
Divulgação

Aplicação de ontologias em segurança da informação

Mauricio B. Almeida

Doutor em Ciência da Informação (UFMG), atualmente é professor adjunto do departamento de Teoria e Gestão da Informação da UFMG, onde está integrado à linha de pesquisa Gestão da Informação e do Conhecimento. Mantém pesquisas nas áreas de Representação do Conhecimento e Ontologias, Sistemas de Informação, Memória Organizacional e Preservação Digital.

RESUMO

Segurança da informação é um assunto relevante em praticamente todas as organizações. Ao mesmo tempo em que sentem necessidade de implementá-la, os gerentes não possuem clareza sobre o que deve ser protegido e como fazê-lo. Este artigo apresenta uma visão geral da pesquisa na área e descreve iniciativas diversas. Destaca a importância de classificar a informação no ambiente corporativo e conclui que existem benefícios na aplicação de ontologias em segurança da informação. Espera-se contribuir com uma revisão de literatura, sem a pretensão de que seja exaustiva e com um roteiro para construção de ontologias, bem como sua integração aos recursos corporativos.

1. Introdução

A expressão segurança da informação representa um conceito amplo. Em geral, nas empresas e nas instituições, está associada a sistemas informatizados e a dados que estes manipulam. Entretanto, uma organização não possui apenas dados em formato digital. Considere-se que muita informação sobre uma empresa está armazenada fora dela (governo, conselhos, fornecedores, etc.). Considere-se, ainda, a complexidade do ciclo de vida da informação, desde sua produção até sua disseminação, e as influências do fator humano. Mesmo se observado apenas o contexto das organizações, não parece tarefa trivial definir segurança da informação.

Os problemas de muitas organizações na implementação de segurança da informação estão relacionados com a dificuldade em definir o que deve ser protegido, qual o nível de proteção necessário e quais ferramentas utilizar no ambiente corporativo. A dificuldade começa na própria definição do objeto a proteger, ou seja, na definição da informação. Wilson (2002) alerta para o uso indistinto dos termos dado e informação. Para o autor, dados são fatos e estão fora da mente de uma pessoa. Informações consistem de dados aos quais se incorpora um contexto relevante para o indivíduo. Cabe então à organização descobrir em quais

contextos a informação crítica se manifesta e quais as necessidades corporativas em relação à segurança, e não apenas buscar proteção para dados em computadores e em redes.

A despeito da discussão, a expressão segurança da informação é amplamente utilizada no ambiente corporativo e envolve uma série de possibilidades, muitas delas, associadas à Tecnologia da Informação (TI): controle de acesso a recursos (dispositivos ou documentos); segurança em comunicação; gestão de riscos; políticas de informação; sistemas de segurança; diretrizes legais; segurança física; criptografia; arquivística; dentre outros (Krause e Tipton, 1997). Para o Legal Information Institute (2005), segurança da informação diz respeito a proteger a informação e os sistemas de informação de acesso não autorizado, uso, divulgação, modificação ou destruição. Está relacionada a três aspectos: integridade, confidencialidade e disponibilidade. Integridade diz respeito à proteção contra alteração indevida ou destruição, assegurando a autenticidade e o não-repúdio. Confidencialidade significa preservar restrições de divulgação e de acesso, garantindo meios para proteção da privacidade pessoal. Disponibilidade significa assegurar o acesso e o uso da informação de forma confiável.

Este artigo destaca a importância da classificação da informação em questões de segurança. Apresenta uma abordagem com base em ontologias para segurança da informação. O termo ontologia nasceu na filosofia, mas tem sido utilizado para designar uma estrutura de organização da informação que se baseia em conceitos e em suas relações. Esperam-se duas contribuições principais ao leitor: i) informar sobre as abordagens disponíveis na literatura, proporcionando uma visão geral da área; ii) apresentar a ontologia como um importante instrumento passível de utilização em iniciativas de segurança.

O restante do presente artigo está dividido em quatro seções: a seção dois apresenta considerações sobre segurança da informação nas organizações, com destaque para iniciativas governamentais e iniciativas normativas; a seção três destaca as iniciativas que envolvem a TI; a seção quatro enfatiza as iniciativas que envolvem a TI e, ao mesmo tempo, utilizam ontologias como ferramenta de classificação, além de apresentar um roteiro sobre como construir ontologias para fins de segurança da informação; e a seção cinco apresenta as considerações finais.

