Contra-inteligência Organizacional: Identificação de Requisitos de Segurança e Priorização de Riscos

Organizational Counterintelligence: Identification of Security Requisites

Rilu Dani Cosme da Silva
Universidade Católica de Brasília

Mestre em Administração pela Universidade Católica de Brasília, UCB-DF
Endereço: Rua Nova, nº 01, Acampamento DFL, Vila Planalto. CEP 70803-170 - Brasília – DF.
Fone (61) 8126-6557
Email: rilu_dani@yahoo.com.br
Lattes: http://buscatextual.cnpq.br/buscatextual/visualizacv.jsp?id=K4445909D7

Eduardo Amadeu Dutra Moresi
Universidade Católica de Brasília

Doutor em Ciências da Informação pela Universidade de Brasília.
Endereço: Universidade Católica de Brasília, QS 07 - Lote 01 - EPCT - Sala C-205 - Águas Claras. 71966-700 - Brasília, DF – Brasil .Telefone: (061) 3356 9025 Fax: (061) 3356 3010
Email: moresi@bol.com.br
Lattes: http://buscatextual.cnpq.br/buscatextual/visualizacv.jsp?id=K4778293H5

Data de submissão: 03 Mar. 2011. **Data de aprovação**: 30 Mar. 2011. **Sistema de avaliação**: *Double blind review*. Centro Universitário UNA. Prof. Dr. Mário Teixeira Reis Neto, Profª. Dra. Wanyr Romero Ferreira

Agência de financiamento: Pesquisa Financiada pela Carta Acordo 2009/11/001 entre a Universidade Católica de Brasília e o Escritório Sobre Drogas e Crimes - UNODC / Nações Unidas, no âmbito do Projeto AD/BRA/05/S07.

Resumo

Este artigo objetiva analisar os requisitos em segurança da informação constantes na norma ISO/IEC 27001 quanto ao atendimento às premissas de contra-inteligência. As áreas de conhecimento neste estudo: Segurança da Informação(SI) e Contra-inteligência(CI). Apresenta-se uma revisão dos conceitos relacionados, fundamentando um método visando à identificação de requisitos de controles que envolvam a Segurança em Operações. Conclui-se da aplicação do método a existência de uma série de requisitos da ISO convergentes com o tema. Ao todo foram identificados 176 requisitos associados com a CI. Deste total foram criados agrupamentos de requisitos denominados de categoria 1, 2 e 3. Essas categorias foram concebidas visando facilitar o processo de identificação ao analisar a associação dos requisitos da norma para com os processos de CI. Na categoria 1 tem-se como característica a associação de 01 requisito de segurança para com 01 processo de CI, nesta categoria foram identificados 51 requisitos. Na categoria 2, tem-se a associação de 01 requisito de segurança com no mínimo 02 ou no máximo 03 processos, nesta categoria foram identificados 46 requisitos. Na categoria 3, a mais abrangente por considerar como condicionante a associação de um requisito com no mínimo 04 ou todos os 05 processos de CI, aqui obteve-se a identificação de 04 requisitos. Em uma análise mais qualitativa percebe-se que os requisitos de segurança direcionados às Ameaças externas e do meio

ambiente; Monitoramento do uso de sistemas; Trabalhos remotos por funcionários; Documentação e Pessoal são os requisitos que mais resguardam o ambiente organizacional da perda de conhecimento sensível.

Palavras-chave: Contra-inteligência; Segurança em Operações; Requisitos de Segurança; Contramedidas; ISO/IEC 27001.

Abstract
This article aims to analyze the control requisites in information security contained in ISO/IEC 27001 regarding the consistence to the Counterintelligence premises. The knowledge areas used in this study are Information Security (SI) and Counterintelligence (CI). Is presented a literature review with the concepts related, substantiating the proposal of a method aimed at identifying requisites for controls involving the Security Operations. It follows from the method the existence of a number of requirements of ISO convergent with the theme. Altogether 176 were identified requirements associated with CI. Of this total were created groupings of requirements called category 1, 2 and 3. These categories were designed to facilitate the identification process to analyze the association of standard requirements for the procedures for IC. In the first category have the characteristic of the association of 01 safety requirements for IC process with 01 in this category were identified 51 requirements. In the second category, we have the association of 01 security requirement with at least 02 or at most 03 CI procedures, 46 were identified in this category requirement. In category 3, the most comprehensive as a condition for considering the combination of a requirement with at least 04 or all 05 cases of IC, we obtained here the identification of 04 requirements.

Keywords: Counterintelligence; Security Operations; Security Requisites; Countermeasures; ISO/IEC 27001.

Introdução

Um espectro de incerteza e insegurança permeia o nosso cotidiano profissional quando o assunto é proteção de vantagens competitivas de uma organização. Talvez o sintoma seja consequência de uma realidade de extrema competitividade na qual se encontram nossas organizações. Vantagens competitivas organizacionais podem, em sua maioria, traduzir-se pelo simples fato de organizações possuírem algum tipo de ativo que possa ser um diferencial em seu modelo de gestão. No que concerne especificamente ao âmbito empresarial, não basta focar somente ações e técnicas relacionadas ao estabelecimento das vantagens competitivas obtidas. 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 trabalho.

Assim, esta questão torna-se pertinente: que mecanismos de segurança podem ser implementados no ambiente organizacional para amenizar essa insegurança?

