UMA PROPOSTA DE ONTOLOGIA DE DOMÍNIO PARA SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES:
descrição do estágio terminológico

Maurício Barcellos Almeida *
Renato Rocha Souza **
Kátia Cardoso Coelho ***

Resumo A evolução da tecnologia tem facilitado a disseminação da informação no contexto organizacional e inter-organizacional. A disponibilidade de informação, aliada a um ambiente de negócios competitivo, tem conferido importância cada vez maior à segurança da informação. Ainda que se perceba a necessidade de implementá-la, em geral não há clareza sobre o que deve ser protegido e sobre como fazê-lo. O presente artigo apresenta uma visão geral da pesquisa na área, descreve iniciativas e destaca a importância de classificar a informação no ambiente corporativo para fins de segurança. Advoga-se o uso de ontologias como alternativa para tal classificação e apresenta-se como resultado parcial de pesquisa em andamento o estágio terminológico de uma ontologia de domínio sobre segurança da informação. O objetivo é contribuir para a pesquisa sobre o assunto no âmbito da Ciência da Informação, bem como nortear o trabalho de profissionais de informação e de gerentes responsáveis por projetos de segurança.

Palavras-Chave: Segurança da Informação. Ontologias. Ciência da Informação. Gestão do Conhecimento.

* Professor adjunto do Departamento de Teoria e Gestão da Informação, Escola de Ciência da Informação, Universidade Federal de Minas Gerais. www.eci.ufmg.br/mba/

**Professor adjunto do Departamento de Organização e Tratamento da Informação. Escola de Ciência da Informação, Universidade Federal de Minas Gerais.
E-mail: rsouza@eci.ufmg.br

*** Mestranda do Programa de Pós-Graduação em Ciências da Informação, Escola de Ciências da Informação, Universidade Federal de Minas Gerais.
E-mail: katiaccoelho@gmail.com

1 Introdução

A expressão *segurança da informação*, em geral, tem sido associada a sistemas informatizados e aos dados que estes manipulam. Diz respeito a uma série de aspectos associados à Tecnologia da Informação (TI), como por exemplo, controle de acesso a recursos, segurança em comunicação, gestão de riscos, políticas de informação, sistemas de segurança, diretrizes legais, segurança física, criptografia, dentre outros (KRAUSE; TIPTON, 1997). Entretanto, cabe destacar que a questão não se limita apenas à proteção de dados em computadores e em redes, uma vez que uma organização não possui apenas dados em formato digital. Além disso, uma empresa não mantém controle sobre todas as informações a seu respeito como, por exemplo, a informação disponível em instituições do governo, conselhos de classe, fornecedores, dentre outros. Segurança também pode envolver questões de natureza física, política e cultural.

Para muitas organizações, a segurança da informação é uma necessidade de negócio e ainda assim, nem sempre práticas dessa natureza são adotadas, visto que projetos e recursos necessários são caros, complexos, demandam tempo e não garantem efetividade. Problemas na implementação de estratégias de segurança da informação começam pela dificuldade em definir o que deve ser protegido, qual nível de

proteção necessário e quais ferramentas devem ser utilizadas no ambiente corporativo. Cabe ainda à organização descobrir em que contexto se manifesta a informação relevante para seus objetivos de negócio, bem como as necessidades corporativas em relação à segurança. Essas necessidades são influenciadas por fatores humanos e por fatores inerentes ao próprio ciclo de vida da informação.

Para lidar com a complexidade da questão, as empresas se valem de mecanismos de proteção baseados em políticas de segurança da informação, da análise de riscos e da classificação da informação (FOWLER, 2005). Uma *política de segurança* é um plano de alto nível que estabelece como a segurança deve ser praticada e em que nível de segurança – com custos e benefícios inerentes – a organização está disposta a aceitar. A *análise de riscos* consiste na prática de confrontar o valor da informação com os riscos inerentes às perdas, bem como identificar meios de proteção para reduzir riscos. Os procedimentos de *classificação da informação* agrupam entidades similares em categorias, possibilitando implementar medidas de proteção com vistas à garantia da confidencialidade da informação.

O presente artigo destaca a importância da classificação da informação em questões de segurança. Como alternativa, apresenta-se uma abordagem baseada em ontologias, bem como os resultados parciais de pesquisa em andamento. Esses resultados correspondem ao *estágio terminológico* de uma ontologia de domínio sobre segurança da informação. O estágio terminológico é a primeira etapa de um processo em que se formaliza gradualmente o conhecimento de um domínio. Segundo Almeida (2006), o processo se inicia em um estágio denominado *informal* (ou *terminológico*), passa por estágios intermediários, até alcançar o estágio denominado *formal*. Justifica-se a apresentação de resultados parciais de pesquisa face à importância crescente do tema e da escassez de iniciativas relacionadas no campo da Ciência da Informação (CI).

Espera-se contribuir para a pesquisa em CI por meio da apresentação de uma visão geral sobre a literatura no assunto, além de material de apoio aos profissionais da informação e gerentes na condução de projetos de segurança. O restante do presente artigo está dividido conforme segue: a seção dois apresenta considerações sobre segurança da informação nas organizações, destacando os principais tipos de iniciativas; a seção três enfatiza iniciativas que envolvem TI e ontologias, além de apresentar os resultados do estágio terminológico de uma ontologia experimental sobre segurança da informação; finalmente, a seção quatro apresenta conclusões, considerações finais e perspectivas de trabalhos futuros.

2 Visão geral das iniciativas para segurança da informação

Existem diversos tipos de iniciativas para lidar com problemas de segurança da informação, dentre as quais se destacam as governamentais, as normativas e as tecnológicas. A seção 2.1 apresenta exemplos de iniciativas governamentais e normativas, enquanto a seção 2.2 descreve iniciativas de caráter tecnológico.

2.1 Iniciativas governamentais e normativas

Uma iniciativa pioneira sobre segurança para informações de caráter científico ocorreu no âmbito da *Federation of American Scientists*, associação formada em 1946 pelos cientistas atômicos do *Projeto Manhattan*[1]. Ao descrever tal iniciativa, Quist (1993) discute a necessidade de uma classificação da informação para fins de segurança e descreve três ações principais, a saber: i) determinar se a informação deve ser classificada; ii) determinar o nível de classificação; iii) determinar a duração da classificação. O autor apresenta os seguintes procedimentos para avaliar se a informação deve ou não ser classificada: i) definir precisamente a informação, descrevendo-a em uma linguagem sem ambigüidades; ii) verificar a existência de classificação específica para o setor da organização em que a informação foi obtida; iii) verificar se a informação é controlada pelo governo; iv) determinar se a divulgação da informação causará danos à segurança nacional; v) especificar precisamente porque a informação deve ser classificada.