2. Visão geral sobre segurança da informação

Para muitas organizações, a segurança da informação é uma necessidade de negócio. Ainda assim, nem sempre se implementam práticas para tal, visto que os projetos necessários são caros, complexos, demandam tempo e não têm garantia de sucesso. Segundo Fowler (2005), os principais mecanismos para proteger as informações corporativas são: as políticas de segurança da informação, a análise de riscos e a classificação da informação.

Uma política de segurança é um plano de alto nível que estabelece como esta segurança deve ser praticada na organização, que ações são aceitáveis e que nível de segurança a organização está disposta a aceitar. A análise de riscos consiste da prática de confrontar o valor da informação e as ameaças com perdas, bem como identificar meios de proteção que possam reduzir riscos. Os procedimentos de classificação da informação agrupam objetos similares em categorias, o que possibilita implementar medidas de proteção que vão garantir a confidencialidade da informação.

Existem diversos tipos de iniciativas para lidar com problemas de segurança da informação, dentre os quais se destacam: iniciativas governamentais; iniciativas normativas; iniciativas tecnológicas.

No contexto da Federation of American Scientists (FAS), associação formada em 1946 pelos cientistas atômicos do Projeto Manhattan[1], Quist (1993) discute a necessidade de uma classificação da informação, para fins de segurança e descreve as três ações principais para tal: i) determinar se a informação deve ser classificada; ii) determinar o nível de classificação; iii) determinar a duração da classificação. O autor também apresenta procedimentos para avaliar, se a informação deve ser classificada: i) definir precisamente a informação, descrevendo-a em linguagem sem ambigüidades; ii) verificar a existência de classificação específica

1 Projeto em que os Estado Unidos tentavam desenvolver a primeira arma nuclear durante a 2º Guerra Mundial.

para o setor da organização, onde 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 é classificada.

O ISOO (2003) estabelece um sistema de classificação da informação para segurança no âmbito do governo norte-americano. São descritas algumas regras sobre classificação de documentos, como, por exemplo: i) apenas pessoas autorizadas podem classificar documentos originais; ii) existem apenas três níveis de classificação: supersecreto, secreto e confidencial; iii) informações não devem ser classificadas pelo sistema de classificação, caso não sejam de interesse da segurança nacional. O ISOO (2003) descreve ainda marcas obrigatórias, aplicadas aos documentos originais, para identificação dos níveis de segurança a adotar: i) marcas em partes do documento, caso tais partes tenham diferentes classificações; ii) classificação do documento como um todo, com o nível mais restrito de classificação presente dentre as partes do documento; iii) inserção dos campos *classificados por, razão da classificação e data final da classificação* no documento.

No Canadá, o Government of Alberta (2005) dispõe de um sistema de classificação de documentos que tem por objetivos: i) proteger a informação pessoal; ii) proteger a informação confidencial contra acesso não autorizado; iii) proteger a propriedade intelectual do governo; iv) dar suporte à disseminação de informação; v) possibilitar cooperação intergovernamental e para segurança pública. O sistema de classificação identifica quatro níveis de segurança para a informação: irrestrita, protegida, confidencial e restrita. Existem casos em que a informação é de interesse nacional e, assim, classificada como: confidencial, secreta e supersecreta. Na prática, a implementação da classificação envolve os seguintes procedimentos: i) marcar a informação; ii) armazená-la; iii) transmiti-la; iv) descartar a informação desnecessária; v) permitir o acesso e a divulgação apropriados; vi) estabelecer responsabilidades.

Baker (2004) estabelece categorias para informação e para sistemas de informação, no âmbito do National Institute of Standards and Technology (NIST)[2]. As categorias propostas – *baixa*, *moderada*, *alta* – têm como base o impacto potencial para a organização, quando ocorrem eventos que colocam em risco a informação e os seus sistemas. A avaliação do impacto em categorias fundamenta-se nos objetivos de segurança para informação e para sistemas de informação (confidencialidade, integridade, disponibilidade) especificados pelo Legal Information Institute (2005).