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 infra-estruturas que sustentam a viabilidade de determinados negócios. Dos vários entendimentos sobre como manter protegidas tais vantagens competitivas, um se sobressai, o de que se minimize a necessidade de aplicar contramedidas para a proteção organizacional, devido à sua complexidade de ações, e eventuais resultados imprevistos. Todavia, no instante em que forem necessárias, elas devem estar presentes e prontas para a ação e defesa da organização.

Como problema de pesquisa, visualiza-se que os requisitos de controle de TI, atualmente vigentes na organização estudada, estão todos voltados para o enfoque em SI, tendo como objetivo atender a poucos requisitos da ISO/IEC 27001:2006. Todavia os demais enfoques de segurança e proteção acontecem na organização de maneira esporádica, muitas das vezes por demandas específicas ou reativas. Perde-se com isso a oportunidade de diagnosticar e tratar uma eventual ameaça ou risco, considerando premissas de contra-inteligência e, consequentemente, podendo minimizar eventual perda de informações organizacionais de caráter sigiloso.

Portanto o objetivo deste trabalho é propor um método para identificar mecanismos de proteção no ambiente organizacional em convergência com conceitos relacionados à Segurança da Informação (SI) e a Contra-inteligência (CI). Como proposição para delimitar o escopo de proteção no ambiente organizacional, foi empregada uma sistemática de Gestão de Riscos (GR) para a identificação e avaliação de riscos.

Conceitos de Contra-inteligência

As atividades de Contra-Inteligência (CI) foram desenvolvidas e adaptadas a partir das técnicas aplicadas no contexto militar e de estado e, no seu sentido mais amplo, tais técnicas são entendidas como sendo as que objetivam neutralizar as ações de espionagem. No que concerne especificamente ao âmbito empresarial, não basta focar somente ações e técnicas relacionadas ao estabelecimento das vantagens competitivas obtidas. Torna-se fundamental a aplicação de técnicas e ferramentas para a manutenção dessas vantagens, incluindo a proteção do chamado conhecimento sensível (ABRAIC, 2008).

A CI, pela perspectiva militar, é definida como um esforço multidisciplinar que contempla a Contra-inteligência Humana (C-HUMINT), a Contra-inteligência de Sinais (C-SIGINT) e a Contra-inteligência de Imagens (C-IMINT) desenvolvidas contra todo processo de coleta de origem externa (FM 34-60, 1995). A força da CI em conjunto com outros ativos de inteligência devem possuir a capacidade de 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 (Equipamentos). Através de sua capacidade analítica, a CI provê recomendações, as quais, se implementadas, irão resultar em negação de informação (*denial of information*) às eventuais ameaças.

O MCWP 2-14 (2000) conceitua a contra-inteligência como sendo a coleta de informações e a condução de atividades que visa a proteger contra espionagem ou outras atividades de inteligência, sabotagem ou assassinatos conduzidos por ou em nome de governos ou elementos estrangeiros, assim como organizações estrangeiras, ou atividades de terrorismo internacional.

Gleghorn (2003, p. 19) se apoia nos referenciais dos manuais FM 34-60 e MCWP 2-14 para afirmar que existem, essencialmente, quatro funções nas quais a contra-inteligência fundamenta-se e opera: coleta, investigação, análise e operações. Enquanto essas quatro funções são derivadas especificamente do FM 34-60 e do MCWP 2-14, os demais organismos de força nacional e o Departamento de Defesa Americano reconhecem que as diretivas de contra-inteligência possuem como princípio essas mesmas funções.

Pela perspectiva civil, as ações de contra-inteligência buscam detectar o invasor, neutralizar sua atuação, recuperar, ou mesmo contra-atacar por meio da produção de desinformação (ABRAIC, 2008). A ABRAIC entende que, especificamente ao ambiente organizacional, não basta focar somente 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.

Quando o processo de decisão envolve as necessidades de segurança e proteção nas organizações, somos impelidos a imaginar somente as perspectivas da tecnologia da informação (TI) como sendo as principais, todavia existem outros aspectos que precisam ser considerados.

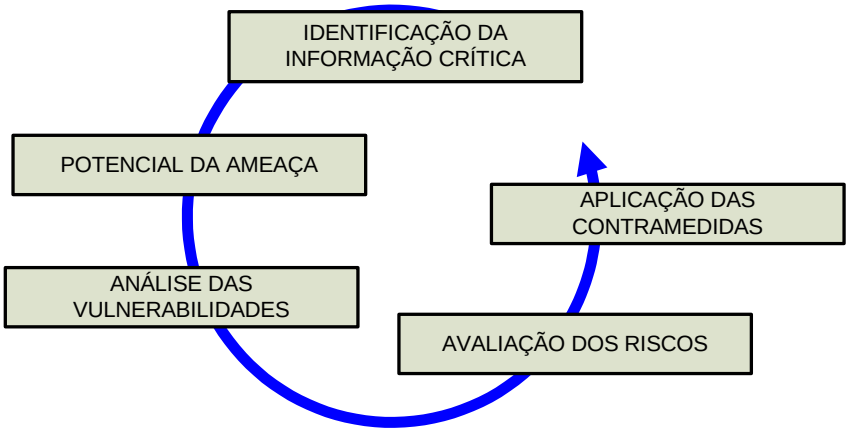
Segundo a Portaria Nr11 do Exército Brasileiro (BRASIL, 2001), com o fim de abranger todas as eventuais vulnerabilidades, as medidas de proteção de CI devem contemplar ações nos mais variados segmentos das instituições. Os domínios de informação sensível relativos à Segurança de Pessoal, da Documentação, do Material, de Áreas e Instalações, da Comunicação e da Informática necessitam de análise e atenção quanto às necessidades de controles e mecanismos de proteção. Essa maior abrangência torna-se fundamental para permitir a redução das vulnerabilidades e ameaças em um ambiente organizacional.