O ISOO (2003) estabelece um sistema de classificação para segurança da informação no governo norte-americano. Algumas regras sobre classificação de documentos são especificadas, como por exemplo: i) apenas pessoas autorizadas

1 Projeto para desenvolvimento da primeira arma nuclear, iniciado ainda na 2ª Guerra Mundial.

podem classificar documentos originais; ii) apenas três níveis de classificação devem ser utilizados: *super-secreto*, *secreto* e *confidencial*; iii) informações que não sejam de interesse da segurança nacional, não devem ser inseridas no sistema de classificação. O ISOO (2003) descreve ainda marcas obrigatórias que, aplicadas aos documentos originais, identificam os níveis de segurança a adotar: i) marcas em partes do documento, caso essas partes possuam diferentes classificações; ii) classificação do documento como um todo, considerando-se o nível de classificação mais restrito atribuído a uma parte do documento; iii) inserção de campos específicos no documento, como por exemplo: *classificado por*, *razão da classificação* e *data final da classificação*.

No Canadá, o *Government of Alberta* (2005) dispõe de um sistema de classificação de documentos que tem por objetivo proteger a informação pessoal e confidencial contra acesso não autorizado, proteger a propriedade intelectual do governo, dar suporte a disseminação de informação e possibilitar cooperação inter-governamental para segurança pública. O sistema de classificação identifica quatro níveis de segurança para a informação: *irrestrita*, *restrita, protegida*, *confidencial*. Existem casos em que a informação é de interesse nacional e, desse modo, classificada como: *confidencial*, *secreta*, *super-secreta*. Na prática, a implementação da classificação envolve procedimentos de marcar a informação, de armazená-la e transmiti-la; de descartar a informação desnecessária, de permitir acesso e divulgação, bem como de estabelecer responsabilidades.

Baker (2004) estabelece categorias para informação e para sistemas de informação no âmbito do *National Institute of Standards and Technology*, do Departamento de Defesa do governo norte-americano. As categorias propostas, denominadas *impacto baixo, moderado e alto* são baseadas no dano potencial para a organização, quando ocorrem eventos de risco para a informação e sistemas corporativos. A avaliação do impacto de acordo com essas categorias se fundamenta nos objetivos de segurança para informação e para sistemas de informação especificados na legislação americana interpretada pelo *Legal Information Institute* (2005).

Para o *Legal Information Institute* (2005), segurança da informação diz respeito à proteção da informação e dos sistemas de informação, em relação ao acesso não autorizado, uso, divulgação, alteração ou destruição. Está relacionada a três aspectos principais: integridade, confidencialidade e disponibilidade. *Integridade* diz respeito à proteção contra alteração indevida ou destruição, além de assegurar a autenticidade e o não repúdio. *Confidencialidade* significa preservar restrições de divulgação, garantindo meios para proteção da privacidade pessoal. *Disponibilidade* significa assegurar que o acesso e o uso da informação sejam conduzidos sem ameaças à segurança.

Baker (2004) apresenta um conjunto de procedimentos para mapear a relação entre um tipo de informação e o impacto que ela pode causar na segurança da organização: i) identificar sistemas de informação; ii) identificar tipos de informação; iii) selecionar níveis de impacto temporários; iv) rever e ajustar níveis de impacto temporários; v) atribuir categoria do sistema de segurança. O autor descreve ainda outro conjunto de procedimentos para identificar os tipos de informações disponíveis: i) identificar as áreas de negócio fundamentais; ii) identificar, para cada área de negócio, as operações que descrevem em termos funcionais o propósito do sistema; iii) identificar as sub-funções necessárias para conduzir os negócios em cada área; iv) selecionar tipos de informações básicas associados às sub-funções; v) identificar qualquer informação que receba manipulação especial por ordem superior ou determinação de agência regulatória.

As iniciativas citadas apresentam considerações sobre segurança da informação sem entretanto definir claramente a qual objeto se referem quando citam o termo "informação". Além disso, também não descrevem o meio pelo qual a informação é disseminada na organização. Uma importante forma de disseminação da informação é o meio digital, representado por documentos eletrônicos, sistemas de informação automatizados, dentre outros recursos de TI.

2.2 Iniciativas de caráter tecnológico

A norma ISO/IEC-15408-1 de 2005 é a principal referência para avaliação de atributos de segurança em produtos e em sistemas de TI, os quais são denominados *objetos de avaliação*. Usuários de TI, sejam eles consumidores, desenvolvedores ou avaliadores, nem sempre possuem conhecimento

ou recursos para julgar questões de segurança. De forma a atender a esses usuários, a ISO/IEC-15408-1 (2005) estabelece um critério comum para avaliação, possibilitando que o resultado seja significativo para audiências variadas.

O resultado das avaliações da ISO/IEC-15408-1 (2005) auxilia consumidores de TI a decidir se um produto ou sistema atende aos requisitos de segurança. Do ponto de vista do desenvolvedor, a norma descreve funções de segurança que devem ser incluídas no projeto do objeto de avaliação. Finalmente, do ponto de vista dos avaliadores e de outros membros da organização, a norma determina as responsabilidades e ações necessárias para a avaliação desse objeto.

Em relação à Internet cabe destacar a atuação do *Computer Emergency Response Team / Coordination Center* (CERT/CC), criado pelo *Defense Advanced Research Projects Agency* após o incidente *worm*[2] em 1988. Segundo Menninger (2005), o *worm* foi criado em um experimento controlado de acesso a computadores na *Cornell University*. Um defeito impediu a auto-detecção de novas cópias e diversos sistemas receberam centenas de *worms*, cada um deles tentando acesso e se replicando em mais *worms*. A partir de então, o CERT/CC passou a centralizar a coordenação de respostas a incidentes de segurança. Além disso, o organismo é responsável por publicar informes, pesquisar sobre segurança e manter um banco de dados sobre segurança em redes e na Internet.