Baker (2004) apresenta um conjunto de procedimentos para mapeamento entre a informação e os níveis de impacto que pode provocar: 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: i) identificar as áreas de negócio fundamentais; ii) identificar, para cada área de negócio, as operações que descrevem o propósito do sistema em termos funcionais; iii) identificar as subfunções necessárias para conduzir cada área; iv) selecionar tipos de informações básicas associados com as subfunções identificadas; v) identificar qualquer tipo de informação que receba manipulação especial por ordem superior ou agência regulatória.

As iniciativas citadas apresentam considerações sobre segurança da informação, sem, entretanto, definir exatamente a qual objeto se refere, quando citam o termo "informação". Além disso, também não é citado o meio onde a informação é disseminada na organização. Uma importante forma para disseminação é o meio digital, representado por documentos em formato digital, sistemas de informação automatizados, dentre outros recursos de TI.

3. Segurança da informação no contexto da TI

Em muitas organizações, os gerentes encarregam as equipes de TI de solucionar questões de segurança da informação. Tal prática tem conduzido a planos de segurança fundamentados em soluções puramente tecnológicas e, dessa forma, ineficientes em atender às necessidades da organização. A comunidade de

2 Parte do U.S. Department of Defense.

negócios é quem realmente sabe da importância de determinada informação no contexto organizacional e deve participar ativamente do planejamento da segurança.

A ISO/IEC-15408-1 (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 consumidores, desenvolvedores ou avaliadores, nem sempre possuem conhecimento ou recursos para julgar questões de segurança. Para atender a esses usuários, a ISO/IEC-15408-1 (2005) estabelece um critério comum para a avaliação, o que possibilita que o resultado seja significativo para audiências variadas. O resultado das avaliações da ISO/IEC-15408-1 (2005) auxilia os consumidores de TI a decidirem se um produto ou sistema atende aos requisitos de segurança. Do ponto de vista do desenvolvedor, a norma descreve as funções de segurança, que devem ser incluídas no projeto do *objeto de avaliação*. Do ponto de vista dos avaliadores e de outros membros da organização, a norma determina as responsabilidades e as ações necessárias para a avaliação do objeto.

No âmbito da internet, cabe destacar o papel do Computer Emergency Response Team/Coordination Center (CERT/CC), criado pelo Defense Advanced Research Projects Agency (ARPA), após o incidente worm[3], em 1988. O objetivo é centralizar a coordenação de respostas a incidentes de segurança. Além disso, o CERT ainda é responsável por publicar informes, pesquisar sobre segurança e manter um banco de dados sobre segurança em redes e na internet.

Além das referências principais, uma grande diversidade de iniciativas para segurança da informação, na área de TI, vem surgindo desde os anos 80: roteiros para avaliações e para auditorias (Kraus, 1980; GAO, 1988; Garfinkel e 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). Os autores advogam a necessidade de uma linguagem comum sobre segurança, que permita o intercâmbio e a comparação de dados sobre incidentes de segurança. Tal linguagem é composta por termos de alto nível, ou seja, genéricos, estruturados em uma taxonomia.

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 (ataque físico, 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, 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 mais um objetivo, o qual pode ser ganho político ou financeiro, danos ou prejuízos, etc.

O uso de uma linguagem única, com significados consensuais, possibilita a construção de modelos sobre um domínio do conhecimento e pode incrementar a forma com que os indivíduos da empresa aprendem novas práticas, compartilham conhecimento e o armazenam com um nível de ambigüidade reduzido (Von Krogh e Roos, 1995; Eccles e Nohria, 1994). As linguagens informais, como a linguagem natural, são expressivas, mas geram interpretações ambíguas. As linguagens formais proporcionam a criação de modelos com nível de ambigüidade reduzido e com significados consistentes para o contexto da organização. Uma ontologia pode operacionalizar a linguagem formal, visto que possui conceitos, relações e atributos semanticamente bem definidos e pode variar em grau de formalidade, conforme a necessidade.

A linguagem representada pela ontologia precisa estar restrita apenas a um vocabulário sobre segurança da informação. Pode abranger conceitos significativos para uma organização naquele domínio, além de permitir a classificação da informação registrada, ou seja, a classificação dos documentos corporativos pelos próprios membros da organização.

