Departamento de Defesa Americano reconhecem que as diretivas de contrainteligência possuem como princípio essas mesmas funções de operações.

Como metodologia a Segurança em Operações (OPSEC) originou-se durante a guerra do Vietnã como um meio de descobrir como o inimigo estava obtendo informações avançadas em certas operações de combate no Sudeste da Ásia. OSPSEC é um programa de contramedidas voltado para a proteção de informações críticas. (ANTÓN et al, 2003, p.21)

No que concerne especificamente ao âmbito empresarial, não basta focar somente em ações e medidas relacionadas ao estabelecimento das vantagens competitivas obtidas. Torna-se fundamental, também, a aplicação de técnicas e ferramentas para a manutenção dessas vantagens. Nesse propósito e com o fim de abranger todas as eventuais vulnerabilidades, as medidas de proteção devem contemplar ações nos mais variados segmentos das instituições, incluindo áreas e instalações, documentos e materiais, sistemas de informação e, principalmente, as pessoas, o elo mais fraco e vulnerável da corrente. Tal nível de abrangência torna-se fundamental para permitir a redução das vulnerabilidades e eventuais ameaças em um ambiente organizacional.

Hoje, os sistemas de segurança tendem a concentrar-se na prevenção, mas isso resolve somente um terço da necessidade. Prevenção cria um obstáculo, mas invasões irão ocorrer. Atualmente há um crescente interesse em tecnologias de detecção, mas, mais uma vez, elas resolvem somente um terço do problema. Na medida em que a invasão tenha se instalado e sido detectada, um ambiente de segurança deve também suportar reação. Sem componentes de detecção e reação, um esquema que só conta com prevenção é destinado a falhar. Até mesmo pior se as pessoas acreditarem que os mecanismos de prevenção são perfeitos, elas não procurarão evidências da invasão (McCARTHY; CAMPBELL, 2003, p.30).

O Processo de Segurança em Operações é um método de contrainteligencia e apresenta-se como um contraponto ao modelo de Inteligência Competitiva. Conforme

Miller (2002), trata-se de um processo disciplinado que propicia proteção a informações e segredos fundamentais de negócios. Possui como objetivo implementar ações concretas em matéria de capacidades, limitações, atividades e intenções, evitando ou controlando, assim, a exploração por adversários ou concorrentes de negócio. O Processo de Segurança em Operações contempla uma estrutura de fluxo contínuo de atividades, em que o resultado de cada uma é saída para as atividades seguintes. Miller (2002) apresenta o referido modelo, tendo como principal objetivo considerar o valor do tempo da informação. Corresponde ao entendimento de que, se qualquer organização tiver algum tipo de invasão, qual seria a capacidade organizacional em identificar e quantificar o potencial da perda. Tal abordagem torna-se fundamental para amenizar eventuais resultados negativos.

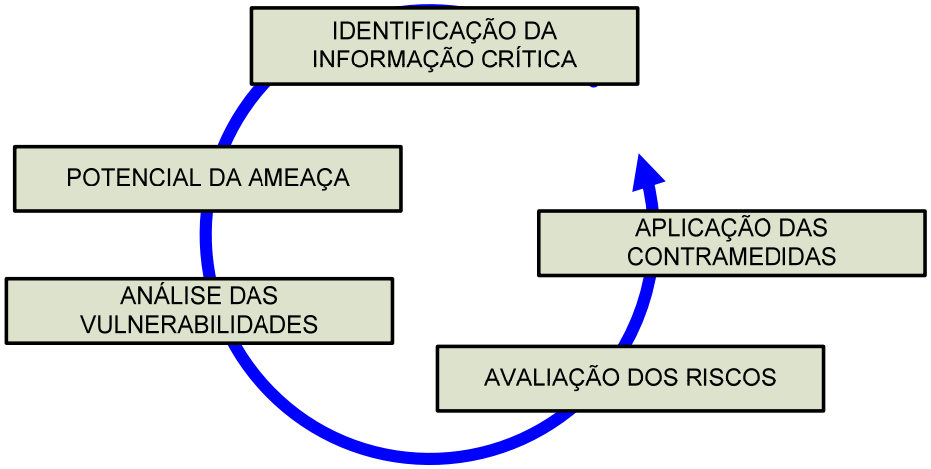


FIGURA 01: Segurança em operações
Fonte: ANTON et al, 2003 e MILLER, 2002.

Conforme a FIG. 01, pode-se observar que o principal aspecto a ser considerado é o uso de mecanismos de defesa, denominados de contramedidas. Conforme Miller (2002, p. 248), contramedidas são ações que impedem ou reduzem a disponibilidade de informação crítica para um adversário ou concorrente. E qualificam-se ao considerar a eliminação de indicadores passíveis de exploração, a inviabilização de ataques adversários tanto na coleta quanto no processamento de informações, e a melhoria contínua das contramedidas através de análises eficazes.