Além da ISO/IEC-15408-1 e do CERT/CC, uma grande diversidade de iniciativas para segurança da informação na área de TI tem sido proposta desde os anos 80, a saber: roteiros para avaliações e para auditorias (KRAUS, 1980; GAO, 1988; GARFINKEL; SPAFFORD, 1996; ISACF, 2000; ISSEA, 2003), listas de verificação (WOOD et al, 1987; CIAO, 2000), diretrizes e critérios (OECD, 1992; WOOD et al, 1990; NIST/CSD, 1998), listas de termos e taxonomias (NEUMANN e PARKER, 1989; MEADOWS, 1992; LEVINE, 1995; HOWARD e LONGSTAFF, 1998). Dentre essas iniciativas destaca-se a taxonomia de incidentes de segurança proposta por Howard e Longstaff (1998), na qual se defende a necessidade de uma linguagem comum sobre segurança. Tal linguagem é composta por termos genéricos, estruturados em uma taxonomia, que permita o intercâmbio e comparação de dados sobre incidentes de segurança.

Na linguagem de Howard e Longstaff (1998), um *evento* corresponde a uma alteração no estado do sistema ou dispositivo. A alteração é resultado de *ações* (autenticar, ler, copiar, etc.) direcionadas a *objetos* (conta, processo, dado, rede, etc.). Um *evento* pode ser parte de um conjunto de processos que objetivam ocorrências não autorizadas. Esse *evento* é, então, parte de um *ataque*. Um ataque utiliza uma *ferramenta* (comando, *script*, etc.) para explorar a *vulnerabilidade* de um dispositivo, que corresponde a uma falha no sistema e permite ação não autorizada. A *vulnerabilidade* pode ser de projeto, de implementação ou de configuração. Além disso, ela provoca um *evento* e gera um *resultado não autorizado* (acesso indevido, roubo de recursos, etc.). Um grupo de *ataques* que envolve diferentes agentes, objetivos, locais, ou horários é denominado *incidente*. Um *incidente* é um *ataque* associado a um *objetivo*, que pode ser, ganho político ou financeiro, danos ou prejuízos, dentre outros.

O uso de uma linguagem organizacional única, com significados consensuais, pode incrementar a forma com que os indivíduos da empresa aprendem novas práticas e compartilham conhecimento com um nível de ambigüidade reduzido (VON KROGH; ROOS, 1995). Uma ontologia é uma estrutura capaz de operacionalizar uma linguagem única no âmbito da organização (ALMEIDA, 2006), e dessa forma, se apresenta como uma alternativa em projetos de segurança da informação. Para se referir a uma ontologia como um tipo de linguagem, cabe considerar que uma ontologia é especificada por uma linguagem de modelagem, que corresponde a um tipo de linguagem formal (FONSECA, 2007; GUARINO, 1998). Essa visão, entretanto, não é conflitante com a linguagem organizacional, uma vez que o vocabulário em questão corresponde a um subconjunto da linguagem.

A importância conferida aos recursos tecnológicos tem levado os gerentes das empresas a designar equipes de TI como responsáveis pela solução dos problemas de segurança da informação. Tal prática tem conduzido a planos de segurança fundamentados em soluções puramente tecnológicas, os quais são pouco eficientes em atender as necessidades sistêmicas da organização. Cabe lembrar, que os funcionários envolvidos nas atividades

2 Programa de computador capaz de auto-duplicação, que gera grande quantidade de tentativas de acesso e, em consequência, de tráfico em redes de computadores.

diárias das organizações são a melhor fonte para determinar a importância das informações no contexto corporativo, e sempre que possível, devem ser convocados a participar ativamente do planejamento da segurança.

3 Ontologias aplicadas à segurança da informação

O termo ontologia é originário da filosofia e tem sido utilizado desde os anos 80 em Ciência da Computação e em Ciência da Informação para designar uma estrutura de organização da informação baseada em um vocabulário representacional. Apresentar questões teóricas relacionadas a ontologias está além dos objetivos do presente artigo.Vários autores têm estudado o assunto, tanto em Ciência da Computação (GENESERETH; NILSSON, 1987; GRUBER, 1993; GUARINO, 1995; GUARINO; GIARETTA, 1995; GUARINO, 1998; SOWA, 2000; SMITH, 2003), quanto em Ciência da Informação (ALMEIDA, 2006; VICKERY, 1997; GILCHRIST, 2003; SØERGUEL, 1997; WAND, STOREY e WEBER, 1999).

Com aplicações em diversas áreas, as ontologias também servem a propósitos de segurança da informação conforme comprovam iniciativas apresentadas na seção 3.1. Em seguida, a seção 3.2 apresenta as ontologias como alternativas para classificação em segurança da informação, descrevendo resultados parciais de pesquisa em andamento.

3.1 Pesquisa anterior significativa sobre ontologias em segurança

Referências ao uso de ontologias em segurança da informação estão disponíveis na literatura, notadamente nos últimos dez anos. Raskin et al (2001) afirmam que a pesquisa em segurança da informação pode se beneficiar da adoção de ontologias. Esses autores apresentam duas propostas distintas para operacionalizar esse tipo de aplicação, uma relacionada à Representação do Conhecimento[3] e outra ao Processamento de Linguagem Natural[4].

A primeira proposta enfatiza a possibilidade de reunir um conjunto de termos e relações representativos do domínio de segurança da informação. Uma ontologia sobre segurança da informação auxilia usuários de produtos e de sistemas de informação ao proporcionar estrutura, possibilidades de intercâmbio e comparação de dados sobre incidentes de segurança, bem como melhores possibilidades na tomada de decisão frente ao incidente.

A segunda proposta consiste em usar fontes de dados em linguagem natural para ações de segurança da informação. Possibilita especificar formalmente o *know-how* da comunidade responsável pela segurança, resultando em melhorias nas medidas de prevenção e de reação a ataques. Aplica-se processamento de linguagem natural aos *logs*[5] de sistemas, os quais são escritos em uma sub-linguagem da linguagem natural.

Para Martiniano e Moreira (2007), o grande volume de dados gerado por diferentes fontes, tais como *logs*, *firewalls*[6], alertas de vulnerabilidade, dentre outros, tem causado problemas aos administradores. O principal problema é a dificuldade em acumular conhecimento para a tomada de decisão e para a solução de incidentes de segurança. Apesar dos esforços em classificar registros sobre segurança, as iniciativas em geral não contemplam o significado dos dados armazenados.