Conforme Kevin Mitnick (*apud* McMarthy; Campbell, 2003, p. 56), as pessoas são o seu melhor ativo de segurança e sua maior vulnerabilidade. Um *hacker* admitiu que raramente precisa-se recorrer a *softwares* de exploração.

Starry e Arnenson (2008) afirmam que, à medida que a tecnologia permite que um maior número de indivíduos, grupos, organizações e nações-estados conectem-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.

Segurança em Operações na Contra-inteligência

O processo de Segurança em Operações é um contraponto ao modelo de Inteligência Competitiva por se configurar na defesa de ações de inteligência. Esse processo representa uma abordagem de contra-inteligência em termos práticos. Essa abordagem trata-se de um processo sistemático que propicia proteção a informações e segredos fundamentais de negócios (QUINN, 2002, p.245). Conforme apresentado na FIG. 1, o objetivo é implantar ações concretas em matéria de capacidades, limitações, atividades e intenções, evitando ou controlando, assim, a exploração por adversários ou concorrentes de negócio.



Fonte: Anton et all, 2003 e Miller, 2002

FIGURA 1: Segurança em Operações

Esse processo contempla uma estrutura de fluxo contínuo de atividades, onde o resultado de cada uma é a saída para as atividades seguintes. O referido autor apresenta o modelo tendo como principal objetivo considerar o valor do tempo da informação. Corresponde ao entendimento de, se qualquer organização sofrer algum tipo de invasão, definir qual seria a capacidade da função Segurança em identificar e quantificar o potencial da perda. Tal postura é fundamental para amenizar os eventuais resultados negativos.

O manual MCWP 2-14 (2000, p.276) conceitua a abordagem de segurança em operações como sendo um processo para identificação de informação crítica e subsequente análise de ações no atendimento e apoio às operações militares e outras atividades com o objetivo de:

- identificar ações que podem ser observadas por sistemas de inteligência adversários;
- determinar indicações de sistemas de inteligência hostis que possam obter ou interpretar de maneira fragmentada informações críticas a tempo de serem úteis aos adversários; e
- selecionar e executar medidas que eliminem ou reduzam a um nível aceitável as vulnerabilidades das ações de exploração adversária.

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

Conforme Miller (2002, p.249), George Lean, o ex-diretor de Segurança em Operações da NSA, comenta que cada uma das fases do Modelo de Proteção é importante para a integridade e eficácia do processo em seu todo. Embora cada uma delas possua valores, isoladamente nessa condição, é só quando se consegue empregá-las em conjunto que se faz possível avaliar o valor sinergético do processo de segurança em operações.

Metodologia

Segundo Vergara (2000, p. 46), a presente pesquisa classifica-se como descritiva quanto aos fins e documental e de campo quanto aos meios. Ela se caracterizada como uma pesquisa mista, abordando premissas qualitativas e quantitativas.
O modelo conceitual adotado encontra-se na FIG. 2 a seguir:

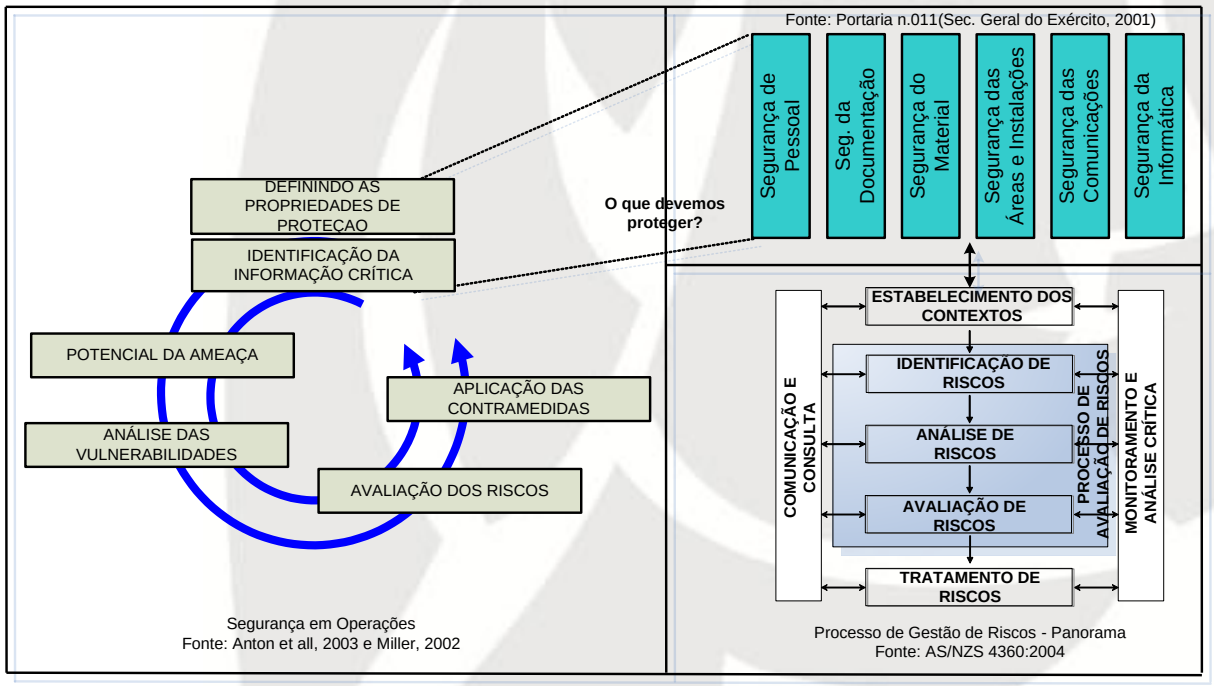


FIGURA 2: Perspectiva e associação dos temas
Fonte: Cosme, 2009

A forma de investigação foi embasada em levantamento bibliográfico e pesquisa de campo. Nesse levantamento foram utilizadas referências bibliográficas dos campos de administração, especificamente de contra-inteligência, segurança da informação e gestão de riscos.