Uma estratégia defensiva tem como objetivo influenciar o processo decisório da concorrência de modo a tornar um ataque à posição de uma empresa menos aconselhável do ponto de vista do desafiante. Isso é feito por uma redução na indução para um concorrente atacar a empresa ou erguendo-se barreiras de entradas e de mobilidade para tornar o desafio mais difícil. Como um ataque por parte de qualquer desafiante muda de caráter com o passar do tempo, etapas defensivas apropriadas irão modificar-se em diferentes estágios do processo (PORTER, 1989, p.445).

2.1. Formas de proteção

Quando se imagina a necessidade de proteção, imaginam-se somente as perspectivas da Tecnologia da Informação (TI), entretanto existem outros aspectos que precisam ser considerados, e se imagina haver tantas vulnerabilidades quanto possíveis. Segundo a Portaria n.11 do Exército Brasileiro (Secretaria Geral do Exército, 2001), os domínios de informação sensível estão diretamente relacionados à Segurança de Pessoal, da Documentação, do Material, de Áreas e instalações, e da Informática. Tais aspectos necessitam de análise e atenção quanto aos controles e mecanismos de proteção.

Conforme Moresi (2008), pode-se categorizar em dois os tipos de formas de proteção organizacional, uma com abordagem passiva e outra ativa. A Segurança Orgânica pode ser entendida como um conjunto de medidas passivas destinadas a prevenir e a obstruir ações adversas de serviços de Inteligência ou elemento ou grupo de qualquer natureza e dirigidas contra a organização. Conforme segue: Segurança de Pessoal; Segurança da Documentação e do Material; Segurança das Comunicações; Segurança da Informática; e Segurança das Áreas e Instalações.

No mesmo entendimento, a Segurança Ativa é o conjunto de medidas, de caráter eminentemente ofensivo, destinadas a detectar, identificar, avaliar e neutralizar as ações adversas de serviços de inteligência ou elemento ou grupo de qualquer natureza e dirigidas contra a organização. Enquanto a segurança orgânica procura criar obstáculos entre os elementos ou grupos adversos ou oponentes e a organização; a segurança ativa atua ofensivamente sobre tais ameaças, tais como Contraespionagem, Contraterrorismo, Contrassabotagem, Contrapropaganda e Desinformação. Conforme Krisan (1999, p.61), nos ambientes governamentais, procedimentos padrão orientam quanto à implementação de controles em segurança em operações e segurança de informações. No setor privado, o que comumente prevalece é a abordagem de tentativa e erro. Organizações que enfatizam métodos para exploração de informação pública sobre seus concorrentes podem demonstrar pouco interesse na proteção delas mesmas.

Conforme orienta a Portaria n.11 (Secretaria Geral do Exército, 2001), para cada domínio alguns aspectos e categorias precisam ser contemplados, de acordo com o QUADRO 1.

Quadro 1 – Domínios de proteção

Domínio	Aspectos
Segurança de Pessoal	Segurança no Processo Seletivo
	Segurança no Desempenho da Função
	Segurança no Desligamento da Função
Segurança da Documentação	Generalidades (prazos de classificação)
	Segurança na Produção
	Segurança na Expedição e recepção
	Segurança no Manuseio
	Segurança no Arquivamento
	Segurança na Eliminação
Segurança do Material	Segurança na Celebração de contratos e convênios
	Segurança no Transporte
	Segurança na Eliminação
Segurança de Áreas e Instalações	Demarcação, sinalização, concessão de acesso
Segurança das Comunicações	Segurança na Remessa ou transmissão
	Segurança do Conteúdo
Segurança da Informática	Segurança de *Hardware*
	Segurança de *Software*
	Segurança Física
	Segurança na *Internet*
	Segurança no Correio eletrônico
	Segurança em Sistemas corporativos, *Intranet* e redes locais
	Segurança Contra furto, roubo ou extravio de dados

Fonte: STARRY e ARNENSON, 2008.

Assim, o escopo a ser delimitado é premissa chave de sucesso, para este fim propõe-se neste trabalho o uso de um método embasado na Avaliação de Riscos, a ser visto na próxima seção deste artigo. Conforme Mcmarthy e Campbell (2003, p.56), “as pessoas são o seu melhor ativo de segurança e sua maior vulnerabilidade, o infame hacker, admitiu que raramente precisava recorrer a *exploits* (softwares de exploração)”.