Sem o significado dos dados sobre segurança, um administrador ou um agente de *software* não é capaz de fazer correlações entre incidentes. Nesse contexto, Martiniano e Moreira (2006) propõem uma ontologia de incidentes de segurança, através da qual buscam definir uma linguagem única. A maioria dos conceitos dessa ontologia é proveniente de glossários e taxonomias sobre segurança da informação (HOWARD; LONGSTAFF, 1998; NSCS, 1988; SHIREY, 2000), de recursos sobre vulnerabilidade (*National Vulnerability Database*[7], *Common Vulnerabilities and Exposures Project*[8]). Para avaliar a sua representatividade quanto ao

3 Na Ciência da Computação, a Representação do Conhecimento se desenvolveu como um ramo da Inteligência Artificial, associado ao desenvolvimento de sistemas especialistas.

4 Processamento da linguagem natural é um campo da Linguistica Computacional que estuda os problemas de compreensão e *geração automática de linguagens naturais.*

5 Um log é um arquivo ou conjunto de arquivos digitais criado automaticamente a partir das atividades executadas em um computador.

6 Um *firewall* é uma aplicação que analisa o tráfico em uma rede, permitindo ou não a passagem de dados a partir de um conjunto de regras.

7 O NVD é um repositório de padrões do governo norte-americano voltado para questões de vulnerabilidade. Disponível na Internet em http://nvd.nist.gov/. Acesso em 20/02/2007.

8 CVE é um dicionário público com informações sobre vulnerabilidades. Disponível na Internet em http://cve.mitre.org/. Acesso em 20/02/2007.

conhecimento acumulado na área, a ontologia ainda é comparada ao SNORT[9].

Fenz et al (2007) propõem a construção de uma ontologia em *Ontology Web Language* (OWL) para suporte à certificação ISO/IEC-27001 (2005), com informações sobre a criação e a manutenção de políticas de segurança. O mapeamento ontológico do padrão ISO/IEC aumenta o grau de automação do processo, reduzindo custos e o tempo despendido para a certificação. A ontologia de suporte é criada a partir da combinação de três recursos principais: i) a *CC Ontology* (EKELHART et al, 2007), que abrange o domínio *Common Criteria*[10] e enfatiza requisitos de garantia de segurança para a avaliação; ii) a *Security Ontology* (EKELHART et al, 2006), que contém dados sobre ameaças e respectivas medidas de proteção; e iii) o próprio padrão ISO/IEC-27001 (2005).

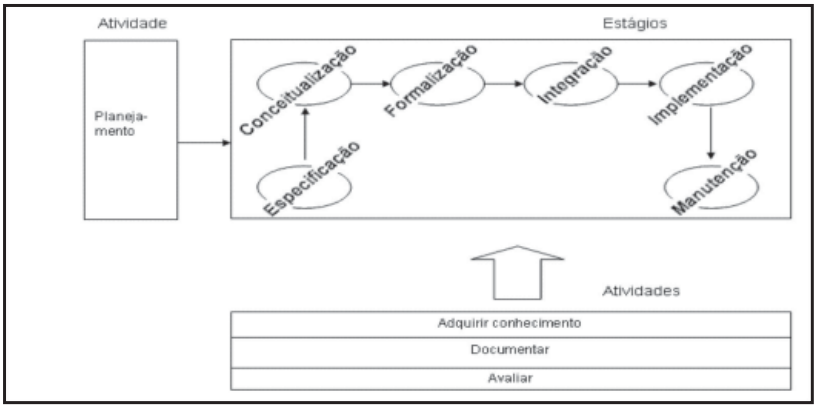

Figura 1 - Representação gráfica do ciclo de vida da ontologia

Fonte: Adaptado de Fernandez, Gomez-Perez e Juristo (1997, p.35)

3.2 Proposta de ontologia de domínio sobre segurança da informação

Existem iniciativas para segurança da informação baseadas em ontologias, conforme comprovam as iniciativas apresentadas na seção 3.1. Algumas dessas iniciativas buscam estabelecer uma linguagem única, consensual, de termos sobre segurança da informação. Na presente seção, apresentam-se resultados de pesquisa que correspondem ao estágio terminológico de uma ontologia de domínio sobre segurança da informação.

Uma ontologia pode ser definida como um objeto ou como um processo (ALMEIDA, 2006). Na acepção "ontologia como processo", a ontologia é caracterizada de acordo com os procedimentos metodológicos adotados em seu desenvolvimento. Esses procedimentos são organizados em etapas diversas, conforme o ciclo de vida da ontologia apresentado na Figura 1: i) especificação, em que se definem a competência da ontologia, seu escopo e as fontes de dados; ii) aquisição de conhecimento, na qual se coletam dados; iii) conceitualização, onde tem lugar o trabalho intelectual de estruturação do domínio; iv) integração, onde se consideram termos e conceitos de outras ontologias; v) implementação, etapa na qual a ontologia é codificada em uma linguagem de representação.

Na etapa de *conceitualização*, o responsável pelo processo modela o conhecimento adquirido traduzindo-o em um modelo conceitual que descreve e representa o domínio. Um dos procedimentos dessa etapa consiste em organizar um glossário de termos representativos de conceitos, relações, propriedades e instâncias. Inicia-se a estruturação do conhecimento obtido na etapa de aquisição de conhecimento, partindo-se do estágio terminológico. Nesse estágio, os termos são listados e organizados pela primeira vez em uma estrutura hierárquica. Nas etapas seguintes, o conhecimento é gradualmente formalizado até o estágio em que é possível sua implementação em ferramenta automatizada.

Ainda na etapa de conceitualização, os termos são distribuídos em camadas de acordo com diferentes níveis de abstração: o *nível genérico* contém conceitos abstratos passíveis de reutilização em outros contextos (por exemplo, pessoa); o *nível organizacional*

9 SNORT é uma rede com recursos sobre prevenção e detecção de invasões em sistemas, a partir de uma linguagem baseada em regras. Disponível na Internet em http://www.snort.org/. Acesso em 20/02/2007.