A organização alvo da aplicação foi caracterizada como empresa de grande porte no segmento de TI e com abrangência nacional e internacional. O processo de coleta de dados foi composto por *workshops* e entrevistas com gestores da organização. Conforme os objetivos propostos, a aplicação dos questionários foi caracterizada como uma observação sistemática por meio de planejamento e de condições controladas. O questionário concebido para o *workshop* de levantamento de riscos (vide apêndice A) foi estruturado com questões abertas e de múltipla escolha.

Foram coletados dados e informações relacionados aos eventuais riscos de controles internos, sistemas informatizados e os níveis de interação que validam as operações de controle vigentes. Para fins desta pesquisa, os gestores respondentes foram entendidos como uma amostra não-probabilística e intencional. Os mesmos foram escolhidos tendo como prerrequisito o nível funcional. Pretendeu-se ouvir os respondentes que tivessem níveis de responsabilidade corporativa e de diferentes áreas organizacionais. Assim, os participantes ocupavam as seguintes funções: Gerente de Apoio Comercial, Gerente de Atendimento, Controller, Assessor Controladoria, Assessor da Diretoria de Atendimento, Gerente de Infra-estrutura e TI, Gerente da Qualidade e Coordenador de Auditorias Internas da Qualidade.

Construção do método

Apresenta-se nesta seção como foi construída a matriz para identificação dos requisitos de segurança associados com a contra-inteligência e a relação com os temas propostos.

ISO / IEC 27001 e a Contra-inteligência

A matriz de identificação foi composta visando a integrar a estrutura da ISO/IEC 17799 (2005), o modelo de Segurança em Operações apresentado por Quinn (2002, p.245) e as possíveis Contramedidas de natureza ativa e/ou passiva. Pretendeu-se que, através desta análise e da associação de cada item citado, fosse obtida uma identificação dos requisitos de controle para atender as premissas de CI.

A sua estrutura foi elaborada seguindo três etapas. Conforme o QUADRO 1. Na primeira etapa, cada requisito de controle constante na ISO foi listado na 1ª coluna da matriz de identificação, ao todo foram citados os 133 controles, conforme a estrutura original da norma.

QUADRO 1 – Coluna de Identificação dos Requisitos de Controle

ISO 27001		
item	Controle	Descrição
1	A.5.1.1	Documento de política de segurança da informação
2	A.5.1.2	Análise crítica da política de segurança da informação

Fonte: ISO/IEC 17799 (2005)

O conjunto dos requisitos de segurança apresentado pela ISO/IEC 17799 possui uma estrutura que consiste em 11 seções de controle, 39 objetivos de controle e 133 controles. Segundo Karabacak e Sogukpinar (2006), esta é considerada a principal norma voltada para a segurança da informação. Considerada como um código de práticas que contempla 133 controles em 11 diferentes domínios de

segurança. Apresenta considerável número de requisitos de controles que podem ser utilizados pelas organizações para checar o quanto estão em conformidade com as orientações normativas.

Conforme o QUADRO 2, a segunda etapa consistiu na identificação das colunas da matriz, constituída pelos cinco processos do modelo de Segurança em Operações.

QUADRO 2 – Matriz de Identificação e Associação dos Requisitos com a CI

Item	Segurança em Operações		Identificação da informação crítica	Análise do potencial de ameaça	Análise das vulnerabilidades	Avaliação dos riscos	Aplicação das contramedidas
82	A.11.4.2	Autenticação para conexão externa do usuário	x		x	x	x
83	A.11.4.3	Identificação de equipamento em redes	x				x

Fonte: Quinn (2002, p. 245)

No terceiro passo, as duas colunas que devem encerrar a matriz citam os tipos de contramedidas (Contramedida ativa e Contramedida passiva)

Como resultado, obteve-se uma estrutura que permitiu analisar a interrelação entre os requisitos de controles e os processos de CI, e quais destes podem ser classificados como mecanismos de proteção ativa e/ou passiva.

Método de aplicação

A aplicação da matriz de identificação considerou as marcações de cada requisito de controle, relacionando com as perspectivas processuais do modelo de Segurança em Operações. Dada cada relação, a matriz também contemplou a existência de possíveis contramedidas ativas e/ou passivas na estrutura da norma ISO/IEC 27001 (2006).

A principal questão a ser respondida: quais são os requisitos de controle e o percentual de cobertura desses requisitos da ISO/IEC 27001 no atendimento às premissas de Contra-inteligência?

O método utilizado aplicou uma simples fórmula matemática na estrutura da matriz, sendo:

$$\% \text{ Cob} = \sum \text{RQaPSO} / (\sum \text{RQ} * \sum \text{PSO}) * (1)$$

Onde:

% Cob é o Percentual de Cobertura;
RQaPSO é a Quantidade total de Requisitos de Controle no Atendimento aos Processos de Seg. em Operações;
RQ é a Quantidade de Requisitos de Controle previstos na ISO 27001; e
PSO são as Etapas do Modelo de Segurança em Operações.