Starry e Arnenson (2008) afirmam que, à medida que a tecnologia permite um maior número de indivíduos, grupos, organizações e nações-estados conectarem-se com o mundo por meio do ambiente de informação global, pode-se esperar que esses usuários persigam seus interesses, tentando manipular e controlar o conteúdo e o fluxo das informações dentro do ambiente de informação militar.

3.Gestão de riscos

A AS/NZS 4360 (2004, p. 6) define a gestão de riscos como a capacidade de identificação de variações potenciais em relação ao que se planeja ou se espera, e o controle dessas variações para que seja possível maximizar oportunidades, minimizar perdas e melhorar as decisões e os resultados. A mesma norma ressalta que a Gestão de riscos possui como finalidade a busca do equilíbrio apropriado entre o

reconhecimento de oportunidades de ganhos e a redução de perdas. Ela é parte integrante das boas práticas de gestão e também um elemento essencial da boa governança corporativa. É um processo iterativo composto por etapas que, quando realizadas em sequência, possibilitam a melhoria contínua da tomada de decisões e facilitam a melhoria contínua do desempenho.

A ISO/DIS 31000 (2008, p.5) afirma que organizações de qualquer tipo e tamanho estão sujeitas a enfrentar uma série de riscos que afetam a conquista de seus objetivos. Tais objetivos podem estar relacionados com todos os tipos de atividades organizacionais, de iniciativas estratégicas a operacionais, de processos a projetos, que são refletidos em termos estratégicos, operacionais, financeiros e com repercussões de impacto na imagem de tais organizações. Dessa maneira, a gestão de riscos pode ser aplicada em qualquer tempo para toda a organização, por entre suas várias áreas e níveis, assim como para funções e atividades específicas.

Segundo McCarthy e Campbell (2003), as respostas a questões que envolvem ameaças, vulnerabilidades e ativos constituem o perfil de risco organizacional, e é preciso delimitar esse risco para definir e estabelecer um adequado ambiente de segurança corporativa.

A gestão de riscos propõe-se a conhecer as limitações de recursos que estão disponíveis, e de maneira realista elaborar uma sistemática de controle apropriado à organização. A gestão de riscos pode ser aplicada a uma grande variedade de atividades, decisões ou operações de qualquer entidade pública, privada ou comunitária, grupo ou indivíduo. Embora sua aplicação seja bastante ampla, os processos de gestão de riscos são comumente aplicados por organizações ou grupos, que possuem necessidades de seus produtos e serviços, bem como de processos e práticas específicas. Conforme a AS/NZS 4360 (2004, p. 7), deve-se encontrar um equilíbrio entre o custo, para evitar as ameaças ou ampliar as oportunidades, e os benefícios a serem obtidos.

3.1.Avaliação de riscos

A seguinte proposta tem como finalidade responder a questões que envolvem os interesses e os receios dos principais gestores organizacionais relacionados aos itens de proteção. Pretende-se propor um método para identificar o que precisa ser protegido no ambiente organizacional, utilizando uma perspectiva da Gestão de Riscos, denominada avaliação de riscos.

Embora tudo isto possa parecer simplista, torna-se, porém, valioso porque assim se evita que a empresa acabe violando um dos preceitos básicos de Bismarck: “Aquele que quer proteger tudo, acaba por nada proteger”. Com esse tipo de abordagem, destina-se maior proporção de proteção aos ativos empresariais merecedores da alocação dos recursos disponíveis (MILLER, 2002, p.234).

Conforme Willis (2007), a avaliação de riscos provê uma estrutura (*framework*), ao considerar ameaças, vulnerabilidades, e consequências de ataques potenciais e o desenvolvimento de estratégias para gerenciar esses riscos de maneira mais efetiva, tendo em vista a limitação de recursos. O mesmo autor afirma que essa discussão leva a duas conclusões. A primeira, que a análise de riscos pode ser utilizada para

aperfeiçoar produtos de inteligência. A segunda, que a análise de riscos pode ser utilizada para a priorização de recursos para a coleta de inteligência. Entretanto é importante perceber que os profissionais que aplicam a análise de riscos devem reconhecer suas limitações para garantir que os resultados são apropriados ao propósito e que a sua utilização não cegue o analista ao potencial de surpresas.