10 O *Common Criteria for Information Tecnhnology Secutity Evaluation* fornece diretrizes para a avaliação e certificação de segurança.

contém conceitos que podem ser utilizados em qualquer organização, independentemente de suas particularidades (por exemplo, funcionário); e o *nível específico*, que atende as particularidades de uma organização específica.

O estágio terminológico descrito no presente artigo corresponde a uma proposta para o nível organizacional, passível de utilização no contexto de forma geral. Os resultados podem, em conseqüência disso, apoiar e fundamentar o trabalho de profissionais de informação e gerentes responsáveis por projetos de segurança da informação. A Figura 2 apresenta um esquema preliminar proposto para a ontologia e os principais conceitos descritos no nível organizacional:

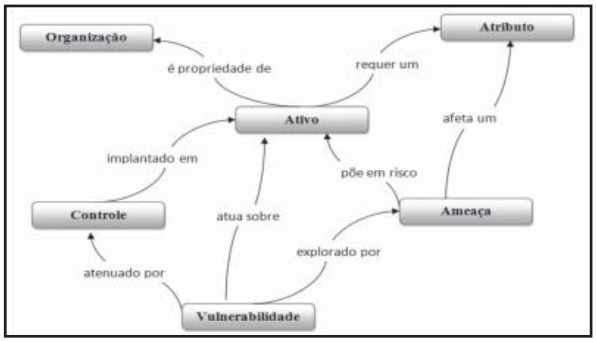

Figura 2: Esquema preliminar da ontologia de segurança da informação

Fonte: Elaborado pelos autores a partir da revisão de literatura

A organização preliminar da Figura 2, bem como as respectivas definições (Tabela 1), foram obtidas a partir das iniciativas descritas na seção dois, em particular, na seção 2.1. Como são definições abrangentes e sujeitas a diferentes interpretações, ainda não são definitivas. Para que sejam representativas de um consenso mínimo, devem ser confrontadas com maior número de fontes e aprovadas por especialistas. Entretanto, o formato da definição conforme apresentado no Quadro 1 já considera as melhores práticas para a definição de conceitos, formando-os a partir de noções intensionais e noções extensionais (ISO704-2000).

Organização	Uma organização é uma entidade social composta por recursos materiais e humanos, a qual possui objetivos comuns, procedimentos sistemáticos para controle de seu desempenho e limites definidos que a separam do ambiente. Pode ser uma instituição pública ou privada.
Atributo de segurança	Um atributo de segurança é uma propriedade atribuída a um ativo, a qual diz respeito a requisitos de segurança. Pode ser um atributo de confidencialidade, de integridade e de disponibilidade
Ativo	Um ativo é um bem de propriedade da organização, utilizado para alcançar seus objetivos sociais. Pode ser um equipamento, estoque, imóvel, dentre outros.
Controle	Um controle é um procedimento padrão sistemático implementado para atenuar vulnerabilidades, bem como para proteger ativos através de medidas preventivas e corretivas.
Ameaça	Uma ameaça é uma possibilidade de dano aos ativos da organização, que afeta os atributos de segurança específicos e explora vulnerabilidades da organização. Pode ser de origem humana ou natural e ter como fonte um evento acidental ou uma ação deliberada.
Vulnerabilidade	Vulnerabilidade é uma situação caracterizada pela falta de medidas de proteção adequadas. Uma vulnerabilidade possui um grau de severidade associado (por exemplo, crítico, moderada ou baixo). Pode ser uma vulnerabilidade de origem administrativa, técnica ou física.

Quadro 1: Principais definições da ontologia de segurança

Fonte: Elaborado pelos autores a partir da revisão de literatura

O Quadro 2 apresenta a hierarquia de termos correspondente ao estágio terminológico preliminar proposto. Nem todas as definições para os termos estão disponíveis no estágio atual da pesquisa. O conjunto terminológico é composto por 165 termos e expressões representativos de conceitos no domínio da segurança da informação. Apresentam-se também as conexões do nível organizacional com o nível superior, nas linhas denominadas "*... classe do nível abstrato*". As classes marcadas em negrito e letra maiúscula correspondem a aquelas definidas no esquema do Quadro 1.

Algo
... classe do nível abstrato
ATIVO
Ativo Imóvel
Prédio
Setor
Ativo Móvel
Sistema tecnologia da informação e comunicação
Sistema de energia
Sistema de vigilância
Sistema de Rede
Rede de computadores
Rede telefônica
Sistema de acesso
Biométrico
Assinatura Digital
... classe do nível abstrato
ORGANIZAÇÃO
Organização pública
Organização privada
ATRIBUTO DE SEGURANÇA
Responsabilidade
Disponibilidade
Confidencialidade
Integridade
Confiabilidade
... classe do nível abstrato
CONTROLE
Controle de acesso a TI
Proteção via senhas
Manutenção de senhas
Política de fornecimento de senhas
Desativação de contas sem utilização
Restrições de acesso a rede
Segmentação da rede
Controle da continuidade dos negócios
Controle da regularidade de cópias de segurança
Controle de mídia para cópias de segurança
Controle da estratégia para cópias de segurança
Controle da estratégia de recuperação de desastres
Controle de fornecimento de energia
Controle de contrato - seguro contra fogo
Controle de contrato - seguro contra descarga elétrica
Controle de seguro - roubo
Controle de seguro - vandalismo
Controle de seguro - danos por água
Controle de operações e de comunicações
Verificação regular de segurança na rede
Auditoria de atividades de rede
Controle de instalação de software
Controle de atualização de software
Controle de operação em servidores
Controle de eventos em servidores
Uso de *gateways* de segurança
Uso de antivírus
Uso de criptografia
Uso de sistemas de detecção e resposta a intrusos
Controle de procedimentos na detecção de *malwares*
Controle dos regulamentos sobre o uso de email
Controle do descarte de recursos confidenciais
Controle do transporte de mídia
Controle de conformidade
Controle de segurança de recursos humanos
Controle de assinatura de termos de segurança
Treinamento em segurança de TI
Treinamento de funcionários em TI
Procedimentos para uso por pessoal externo
Procedimentos durante contrato de trabalho
Supervisão de pessoal externo ou de visitantes
Controle da informação sobre incidentes
Obtenção regular de informação sobre vulnerabilidades
Obtenção regular de informação sobre ameaças
Controle da criação, manutenção e aquisição de SI
Gestão de licenças de software
Gestão de atualizações de software
Controle da segurança física e ambiental
Controle do regulamento de acesso
Controle de ar condicionado
Controle de dispositivos anti-roubo
Controle de drenagem
Controle de proteção de equipamentos
Controle de conformidade com padrões técnicos
Controle de sistemas, normas e inspeções contra fogo
Controle da proteção em rotas de cabeamento
Controle de chaves
Controle de proteção contra variação de voltagem