Conforme a TAB. 1, foi identificada a variável $\sum$ **RQaPSO**, sendo a quantidade dos requisitos de controle identificados que possuem alguma relação com as premissas de CI.

TABELA 1 – Quantidade dos Requisitos de Controle e a relação com a CI

Etapas em Segurança em Operações	Quantidade de Requisitos de Controle	% de cobertura
Identificação da informação crítica	45	26%
Potencial de ameaça	4	2%
Análise de vulnerabilidades	42	24%
Avaliação dos riscos	10	6%
Aplicação das contramedidas	75	43%
Total	176	100%

Fonte: Elaborado pelos autores com os dados da pesquisa

Conforme a TAB. 2, foi identificada a variável **∑ RQ * ∑ PSO**, sendo o somatório total dos requisitos de controle pelo total das etapas do modelo de segurança em operações.

TABELA 2 – Requisitos de Controle pelo total das etapas da Segurança em Operações

Quantidade	Abrangência (SI x CI)
133	Requisitos de controle da ISO / IEC 27001
5	Etapas do modelo de Segurança em Operações
665	

Fonte: dados da pesquisa

Conforme a TAB. 3, foi identificado percentual de cobertura, assim representado como **% Cob = ∑ RConPSO/ ∑ RCon * ∑ PSO,** onde tem-se a quantidade de Requisitos de Controle identificados e relacionados com as premissas de CI dividido pelo Somatório total dos Requisitos de Controle multiplicado pelas etapas do modelo de Segurança em Operações.

TABELA 3 – Percentual de Cobertura

Quantidade	Abrangência (SI x CI)	% de cobertura
133	Requisitos de controle da ISO / IEC 27001	176
5	Etapas do modelo de Segurança em Operações	
665		26%

Fonte: Elaborado pelos autores com os dados da pesquisa

A consistência da etapa de identificação relativa à associação dos Requisitos de Controle x Processos de CI foi validada pelo preenchimento da matriz por 2 profissionais com certificação como auditor líder (*Lead Auditor*) pelo IRCA na ISO/IEC 27001.

Avaliação de riscos de operações de informações

Este item analisa a função de avaliação de riscos como proposta de um método para definir o critério de identificação das propriedades de proteção no ambiente organizacional. O

método teve como finalidade responder a questões que envolvam os interesses e receios dos principais gestores organizacionais relacionados aos itens de proteção.

Nessa etapa, foram aplicados dois questionários, 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 críticos. Por meio desse levantamento, delimitou-se quais os principais ativos que devem ser protegidos no ambiente organizacional e quais possíveis contramedidas podem ser aplicadas.

Dessa maneira, recomenda-se a seguinte sequência de ações para implantar tal sistemática de identificação: planejar uma atividade de *workshop* para aplicar o método de identificação e priorizar os riscos no ambiente organizacional; por meio do questionário, identificar quais os riscos que a organização está ou foi exposta; identificar o(s) Gestor(es) e área de atuação que formalizou o risco; associar a cada risco a categoria à qual está relacionado; associar o processo inerente a cada risco; associar para cada risco o impacto do evento ou incidente, como consequência no ambiente organizacional; definir quais requisitos de controle da ISO/IEC 17799 (2005) podem ser relacionados; determinar quais Contramedidas Ativas e Passivas podem ser aplicadas para o tratamento do risco em questão; e associar para cada risco quais recursos e responsáveis devem ser dispostos para a aplicação das referidas contramedidas.

A matriz de identificação riscos organizacionais

Neste item é apresentado um modelo de matriz que se propõe a identificar e priorizar quais ativos organizacionais possuem correlação com as premissas de Contra-inteligência.

A proposta da sistemática de identificação é a de listar todos os principais ativos organizacionais vigentes na organização. Na mesma estrutura da matriz, estão identificados possíveis riscos relacionados aos ativos, as categorias de processos e a descrição dos impactos dos respectivos riscos. A identificação, análise e a associação de cada risco aos ativos organizacionais fornecem um critério de priorização de quais requisitos de controle poderiam atender as premissas de CI, quanto à proteção dos respectivos ativos organizacionais, entendidos como aspectos de vantagem competitiva. Vide matriz no Apêndice B. Com essa estrutura, foi possível identificar e avaliar os riscos organizacionais e associar quais requisitos de controle presentes na ISO/IEC 27001 e na ISO/IEC 17799, e quais contramedidas ativas e/ou passivas poderiam ser utilizadas para a proteção da informação sensível no ambiente organizacional. Tais ações de proteção podem estar presentes nessas normas ou podem ser de conhecimento dos especialistas em segurança envolvidos nessa etapa do levantamento.

Resultados e discussão

No início deste trabalho foi mencionado que, em geral, as organizações poderiam acrescentar aos esforços de segurança da informação outros aspectos de gestão que não sejam preferencialmente a TI. Assim há um risco inerente a essa postura, que considera somente aspectos tecnológicos, de perdas de informações sensíveis acontecerem por outras vias, seja por pessoas, por documentação não controlada, por áreas ou instalações inseguras, entre outras. Nesse sentido, decidido discorrer sobre os requisitos de segurança da informação identificados ao considerar premissas de contra-inteligência. A identificação de tais requisitos é necessária para analisar a possível implantação de mecanismos de defesa e/ou proteção organizacional em um contexto empresarial e com a aplicação complementar da avaliação de riscos para atestar as condicionantes propostas.