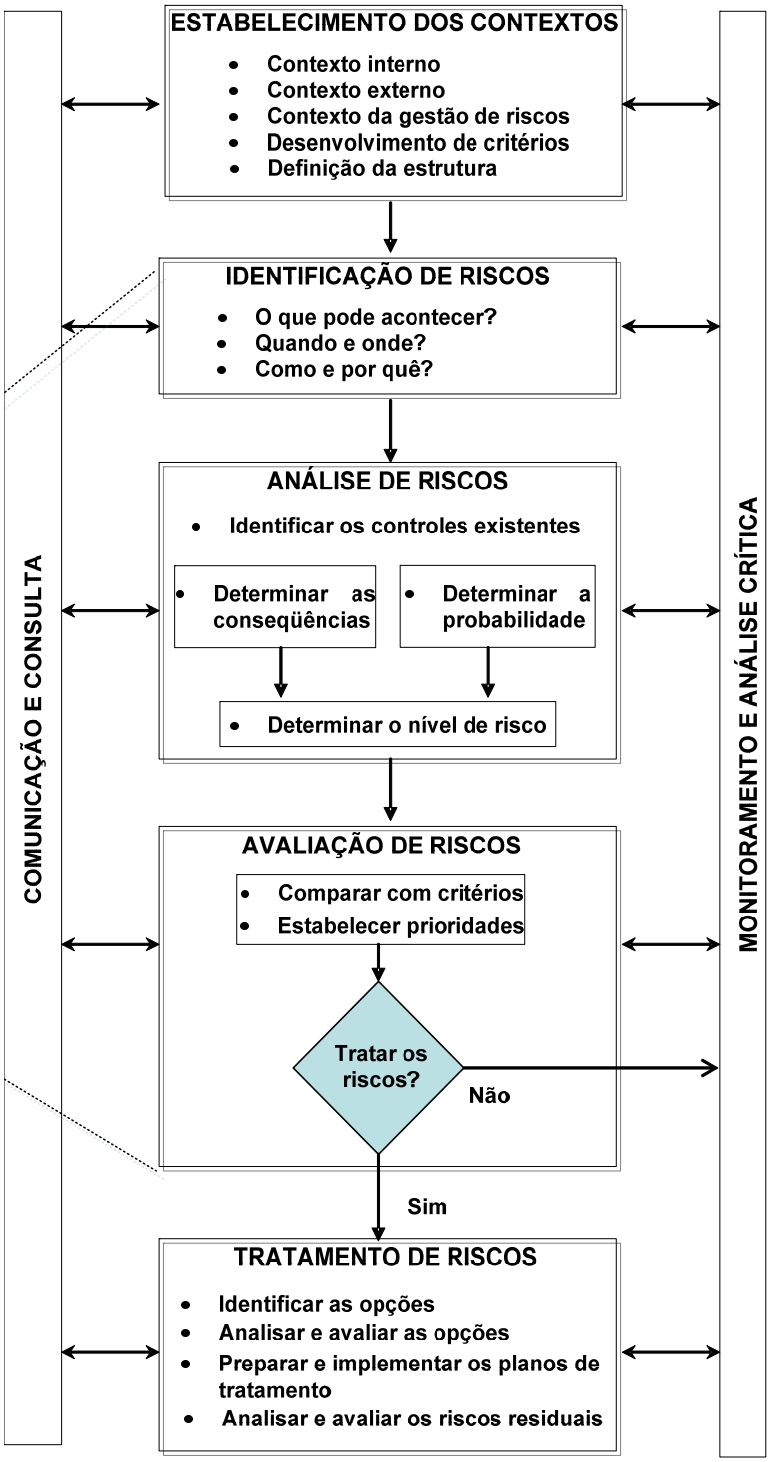


FIGURA 2: Atividades de avaliação de riscos e a relação com categorias gestão
Fonte AS/NZS 4360, 2004.