Controle de proteção contra descargas elétricas
Verificações físicas regulares de conexões existentes
... classe do nível abstrato
AMEAÇA
Acesso a internet
Alteração de software
Poluição
Privacidade de linhas telefônicas
Dano a ativos
Danos a componentes de TI
Falha no transporte de mídia de dados
Danos físicos à construção
Desastre natural
Destruição de ativos
Vandalismo
Infra-estrutura deficiente
Perda de ativos
Perda de dados
Interferência em dados
Ambiente de trabalho inadequado
Exposição de dados
Mídia de dados defeituosa
Distúrbio elétrico
Efeitos climáticos
Espionagem
Sabotagem
Roubo
Falta de pessoal
Fim de contrato de trabalho de empregado
Pessoal externo
Acesso físico não autorizado
Uso não autorizado de sistemas
Violação de direitos autorais
Erro de configuração de TI
Ataque à componente de TI
Ataque em protocolos
Ataque em serviços
Ataque em senhas
Softwares perigosos (*malware*)
Spam
Uso descontrolado de email
Erro de usuário
Uso inadequado de dados
Uso inadequado de sistemas
Perda de integridade de dados
Não conformidade com medidas de segurança
... classe do nível abstrato
VULNERABILIDADE
Vulnerabilidade administrativa
Falha na mídia de dados
Falha no descarte de mídias de dados
Falha na instalação de software
Falha na operação de servidores
Falha na autenticação de equipamentos de rede
Inexistência de cópias de segurança
Inexistência de histórico de funcionários
Falta de treinamento em TI
Falta de treinamento sobre segurança
Inexistência de estratégia de recuperação de ativos
Inexistência de estratégia de cópia de segurança
Falta de controle de acesso
Inexistência de documentação de senhas
Falta de inspeções de segurança
Falta de precaução contra *malware*
Inexistência de procedimentos para uso por pessoal externo
Inexistência de regulamentos para fim de contrato de trabalho
Falta de informação regular sobre vulnerabilidades
Falta de verificação regular de segurança de rede
Inexistência de regulamentação no uso de emails
Inexistência de supervisão de pessoal externo e de visitantes
Vulnerabilidade física
Falha em dispositivos de segurança
Falha na localização de componentes de TI
Falha de controle de regulamento de acesso
Falha de sistema de ar condicionado
Falha de dispositivo anti-furto
Falha de sistema de alarme contra intrusos
Falha de detecção de incêndio
Falha de proteção em rotas de cabeamento
Falha de conformidade a padrões técnicos
Falha na verificação de conexões físicas
Falha de manutenção
Vulnerabilidade técnica
Falha na garantia de direitos de acesso
Falha na configuração de rede
Falta de segmentação em redes
Falha no registro de atividades de rede
Falha na proteção da confidencialidade de dados
Falha na proteção da integridade de dados
Falha na restrição ao usuário
Falha no descarte da mídia de dados
Falha na criptografia
Falha no sistema de detecção e resposta a invasões

Quadro 2: Hierarquia de conceitos descrita na etapa terminológica

Fonte: Elaborado pelos autores

4 Considerações finais

O presente artigo discorreu sobre segurança da informação, destacando iniciativas governamentais, normativas e tecnológicas. Não se pretendeu esgotar o assunto de segurança da informação, mas apresentou-se o necessário para uma visão geral da área. Introduziu-se o uso de ontologias como instrumento para classificação em projetos de segurança da informação e apresentou-se o resultado do estágio terminológico de uma ontologia de domínio. Enfatizou-se a concepção do nível organizacional, propondo bases para uma linguagem única sobre segurança da informação a partir de iniciativas descritas na revisão de literatura.

A ontologia de domínio pode apoiar o trabalho em projetos de segurança da informação de várias formas: i) na criação de modelos conceituais que possibilitem a empresa conhecer mais sobre incidentes de segurança; ii) no apoio a interoperabilidade entre diferentes ferramentas de segurança; iii) na criação de um padrão para estruturar dados sobre segurança, permitindo que termos diversos sejam mapeados para a ontologia; iv) na reutilização de dados sobre segurança, através da importação e exportação de ontologias; v) no apoio aos administradores em decisões sobre a gestão de segurança, através de consultas e inferências automáticas.

O desenvolvimento de uma ontologia pressupõe algum nível de consenso sobre o conhecimento do domínio em questão. A busca pelo consenso ocorre em diferentes níveis que compõem a ontologia: no *nível específico*, onde se busca obter consenso relativo a conceitos específicos da empresa e; no *nível organizacional*, em que se busca algum tipo de consenso entre conceitos geralmente aceitos pela área. Para a construção do nível organizacional são consultadas normas, leis, documentos regulatórios, dados sobre pesquisa anterior, dentre outras fontes. Tais fontes devem contribuir para a compreensão do domínio, além de fundamentar o desenvolvimento do nível especifico.

No conjunto de termos apresentado na Tabela 2, observa-se certa ênfase em conceitos relacionados a TI. Essa tendência parece aceitável quando se verifica que a TI permeia praticamente todas as atividades de uma empresa. Entretanto, conforme já mencionado na seção 2, acredita-se que um projeto de segurança da informação bem fundamentado deve atender a outras necessidades organizacionais e não somente aquelas de caráter estritamente tecnológico.

A proposta da linguagem única, operacionalizada pela ontologia, possibilita abordagens à segurança através de facetas organizacionais que vão além daquelas ligadas a TI, como por exemplo: i) questões relativas à cultura organizacional, como o ambiente de trabalho inadequado, exposição de dados, dentre outros; ii) questões que envolvem ativos tangíveis da organização, como segurança e acesso a locais de trabalho (prédios, instalações), segurança física do patrimônio, proteção contra desastres naturais e vandalismo, dentre outras; iii) questões sobre documentos, em geral abordadas na Arquivística, como, por exemplo: confidencialidade, integridade, confiabilidade; iv) questões relacionadas ao fator humano, como: treinamento, conscientização, regulamentação do término de contratos de trabalho, regulamentação de contratos com terceiros, dentre outras.