Conforme a TAB. 4, na aplicação das matrizes de identificação, pode-se observar que os requisitos de segurança referenciados pela ISO 27001 e ISO 17799 foram validados como uma abordagem parcial às necessidades de proteção a partir das premissas de contra-inteligência. As matrizes de identificação aplicadas mostraram que os atendimentos desses requisitos de controle correspondem a 26% de cobertura frente a esses conceitos. As matrizes de identificação também revelaram que a norma possui 85% de contramedidas passivas e 15% de contramedidas ativas.

TABELA 4 – Identificação de Requisitos; Percentual de Cobertura e Contramedidas

	Etapas da Segurança em Operações	Quantidade de Requisitos de Controle	% de cobertura
	Identificação da informação crítica	45	26%
	Potencial de ameaça	4	2%
	Análise das vulnerabilidades	42	24%
	Avaliação dos riscos	10	6%
	Aplicação das contramedidas	75	43%
		176	100%

Quantidade	Abrangência (SI x CI)	% de cobertura
133	Requisitos de controle da ISO / IEC 27001	176
5	Etapas do modelo de Segurança em Operações	
665		26

	Contramedidas	Quantidade Requisitos	
	Ativa	8	15%
	Passiva	45	85%
	Quantidade	53	100%

Fonte: Elaborado pelos autores com os dados da pesquisa

Com o objetivo de facilitar o processo de identificação como resultado da pesquisa, os requisitos de segurança foram categorizados tendo como principal característica a relação com os conceitos de CI. Com essa classificação, pretendeu-se identificar quais agrupamentos de requisitos de segurança possuem relação direta com os conceitos de CI. Após essa análise, observou-se que o agrupamento denominado de categoria 1 foi definido como sendo o conjunto de requisitos de segurança que possui relação direta com no mínimo 1 processo de CI. Na categoria 2, tem-se a relação com no mínimo 2 e no máximo 3 processos e, na categoria 3, apresentam-se os requisitos relacionados com no mínimo 4 ou com todos os processos de CI. Obteve-se assim a TAB. 5 como resultado desta classificação.

TABELA 5 – Categorias de Requisitos

Categorias	Quantidade de requisitos x conceitos CI	%
Categoria 1	51	50%
Categoria 2	46	46%
Categoria 3	4	4%
Quantidade	101	100%

Fonte: Elaborado pelos autores com os dados da pesquisa

Os requisitos de segurança da ISO 27001 das categorias 1 e 2 em conjunto obtiveram 96% da abrangência relacionada com a contra-inteligência. Os 4% restantes da categoria 3 representam um agrupamento de requisitos com uma abrangência bastante completa frente aos processos de CI.

Definição do Escopo de Proteção

Do processo de levantamento de riscos, participaram os representantes dos seguintes níveis funcionais na organização em questão: Assessoria de Segurança, Gerência da Qualidade, Gerência Comercial, Gerência de TI, Assessoria da Diretoria de *PMO* e Controladoria. Todos esses profissionais participam ativamente no processo decisório da organização e suas responsabilidades são corporativas.

O *workshop* teve como finalidade a aplicação do formulário para levantamento de riscos. Conforme apresentado na TAB. 6, foram identificados 117 riscos organizacionais. Pelo instrumento de pesquisa tais riscos estão diretamente associados aos 6 domínios de segurança (BRASIL, 2001).

TABELA 6 – Riscos Organizacionais

Contar de Domínio	Domínio						
Perda esperada	Áreas e instalações	Comunicação	Documentação	Informática	Material	Pessoal	Total geral
Alta	9	6	22	18	11	21	87
Baixa				1	1	1	3
Média	4	4	5	8	1	5	27
Total geral	13	10	27	27	13	27	117
% riscos	11%	9%	23%	23%	11%	23%	
%riscos categoria *f*	10%	7%	25%	21%	13%	24%	

Fonte: elaborado pelos autores com os dados da pesquisa

Validação preliminar

Com o objetivo de realizar uma validação preliminar da pesquisa, foram submetidos a uma pesquisa semi-estruturada dois especialistas em segurança da informação. Os mesmos preencheram um questionário em que foram coletadas informações quanto ao perfil do

especialista, informações sobre como funciona controles de segurança somente pela visão da ISO, qual seria a utilidade do método a partir da visão da contra-inteligência e a caracterização de contribuições para esta pesquisa que fossem pertinentes.

Os respondentes atuam como Gestores nas áreas de Suporte e *Outsourcing* (ênfase em ITIL) e como auditores líderes segundo as normas NBR ISO 9001, TL 9000, QWeb e *GoodPriv@cy*. Considerando o conhecimento sobre o tema, cabe ressaltar que os respondentes possuem as seguintes certificações: Certificado MS-MCSE (*Microsoft Certified System Engineer*) e Certificado NSAE-DoD (*National Security Agent Engineer-Department of Defense*).

Segundo a percepção dos mesmos, atualmente os controles de segurança com foco na ISO 27001 não são capazes de reagir aos ataques e vazamento de informações do seu ambiente computacional a tempo de impedir prejuízos financeiros diretos e indiretos aos negócios. Sendo assim, o maior desafio das empresas é aplicar Gestão à Segurança de forma estratégica, alinhando a TI com técnicas de Contra-Informação. Outro entendimento é o de que a base de processos continua sendo a reação aos acontecimentos e não uma ação pró-ativa.