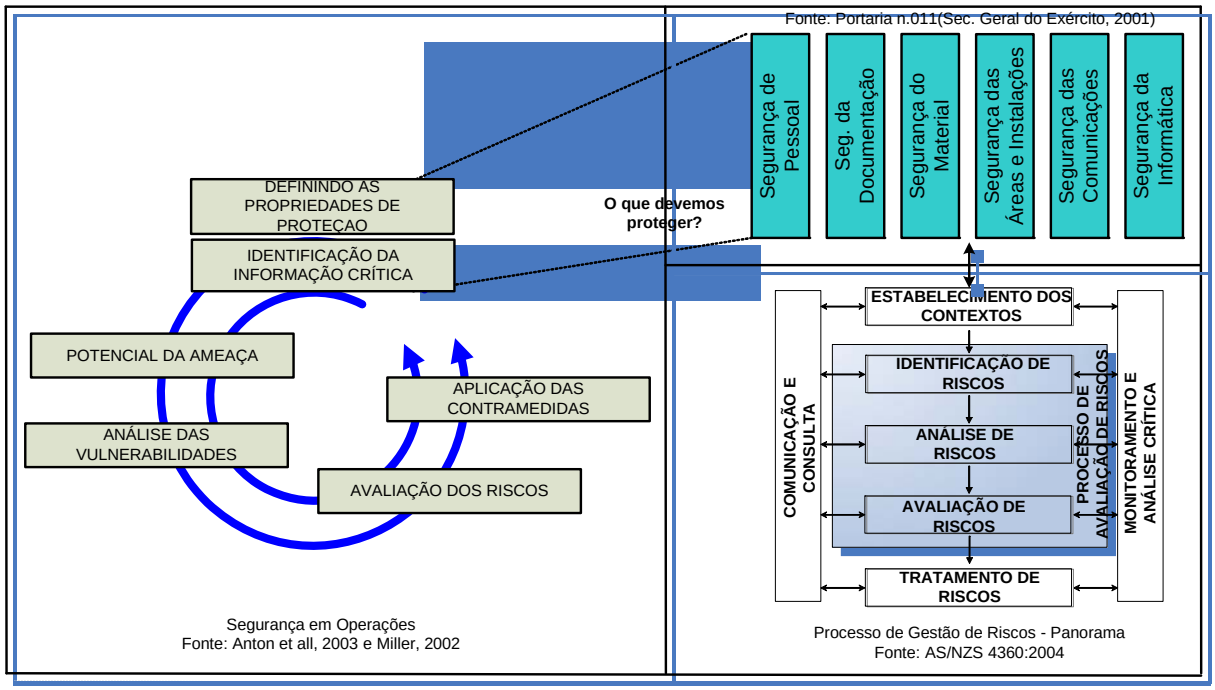
Conforme AZ/NZS 4360 (2004, p.28), a finalidade da identificação e avaliação de riscos é desenvolver uma lista abrangente de fontes de riscos e eventos que podem ter um impacto na consecução de objetivos organizacionais. Para fins desta pesquisa, adapta-se tal afirmação para as vantagens competitivas da organização. Como resultado dessa identificação, formaliza-se uma lista de riscos que poderá ser abrangente, pois os eventuais riscos não identificados podem se tornar uma ameaça à organização ou fazer com que se percam oportunidades importantes.

A ISO/IEC 27001 (2006, p. 3) define a gestão de riscos como sendo um conjunto de atividades coordenadas para direcionar e controlar uma organização no que se refere aos riscos, e a análise de riscos como um processo completo de análise e avaliação de riscos. Mesmo que essa norma possua um escopo voltado para a segurança da informação, ela apresenta uma abordagem para a análise e avaliação de riscos organizacionais como atividade chave para delimitar o escopo a ser contemplado no Sistema de Gestão de Segurança da Informação.

4. Metodologia

A pesquisa deste artigo classifica-se como descritiva quanto aos fins, e documental quanto aos meios. Sendo caracterizada como uma pesquisa que aborda premissas qualitativas. Para a classificação desta pesquisa, tomou-se como base a orientação de Vergara (2000, p.46). O modelo conceitual da pesquisa é apresentado na FIG. 3.

FIGURA 3: Perspectiva e associação dos temas



Fonte: COSME, 2009.

Nesse instante do artigo, sugere-se a aplicação de um questionário (APÊNDICE A), com o objetivo de formalizar junto aos gestores qual o entendimento e grau de importância dos ativos organizacionais (propriedades de proteção) que são reconhecidos como críticas. Por meio desse levantamento, sugere-se delimitar quais os principais ativos que devem ser protegidos no ambiente organizacional. Recomenda-se a seguinte sequência de ações para implantar tal sistemática de identificação:

- identificar os principais Gestores segundo critério a definir (Recomenda-se que o critério para escolha dos gestores deva ser definido considerando a posição funcional estratégica e experiência na função negócio da organização alvo da pesquisa. A forma de aplicação do questionário pode ser a distância via mensagem eletrônica);
- aplicar o questionário junto a esses gestores com objetivo de identificar riscos e delimitar escopo organizacional a ser protegido. Vide matriz (APÊNDICE A);
- para cada risco organizacional, categorizado como alto, propor ações de contramedidas com vistas à proteção organizacional; e
- propõe-se a mensurar a aderência desses controles no tocante à capacidade de identificação, detecção, bloqueio, contramedidas, recuperação e, se necessário, o uso de desinformação das informações atacadas.

5. Resultados e discussão

Visando ao objetivo de convergência dos temas propostos, apresenta-se, nesta seção, como foram construídas as matrizes para identificação e correlação com esses temas. No início deste trabalho, menciona-se que as organizações poderiam acrescentar aos esforços de proteção aspectos de gestão que não estejam exclusivamente relacionados à Tecnologia da Informação. Nesse sentido, apresentam-se as seguintes matrizes de avaliação de riscos com enfase nos aspectos de contrainteligência.