Cabe destacar a influência do fator humano, uma vez que grande parte dos problemas de segurança é gerado por ações, intencionais ou não, de pessoas em suas atividades no âmbito da organização. A classificação da informação e a busca por consenso entre usuários pode atenuar os efeitos do fator humano, pois as pessoas são consideradas partes integrantes desses processos. Dessa forma, os responsáveis pelas atividades influenciam a classificação das informações que manipulam rotineiramente, o que permite definir níveis de segurança condizentes com a realidade.

Os resultados parciais apresentados no presente artigo são provenientes de esforços conduzidos na pós-graduação da Escola de Ciência da Informação da Universidade Federal de Minas Gerais (UFMG). Acredita-se que, mesmo em se tratando de pesquisa em andamento, os resultados apresentados são significativos principalmente se considerada a escassez de pesquisas sobre segurança da informação no escopo da CI. Como perspectiva para pesquisas futuras, pretende-se seguir as etapas de construção da ontologia, além de conduzir levantamentos em empresas para obtenção de dados. Esperam-se assim gerar novas oportunidades de pesquisa, benefícios para empresas e profissionais envolvidos com segurança da informação.

A PROPOSAL FOR A DOMAIN ONTOLOGY ABOUT INFORMATION SECURITY IN ORGANIZATIONS: description of the terminological stage

Abstract *The evolution of information technology has facilitated the dissemination of information in the organizational and inter-organizational context. The availability of information and today's competitive business environment has focused on information security issues. Although the managers realize the need to implement security guidelines, they do not have a clear understanding of what must be protected and how to do that. This article presents a general overview of the field of security research, describes distinct related initiatives and highlights the significance of information classification in achieving security goals in the organizational environment. It is advocated that organizations can benefit from adopting ontologies as an alternative means for classifying information, it is also presented the partial results of the current research regarding the terminological stage of a domain ontology about security information. The aim is to contribute to other researches related to the Information Science area, as well as to guide the information professionals and managers who drive security projects.*

Keywords: *Information Security. Ontologies. Information Science. Knowledge Management.*

Artigo recebido em 09/02/2010 e aceito para publicação em 17/04/2010

Referencias

ALMEIDA, M. B. **Um modelo baseado em ontologias para representação da memória organizacional**. 2006. 321f. Tese (Doutorado em Ciência da Informação) - Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2002.

BAKER, W. **Information security**; volume I. (2004). Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf >. Acesso: 02 Mai. 2006.

CRITICAL INFRASTRUCTURE ASSURANCE OFFICE (CIAO). **Practices for Securing Critical Information Assets**. (2000). Disponível em: <http://www.infragard.net/library/pdfs/securing_critical_assets.pdf> Acesso: 02 Dez. 2007.

EKELHART, A. et al. Ontological Mapping of common criteria's security assurance requirements. **International Information Security Information**, 2007, Sandton, Proccedings… Springer: [s.n.], 2007.

EKELHART, A. et al. **Security ontology**: simulating threats to corporate assets. (2006). Disponível em: <http://www.springerlink.com/index/w530v5081301j833.pdf>. Acesso: 30 Jul. 2007.

FENZ, S. et al. **Information security fortification by ontological mapping of the ISO/IEC 27001 Standard**. (2007). Disponível em: <http://www.ifs.tuwien.ac.at/node/4274 >. Acesso: 19 Nov. 2007.

FERNANDEZ, M.; GOMEZ-PEREZ, A.; JURISTO, H. **Methontology; from ontological art towards ontological engineering**. (1997). Disponível em: <http://citeseer.ist.psu.edu/context/544607/0/>. Acesso: 20 Jul. 2005.

FONSECA, F. The Double Role of Ontologies in Information Science Research. **Journal of the American Society for Information Science and Technology**. v. 58, n. 6, p. 786-793, Fev. 2007.

FOWLER, S. *GIAC* **Security essentials certification**. (2003). Disponível em: <http://www.sans.org/reading_room/whitepapers/auditing/846.php>. Acesso: 13 Abr. 2005.

GENERAL ACCOUNTING OFFICE OF UNITED STATES (GAO). **GAO Audit Guide**. (1988). Disponível em: <http://www.gao.gov/index.html>. Acesso: 15 Nov. 2007.

GARFINKEL, S.; SPAFFORD, G. **Practical Unix and Internet Security**, 2a ed. 1996. Sebastopol : O'Reilly. 1000 p.

GENESERETH, M. R.; NILSSON, L. **Logical foundation of AI**. San Francisco: Morgan Kaufman. 1987, 405p.

GILCHRIST, A. **Thesauri, taxonomies and ontologies**; an etymological note. (2003). Disponível em: <http://dois.mimas.ac.uk/DoIS/data/Articles/julkokltny:2003:v:59:i:1:p:7-18.html>. Acesso: 2 Mar. 2006.

GOVERNMENT OF ALBERTA. **Information Security Classification**. (2005). Avalaible from Internet: <http://www.im.gov.ab.ca/publications/pdf/InfoSecurityClassification.pdf>. Acesso: 20 Out. 2006.

GRUBER, T. **What is an ontology***?* (1993). Disponível em: <http://www-ksl.stanford.edu/kst/what- is-an-ontology.html>. Acesso: 14 Set. 2002.

GUARINO, N. **Formal ontology in information systems**. (1998). Disponível em: <http://citeseer.ist.psu.edu/guarino98formal.html>. Acesso: 03 Jan. 2002.

_____. **Formal ontology, conceptual analysis and knowledge representation** (1995). Disponível em: <http://citeseer.ist.psu.edu/guarino95formal.html>. Acesso: 03 Jan. 2002.

GUARINO, N.; GIARETTA, P. **Ontologies and KBs, towards a terminological clarification.** In: MARS, N. (Ed.). Towards a Very Large Knowledge Bases; Knowledge Building and Knowledge Sharing. [S.l.]: IOS Press, 1995. p. 25-32.

HOWARD, J.D.; LONGSTAFF, T. A. **A common language for computer security incidents.** (1998). Avalaible from Internet: <http://www.cert.org/research/taxonomy_988667.pdf>. Acesso: 13 Dez. 2006.