Eles entendem que o método pode ter a sua utilidade na aplicação onde as empresas passam a gerenciar a Segurança das Informações, desenvolvendo estratégias pró-ativas, analisando todos os riscos para o processo de negócio do ponto de vista da competição de mercado. A elaboração de um trabalho voltado para a Gestão da Segurança com Inteligência permitirá que as empresas analisem com eficiência o estado atual do ambiente, determinando o grau de proteção dos ativos em informações contra possíveis ameaças. Sendo assim, os esforços e orçamentos serão direcionados para atividades mais prioritárias para o processo de negócios.

Para que o método proposto possa ser efetivo, recomenda-se que o corpo gestor da organização possua a capacidade de tomar decisões rápidas e precisas; que haja comprometimento da Alta Direção, pois determinadas decisões que envolvam o uso de contramedidas possuem uma alta carga de responsabilidade; que a organização reconheça a possibilidade de altos investimentos em controles preventivos; que haja reserva de capital para eventuais processos jurídicos; que se mantenha no quadro funcional equipes multiespecializadas em segurança física e lógica no ambiente tecnológico; e que a organização em foco esteja atenta quanto à capacitação de gestores nos temas Inteligência Competitiva, Contra-inteligência e Segurança da Informação.

Conclusões

Nos tempos atuais, o mercado global preconiza a necessidade das organizações conquistarem diferenciais competitivos como a força-motriz para se manterem bem sucedidas em determinados segmentos de negócios. Muito se investe na conquista de vantagens competitivas empresariais. Diferenciais tecnológicos, de conhecimento, na formação de equipes de alto desempenho e os mais variados esforços fazem-se presentes nas arenas competitivas do mercado. Por outro lado, quais seriam as capacidades organizacionais e motivacionais que tais empresas possuem para manter e proteger esses diferenciais competitivos? Foi com essa pergunta que se iniciou este trabalho de pesquisa. E é ao tentar achar respostas por meio do processo metodológico e científico que se percebe o quanto esse assunto poderia ser mais explorado nos ambientes acadêmicos e empresariais. As linhas mestras deste estudo focalizaram o processo de Contra-inteligência pelas publicações de organismos do segmento militar e de segurança de estado e conceitos de Segurança da Informação pelas normas ISO.

Conclui-se, por meio da aplicação da matriz de identificação dos requisitos de segurança com foco na contra-inteligência, a existência de uma série de requisitos da ISO que são convergentes com esse tema. Ao todo foram identificados 176 requisitos associados com a

CI. Desse total foram criados agrupamentos de requisitos denominados de categoria 1, 2 e 3. Essas categorias foram concebidas com o intuito de facilitar o processo de identificação ao analisar a associação tanto de requisitos da norma para com os processos de CI, quanto inversamente. Na categoria 1, tem-se como característica a associação de 1 requisito de segurança para com 1 processo de CI, nessa categoria foram identificados 51 requisitos. Na categoria 2, tem-se como atributo a associação de 1 requisito de segurança com no mínimo 2 ou no máximo 3 processos de CI, nessa categoria foram identificados 46 requisitos. Na categoria 3, a mais abrangente por considerar como condicionante a associação de um requisito com no mínimo 4 ou todos os 5 processos de CI, aqui obteve-se a identificação de 4 requisitos de segurança definidos pelas normas ISO/IEC 27001:2006 e ISO/IEC 17799:2005.

Outro aspecto resultante da pesquisa e também relacionado com o processo de identificação foi apresentar por meio do cálculo da quantidade de requisitos associados com o tema CI qual seria o percentual de cobertura das referidas normas. O valor 26% de cobertura surge como resultante dessa aplicação teórica, isso traz o entendimento de que o atual conteúdo da norma é parcial frente às necessidades de proteção, tendo a CI como principal referência ao envolver outros aspectos de gestão.

Outro produto da pesquisa foi definir qual seria o escopo de proteção organizacional. Aqui, com o valor agregado, outros aspectos de gestão estariam sendo considerados. Para esse objetivo, foi concebida uma matriz de levantamento de riscos. Essa matriz foi aplicada por meio de uma série de *workshops*, realizados tendo como premissa a participação de gestores da organização em questão. Como resultado desse diagnóstico, pode-se formalizar 117 riscos organizacionais. Nesse levantamento, foram avaliadas as perdas esperadas de riscos ao considerar as variáveis de probabilidade de ocorrência e impacto como alto, médio e baixo. Os riscos foram assim identificados e associados, conforme os domínios de segurança, em primeiro, o domínio de Documentação (23%); em seguida, Pessoal (23%); Informática (23%); Material (11%); Áreas e instalações (11%); e Comunicação (9%). Ao considerar riscos com alta prioridade tem-se a seguinte configuração, Documentação (25%); Pessoal (24%); Informática (21%); Material (13%); Áreas e instalações (10%); e Comunicação (7%).

Em uma análise mais qualitativa, percebe-se que os aspectos Documentação e Pessoal foram os que mais preocuparam os gestores, quando a decisão estiver relacionada com a perda do conhecimento sensível. Nesses segmentos, pode-se relacionar: as atividades relacionadas com informações críticas de fácil acesso a pessoas não autorizadas; a ausência de diretrizes para controle de informações sigilosas; e atos ilícitos cometidos por profissionais na organização que se sobressaíram como os quesitos de maior preocupação. Consequentemente, por meio deste estudo, sugere-se que os maiores investimentos no tocante à implantação de requisitos de controle previstos nas normas devem ser direcionados à mitigação e ao contingenciamento nessas atividades organizacionais.