A matriz de levantamento de riscos (Vide APÊNDICE A) foi composta, visando a identificar quais propriedades organizacionais necessitam ser protegidas. Pretende-se, através desse levantamento, que possam ser apresentadas a qualificação dos riscos organizacionais com as suas respectivas ações com responsáveis para o tratamento dos mesmos.

A sua estrutura foi elaborada da seguinte maneira, considerando alguns exemplos:

O primeiro conjunto de campos está organizado para a identificação do risco, sendo formado pelas seguintes questões:

- Descrição do risco: invasão da Rede por colaborador da organização.
- Categoria de ativo organizacional: A categorização do risco identifica a área de conhecimento à qual se aplica. Esse atributo é importante para que o gerenciamento dos riscos possa ser realizado de forma unificada para cada categoria. Os tipos de categorias são: Sistemas, Pessoal, Capacitação, Infraestrutura, Comunicação.
- Processo: Indicação do processo e controle de Redes.

- Descrição do impacto: Descrição dos possíveis impactos negativos que o risco venha a causar na organização, como perda de informações e inclusão de vírus..

O segundo conjunto de campos da matriz relaciona-se com a priorização do risco.

- Fonte e data: Origem do *report* e data.
- Probabilidade e Impacto: Categorizados entre baixo, médio e alto.
- Perda esperada: Célula normalizada para qualificar automaticamente as percepções de probabilidade de ocorrência e o impacto do risco.
- Situação: Categorizado entre ativo, em mitigação, ocorrido e inativo.

A seguir tem-se os campos para associação de ações de Contramedidas ativas e/ou passivas e lista de recursos e responsáveis por essas ações.

- Contramedidas ativas: DTS.
- Contramedidas passivas: *firewallss*, sistemas de detecção de intrusos, tecnologias aplicadas para segurança de redes de identificação, encriptação.
- Recursos e responsabilidades: quais as unidades organizacionais podem estar envolvidas na aplicação dos requisitos de controle e contramedidas associadas.

Com essa estrutura e a aplicação matriz (Vide APÊNDICE A), propõe-se identificar e avaliar os riscos organizacionais e associar quais contramedidas ativas e passivas podem ser utilizadas para a proteção da informação sensível no ambiente organizacional.

6. Riscos e a Contrainteligência

A matriz de identificação (Vide APÊNDICE A) foi composta visando a demonstrar os riscos identificados, o modelo de Segurança em Operações (MILLER, 2002) e as possíveis Contramedidas de natureza ativa e/ou passiva relacionados a cada risco. Pretende-se que, através dessa análise e da associação de risco citado, possa ser apresentada uma contramedida, com vistas a atender as premissas de CI.

O segundo conjunto de colunas da matriz foi constituído pelos cinco processos do modelo de Segurança em Operações (MILLER, 2002).

QUADRO 2 - Cinco processos do modelo de Segurança em Operações

Identificação da informação crítica	Análise do potencial da ameaça	Análise das vulnerabilidades	Avaliação dos riscos	Aplicação das contramedidas
X		**X**	**X**	**X**
X				**X**

Fonte: Elaborado pelo autor a partir de MILLER, 2002

Em seguida, como parte do processo de identificação de riscos, tem-se a associação dos mesmos com os elementos do modelo de proteção da inteligência de negócios, conforme Miller (2002), sendo:

Identificação da informação crítica ou propriedades de proteção: o que é interessante a um concorrente saber sobre uma organização? O que é indispensável a um

adversário ter conhecimento na tentativa de atingir seus objetivos? O que é de interesse de uma organização para se manter protegida? Para fins deste artigo, associam-se, a informações críticas, outros ativos organizacionais, que permitem a um concorrente planejar e agir para garantir fracasso ou consequências inaceitáveis em um meio competitivo.

Análise do potencial da ameaça: quais são os potenciais dos concorrentes na obtenção de informações relacionadas com as propriedades de proteção? Potenciais entendidos como capacidades e propósitos. O que pretendem, por que pretendem e como pretendem chegar à concretização desses objetivos? Associar controles para executar essa avaliação pode ser fundamental para o processo de proteção da inteligência de negócios.

Análise das vulnerabilidades: utiliza-se, nessa etapa, uma abordagem simulada de risco com a atitude de um adversário. Coloca-se na posição de um adversário, ou concorrente, e estudam-se as operações/atividades passo a passo em todas as suas fases a partir do ponto de vista do adversário. A identificação dos pontos fracos no ambiente organizacional também é prevista nesse modelo de processos orientado para a proteção.