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION (ISACF). **Control Objectives for Information and Related Technology (COBIT).** (2000). Disponível em: <http://www.isaca.org/>. Acesso: 01 Dez. 2007.

INTERNATIONAL SYSTEMS SECURITY ENGINEERING ASSOCIATION (ISSEA). **SSE/CMM-System Security Engineering/Capability Maturity Model,** V3*.0.* (2003). Disponível em: <http://www.sse-cmm.org/>. Acesso: 02 Dez. 2007.

INTERNATIONAL ORGANIZATIONAL FOR STANDARTIZATION; ISO Standard 704 (2004) . **Terminology Work, Principles and Methods**. Disponível em: <http://www.iso.org/>. Acesso em 20 jan. 2004.

ISO/IEC 15408-1. Internacional Standard – Information Technology – Security Techniques; **Evaluation Criteria for IT Security – part 1.** (2005). Disponível em: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40612> . Acesso: 21 Abr. 2006.

ISO/IEC-27001. International Standard – Information Technology – **Security Techniques; information security management systems – requirements**. (2005). Disponível em : <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103> . Acesso: 21 Abr. 2006.

THE INFORMATION SECURITY OVERSIGHT OFFICE (ISOO). **Marking classified national security information**. (2003). Disponível em: <http://www.archives.gov/isoo/training/marking-booklet.pdf>. Acesso: 12 Jan. 2006

KRAUSE, M.; TIPTON, H.F. **Handbook of Information Security Management.** 3 ed., 1997. Boca Raton: Auerbach. 729 p.

KRAUSS, L.; SAFE, I. **Security audit and field evaluation for computer facilities and information systems.** New York : Amacom, 1980. 336 p.

LEVINE, D. E. **Auditing Computer Security**. In: HUTT, A. E. et al. (Ed.). Computer Security Handbook. 3 ed. New York : Wiley, 1995. p. xx-xx.

LEGAL INFORMATION INSTITUTE of Cornell University. U.S. **Code collection; 3452 Definitions**. (2005). Disponível em: <http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542----000-.html>. Acesso: 8 Dez 2007.

MARTINIANO, L.A.F.; MOREIRA, E. S. **An OWL-based security incident ontology**. (2007). Disponível em: <http://protege.stanford.edu/conference/2005/submissions/posters/poster-martimiano.pdf >. Acesso: 20 Nov. 2007.

MARTINIANO, L.A.F.; MOREIRA, E. S. **The evaluation process of a computer security incident ontology**. (2006). Disponível em: <http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-199/wonto-06.pdf >. Acesso: 20 Nov. 2007.

MEADOWS, C. **An outline of a taxonomy of computer security research and development**. (1992). Disponível em: <http://portal.acm.org/citation.cfm?id=283770>. Acesso: 2 Jan.2005.

MENNINGER, M. R. **The birth of incident response**; the story of the first Internet worm. (2005). Disponível em: <http://www.selfseo.com/story-9757.php >. Acesso: 20 Nov. 2006.

NATIONAL COMPUTER SECURITY CENTER (NCSC). **Glossary of computer security itens**. (1988). Disponível em: <http://packetstormsecurity.org/docs/rainbow-books/NCSC-TG-004.txt >. Acesso: 15 Nov. 2007.

NEUMANN, P.; PARKER, D. **A summary of computer misuse techniques**. (1989). Disponível em: <http://www.emeraldinsight.com/Insight/ViewContentServlet?Filename=Published/EmeraldFullTextArticle/Pdf/0460110503_ref.html>. Acesso: 8 Jul. 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY/COMMON CRITERIA/ COMPUTER SECURITY DIVISION (NIST/CSD). **Common Criteria for Information Technology Security Evaluation.** (1998). Disponível em: <http://csrc.nist.gov/nissc/1999/proceeding/papers/p15.pdf >. Acesso: 01 Dez. 2007.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). **Guidelines for the Security of Information Systems**. (1992). Disponível em: <http://www.oecd.org/ >. Acesso: 01 Dez. 2007.

QUIST, A. S. **Security Classification of Information**; volume 2, principles and techniques for classification of information. (1993). Disponível em: <http://fas.org/sgp/library/quist2/index.html>. Acesso: 02 Dez. 2007.

RASKIN, V. et al. **Ontology in information security; a useful theoretical foudation and methodological tool**. (2001). Disponível em: <http://portal.acm.org/ft_gateway.cfm?id=508180&type=pdf&dl=portal&dl=ACM>. Acesso: 16 Ago. 2005.

SHIREY, R. *RFC 2828*; **Internet Security Glossary**. (2000). Disponível em: <http://rfc.dotsrc.org/rfc/rfc2828.html>. Acesso: 19 Nov. 2007.

SMITH, B. **Ontology and Informations Systems**. (2003). Disponível em: <http://www.ontology.buffalo.edu/ontology> Acesso: 22 Jan. 2006.

SØERGUEL, D. **Functions of a thesaurus, classification and ontological**. knowledge bases. (1997). Disponível em: <http://www.clis.umd.edu/faculty/soergel/soergelfctclass.pdf>. Acesso: 12 Dez. 2003.

SOWA, J. F. Ontology, Metadata, and Semiotics. (2000). Disponível em: <http://users.bestweb.net/~sowa/peirce/ontometa.htm>. Acesso: 05 Jul. 2003.

VICKERY, B. C. (1997). Ontologies. **Journal of Information Science**. v. 23, n. 4. p. 227-286.

VON KROGH, G.; ROOS, J. Conversation Management. **European Management Journal**. [online].v. 13, n. 4, p. 390-394, 1995a. Disponível em: <http://www.sciencedirect.com>. Acesso: 10 Mar. 2005.

WAND, Y., STOREY, V. C. e WEBER, R. (1999). An ontological analysis of the relationship construct in conceptual modeling. **ACM**

Transactions on Database Systems. v. 24, n. 4, p. 494-528.

WOOD, C. C. **Principles of Secure Information Systems Design**. (1990). Disponível em: <http://portal.acm.org/citation.cfm?id=85089.85091>. Acesso: 22 Set. 2007.

WOOD, C. C. et al. **Computer Security**; a comprehensive controls checklist. New York: Wiley, 1987. 214 p.