Ao encerrar as atividades de pesquisa relacionadas com o processo de medição de cobertura da norma, identificação dos requisitos de segurança e do levantamento de riscos, iniciou-se uma sistemática de validação preliminar da pesquisa. Tal validação foi realizada com a aplicação de um questionário semi-estruturado com 2 especialistas de segurança da informação. As questões do questionário foram relativas a informações do perfil do respondente; informações sobre como funciona controles de segurança somente pela visão atual da ISO; qual seria a utilidade do método a partir da visão da contra-inteligência e a caracterização de contribuições que fossem pertinentes para esta pesquisa. A percepção dos especialistas referente ao método foi de que, nesse cenário em que se deve garantir a autonomia de processos que geram, tratam e manejam a informação, motor propulsor dessa nova sociedade, deve-se estar preparado para gerenciar a segurança da informação de maneira efetiva, por meio do conhecimento e da utilização de formas sistêmicas e planejadas, e o método proposto vem apoiar a análise cartesiana da análise de riscos. Outro

entendimento relatado foi o de que, com a aplicação do método proposto, as empresas passam a gerenciar a Segurança das Informações desenvolvendo estratégias pró-ativas, analisando todos os riscos para o processo de negócio do ponto de vista da competição de mercado. A elaboração de um trabalho voltado para a Gestão da Segurança com Inteligência permitirá que as empresas analisem com eficiência o estado atual do ambiente, determinando o grau de proteção dos ativos em informações contra possíveis ameaças. Dessa maneira, os esforços e orçamentos poderão ser direcionados para as atividades mais prioritárias ao processo de negócios.

Como extensão desta pesquisa para trabalhos futuros, sugere-se a aplicação prática do processo de identificação e a análise direta no ambiente operacional de qualquer organização. Os seguintes temas podem ser partes integrantes desta extensão: Ações de vigilância que gerem possíveis conflitos com uma sociedade; Protocolos para relações internacionais quanto à conduta e investigação em *cybercrimes*; Aplicação e análise criteriosa de Contramedidas com muita complexidade em ações; Elementos de um segredo de negócios ao considerar sigilo: valor; Precauções razoáveis do proprietário; Diretrizes para a proteção de segredos de negócios e propriedades intelectuais; Da comparação com grupos de funções com as operações de inteligência de negócios; Valor do dinheiro no tempo x Valor da informação que se quer proteger; e Análise de Contramedidas quanto àquilo que você pretende atingir e o que está sendo praticado no mercado.

Referências

ABRAIC, Associação Brasileira dos Analistas de Inteligência Competitiva (n.d.). Perguntas Frequentes. http://www.abraic.org.br/site/faqs.asp Acesso em 02 abril 2008.

ANTÓN, P. S., & Anderson, R. H., Mesie, R. & Scheiern, M. *The Vulnerability Assessment & Mitigation Methodology.* Santa Monica: National Defense Research Institute, 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS . ABNT NBR ISO/IEC 17799:2005: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro.

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.

BRASIL. 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). http://www.dee.ensino.eb.br/legislacao. Acesso em 24 setembro 2008.

COSME, R. D. Análise de Requisitos de Segurança no Atendimento as Premissas de Contra-inteligência. Brasília. 2009. 88 f. Dissertação (Mestrado em Gestão do Conhecimento e TI) – Universidade Católica de Brasília, Brasília, 2009.

GLEGHORN, T. E. Exposing the seams: The impetus for reforming U.S. counterintelligence. California. 2003. 92 f. Thesis – Naval Postgraduate School, California. 2003.

KARABACAK, B. & Sogukpinar, I. A quantitative method for ISO 17799 gap analysis: Elsevier. 2006.

MCCARTHY, M. P. & Campbell, S. *Transformação da Segurança Eletrônica*. São Paulo: Pearson Education do Brasil, 2003.

MILLER, J. *O Milênio da Inteligência Competitiva* (Org.). Porto Alegre: Bookman, 2001.

NOLLAN, J. A. *Inteligência e Segurança nos Negócios*. In: Miller, J. (Org.). *O Milênio da Inteligência Competitiva.* Porto Alegre: Bookman, 2002. p. 230 a 245.

QUINN, J. F. A Segurança em Operações e as Contramedidas da Inteligência Competitiva. In: MILLER, Jerry (Org.). *O Milênio da Inteligência Competitiva*. Porto Alegre: Bookman, 2002. p. 245 a 249.

SAUNDERS, K. Open Source Information – A True Collection Discipline. Canada. 2000. 85. Dissertação (Mestrado em *Studies War*) – Royal Military College of Canada, Canada. 2000.

STARRY, Coronel M. D. & Arneson, Tenente-coronel C. W. Jr. (n.d.). FM 100-6 Operações de Informações. Military Review. file://F:\ info op\ FM 100-6 Operações de Informações.htm Acesso em 09 de junho 2008.

TZU, S. *A Arte da Guerra.* Adaptação e prefácio de James Clavell.; tradução de José Sanz, 26. ed. , Rio de Janeiro: Record, 2001.

US Army, Field Manual. Information Operations. Washington, D.C.: Department of the Army, n. 100-6. 1996.

US Army, Field Manual. Counterintelligence Operations. Washington, D.C.: Department of the Army, n. 34-60. 1995.

US Navy, Marine Corps Warfighting Publication. Counterintelligence. Washington, D.C.: Department of the Navy, n. 2-14, September. 2000.

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