Avaliação dos riscos: Essa etapa é decisiva para o processo de Segurança em Operações. Inicia-se com uma estimativa dos efeitos potenciais relativa às vulnerabilidades sobre determinadas operações/ atividades e é seguida por uma análise do custo-benefício para implantação dos controles recomendados. Todavia pode-se considerar essa etapa como não aplicável, isso porque todo o contingente de riscos, nesse instante, já estaria devidamente identificado.

Aplicação das contramedidas adequadas: O acúmulo do conhecimento nessa etapa do modelo torna-se pré-requisito para o ponto alto dessa sistemática. Saber o que é mais importante para a organização proteger; conhecer o potencial de ameaça e quais são as vulnerabilidades. Nesse momento, é necessário planejar e aplicar as ações de defesa para um contexto de eventual ataque.

Aqui não se trata de apenas colocar em prática as contramedidas, conforme Nollan (*apud* MILLER, 2002), de natureza ativa ou passiva, de acordo com Moresi (2008), necessário faz-se realizar uma análise das consequências dessas ações. Uma estimativa de impacto para o uso efetivo das contramedidas é fator essencial a qualquer operação de defesa organizacional. Essencialmente, é fundamental a certeza de que aquilo que você pretende atingir está sendo praticado no mercado. Como extensão dessas aplicações, necessário se faz um exame e a validação se tais contramedidas foram efetivas e, quando houver a possibilidade, de aplicar uma melhoria de caráter contínuo ao processo de proteção. Isso demonstra a necessidade de atividades de análise, conforme Nollan (*apud* MILLER, 2002). Outro processo a ser considerado é a Disseminação, ou seja, a maneira como se dá o processo de comunicação e o retorno aos gestores da organização a respeito dos resultados do processo de proteção. Como dito anteriormente, eventuais retaliações de natureza jurídica podem ser consequência de uma ação.

Como resultados esperados, tem-se a interrelação dos riscos organizacionais com as atividades de CI e quais estariam classificados como mecanismos de proteção ativa e/ou passiva.

Sendo assim, espera-se que esse método apresente o potencial de convergência dos temas desta pesquisa. Áreas do conhecimento que possuem meios de aplicação distintos para fins que podem ser semelhantes. Pretende-se, com esta análise, oferecer um ferramental aos gestores que demonstre uma maior eficiência dos mecanismos de proteção organizacional e a garantia de proteção de vantagens reconhecidas como competitivas.

7.Conclusão

O objetivo deste trabalho foi propor um método para identificar riscos organizacionais em convergência com conceitos relacionados à Contrainteligência, utilizando uma sistemática de identificação e avaliação de riscos como proposição para delimitar o escopo que necessita ser protegido no ambiente organizacional.

Este trabalho considerou como base o modelo de Proteção de Inteligência de Negócios, que possui como premissa considerar o valor do tempo da informação. Corresponde a um entendimento de como uma organização se mobiliza para identificar e quantificar o potencial da perda, se tiver qualquer tipo de ataque de inteligência no seu ambiente. Entende-se que isto é fundamental para se amenizarem os eventuais resultados negativos.

Dos vários entendimentos sobre como manter protegidas tais vantagens competitivas, uma se sobressai, a de que se evite ao máximo precisar aplicar contramedidas para a proteção organizacional. Todavia, no instante em que sejam necessárias, elas devem se fazer presentes e prontas para a ação e defesa da organização, pois a manutenção das vantagens competitivas é aqui, neste artigo, vista como prioritária. Por outro lado, um ponto de atenção foi identificado, na revisão da literatura, de que a aplicação de ações de contrainteligência seja extremamente necessária e justificada. Isso porque, dependendo das ações de contramedidas, podem existir possíveis retaliações jurídicas.

Também como resultado foi apresentado o modelo de Proteção de Inteligência nos negócios com base na Segurança em Operações. Foram apresentadas as 5 perspectivas processuais de Contrainteligência. Para o processo de identificação e convergência dos controles e respectivos temas, foi proposta uma matriz de riscos. Como fundamento para o método de identificação e priorização do que precisa ser protegido, sendo parte da atividade de Identificação da Informação Crítica, foi proposta uma matriz para identificar e priorizar riscos organizacionais.

Como extensão desta pesquisa para trabalhos futuros, sugere-se a aplicação do processo de identificação e a correlação direta ao ambiente operacional de qualquer organização.

Os seguintes itens podem ser partes integrantes desta extensão:

- Ações de vigilância que gerem possíveis conflitos em uma sociedade aberta (*open society*).
- Definição de indicadores de contrainteligência e medições de sua eficácia.
- Formação de gestores com conhecimentos em temas relacionados à Inteligência Competitiva, Contrainteligência.

- Possível reserva de capital para eventuais processos jurídicos.

A expectativa deste trabalho é que a aplicação da matriz e do questionário de riscos propicie a uma organização uma lista de ações a serem implementadas para a proteção de suas vantagens competitivas.

Referências

ABRAIC, Associação Brasileira dos Analistas de Inteligência Competitiva. *Perguntas Frequentes*. Disponível em: < http://www.abraic.org.br/site/faqs.asp> Acesso em 02 abr. 2008

ANTÓN, Philip S.; ANDERSON, Robert H.; MESIE, Richard; SCHEIERN, Michael. *The Vulnerability Assessment & Mitigation Methodology.* Santa Monica: National Defense Research Institute, 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27001:2006: Tecnologia da informação – Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos***.** Rio de Janeiro, 2006.

COSME, R. D.. *Análise de Requisitos de Segurança no Atendimento as Premissas de Contra-inteligência. Brasília.* Dissertação (Mestrado em Gestão do Conhecimento e TI) – Universidade Católica de Brasília, Brasília, 2009.

GLEGHORN, Todd E.. *Exposing the seams*: The impetus for reforming U.S. counterintelligence. California. Thesis – Naval Postgraduate School, California, 2003.

KRISAN, Lisa. Intelligence Essentials for Everyone. *Occasional Paper. Joint Military Intelligence College,* Washington, DC, n. 6, p. 61-70, jun., 1999.

Manual para apresentação de trabalhos acadêmicos da Universidade Católica de Brasília/ coordenação Maria Carmem Romcy de Carvalho... [et al], Universidade Católica de Brasília, Sistema de Bibliotecas. – Brasília: [s.n.], 2008.

McCARTHY, Mary Pat; CAMPBELL, Stuart; BROWNSTEIN, Rob. *Transformação da Segurança Eletrônica*. São Paulo: Pearson Education do Brasil, 2003.

MILLER, Jerry (Org.). *O Milênio da Inteligência Competitiva*. Porto Alegre: Bookman, 2002.

MORESI, Eduardo. *Tópicos de Inteligência Organizacional*. Brasília: Universidade Católica de Brasília, Notas de aula. 2008.

PORTER, Michael. *Vantagem competitiva*: criando e sustentando um desempenho superior. Rio de Janeiro: Campus, 1989.

SECRETARIA GERAL DO EXÉRCITO. *Portaria n.11, de 10 de janeiro de 2001. Aprova as Instruções gerais para salvaguarda de assuntos sigilosos no Exército Brasileiro (IG 10-51).* Boletim do Exército. Brasília, DF, 26 janeiro. 2001. Disponível em: < http://www.dee.ensino.eb.br/legislacao > Acesso em 24 set 2008.

STARRY, Coronel Michael D.; ARNESON, Tenente-coronel Charles W. Jr. *FM 100-6 Operações de Informações. Military Review*. Disponível em: < file://F:\ info op\ FM 100-6 Operações de Informações.htm > Acesso em 09 jun.2008

STANDARDS AUSTRALIA E STANDARDS NEW ZEALAND. *AS/NZS 4360:2004: Gestão de Riscos.* São Paulo: Risk Tecnologia Editora, 2004.

US Army, Field Manual 34-60*. Counterintelligence Operations*. Washington, D.C.: Departament of the Army, p. 34-60, Oct., 1995.

VERGARA, Sylvia Constant. *Projetos e relatórios de pesquisa em administração*. São Paulo: Atlas, 2000.

WILLIS, Henry H.. *Unpublished work on Using Risk Analysis to Inform Intelligence Analysis. WR-464-ISE. RAND Corporation*, Santa Monica, 2007.

APÊNDICE

APÊNDICE A - MATRIZ IDENTIFICAÇÃO DE RISCOS

Definindo propriedades de proteção - Matriz de Riscos

Instruções de Preenchimento
As colunas em amarelo escuro são prenchidas durante a **identificação** do risco e normalmente não são alteradas durante a execução do projeto.
As colunas em amarelo claro são preenchidas durante a avaliação qualitativa dos riscos e periodicamente revisadas durante as reuniões de monitoramento e controle. Todos os riscos de **Perda Esperada Média** ou **Alta** devem obrigatoriamente passar por revisão d
As células em branco contém fórmulas e **não devem ser editadas**

Riscos									
ID	Identificação das proriedades de proteção								
	Descrição					Categoria		Processo	Descrição do Impacto
1	Invasão em sistema de informação					Sistemas			
						Estratégia de Resposta			
	Data	Probabilidade	Impacto	Perda Esperada	Situação	Plano de Mitigação	Plano de Contingência	Recursos	Responsabilidade
	1-mai-08	Alta	Alto	Alta	Ativo				
				#VALOR!					
				#VALOR!					