3 Robert T. Morris, estudante da *Cornell University*, criou, em 1988, um *worm* para um experimento de acesso a computadores. O programa deveria detectar a existência de cópias de si mesmo e não reinfectar computadores. Um bug impediu a detecção e sistemas foram infestados com centenas de cópias do worm, cada uma delas tentando acesso e se replicando em mais worms. (Menninger, 2005)

4. Ontologias aplicadas à segurança da informação

O termo ontologia é originário da filosofia e tem sido utilizado desde o início dos anos 80, em Ciência da Computação e em Ciência da Informação, para designar uma estrutura de organização da informação, com base em um vocabulário representacional. Segundo Borst (1997), uma ontologia é uma especificação formal e explícita de uma conceitualização compartilhada. Nessa definição, formal significa legível por computadores; especificação explícita diz respeito a conceitos, relações e a axiomas explicitamente definidos; compartilhado quer dizer conhecimento consensual; conceitualização diz respeito a um modelo abstrato de algum fenômeno do mundo real[4].Com aplicações em diversas áreas, as ontologias também servem a propósitos de segurança da informação, conforme comprovam exemplos apresentados na seção 4.1. A seção 4.2 apresenta um breve roteiro sobre como construir uma ontologia organizacional, para classificação da informação em projetos de segurança da informação.

4.1 Pesquisa anterior significativa sobre ontologias em segurança

Segundo Raskin et al. (2001), a pesquisa em segurança da informação pode se beneficiar da adoção de ontologias. Os autores apresentam duas propostas para utilização da ontologia na pesquisa em segurança da informação.

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 os usuários de produtos e sistemas de informação ao proporcionar intercâmbio, organização e comparação de dados sobre incidentes de segurança, bem como melhorias na capacidade de tomada de decisão diante de um incidente.

A segunda proposta consiste em incluir fontes de dados em linguagem natural na aplicação de ações em segurança da informação. Dessa forma, seria possível especificar formalmente o know-how da comunidade de segurança, possibilitando o incremento de medidas para prevenção e para reação a ataques. O Processamento de Linguagem Natural (PNL)[5] pode ser aplicado, por exemplo, no processamento de logs de sistemas, os quais são escritos em uma sublinguagem da linguagem natural.

Para Martiniano e Moreira (2007), o grande volume de dados gerado por diferentes fontes, tais como logs de sistemas, de firewalls[6], alertas de vulnerabilidade, etc., tem causado problemas aos administradores. O principal problema está relacionado com a dificuldade em acumular conhecimento para a tomada de decisão e para a solução de incidentes de segurança.

Apesar dos esforços em classificar dados sobre segurança, as iniciativas, em geral, não contemplam a semântica dos dados armazenados. Sem o significado dos dados, um administrador ou um agente de software não é capaz de fazer correlações sobre os incidentes de segurança. Nesse contexto, Martiniano e Moreira (2006) propõem uma ontologia de incidentes de segurança, a qual define um vocabulário único. A maioria dos conceitos da ontologia sobre incidentes de segurança foi obtida de glossários e taxonomias sobre segurança da informação (Howarde Longstaff, 1998; NSCS, 1988; Shirley, 2000), em recursos sobre vulnerabilidade (NVD-National Vulnerability Database[7], CVE-Common Vulnerabilities and Exposures Project[8]). Para avaliar se é representativa, a ontologia foi confrontada com o SNORT[9].

Fenz et al. (2007) também propõem a construção de uma ontologia,

4 Para um estudo comparativo das diversas definições de ontologias e suas aplicações ver Almeida (2003).

5 *Processamento da linguagem* natural é um campo da lingüística computacional que estuda os problemas de compreensão e geração automática de linguagens naturais.

6 Um *firewall* é uma aplicação que analisa o tráfico em uma rede, dando permissão ou não para 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/.

8 CVE é um dicionário público com informações sobre vulnerabilidades. Disponível na internet em http://cve.mitre.org/.

9 SNORT é uma rede com recursos sobre prevenção e detecção de invasões em sistemas, a partir de uma linguagem com base em regras. Disponível na internet em http://www.snort.org/.

em Ontology Web Language (OWL), de suporte à certificação ISO/IEC-27001 (2005), com informações para criação e manutenção de políticas de segurança. O mapeamento ontológico do padrão ISO aumenta o grau de automação do processo, reduzindo custos e o tempo 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), a qual contempla o domínio Common Criteria[10] (CC) 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; iii) o próprio padrão ISO/IEC-27001 (2005). A Figura 1 apresenta um fragmento de uma ontologia sobre segurança.

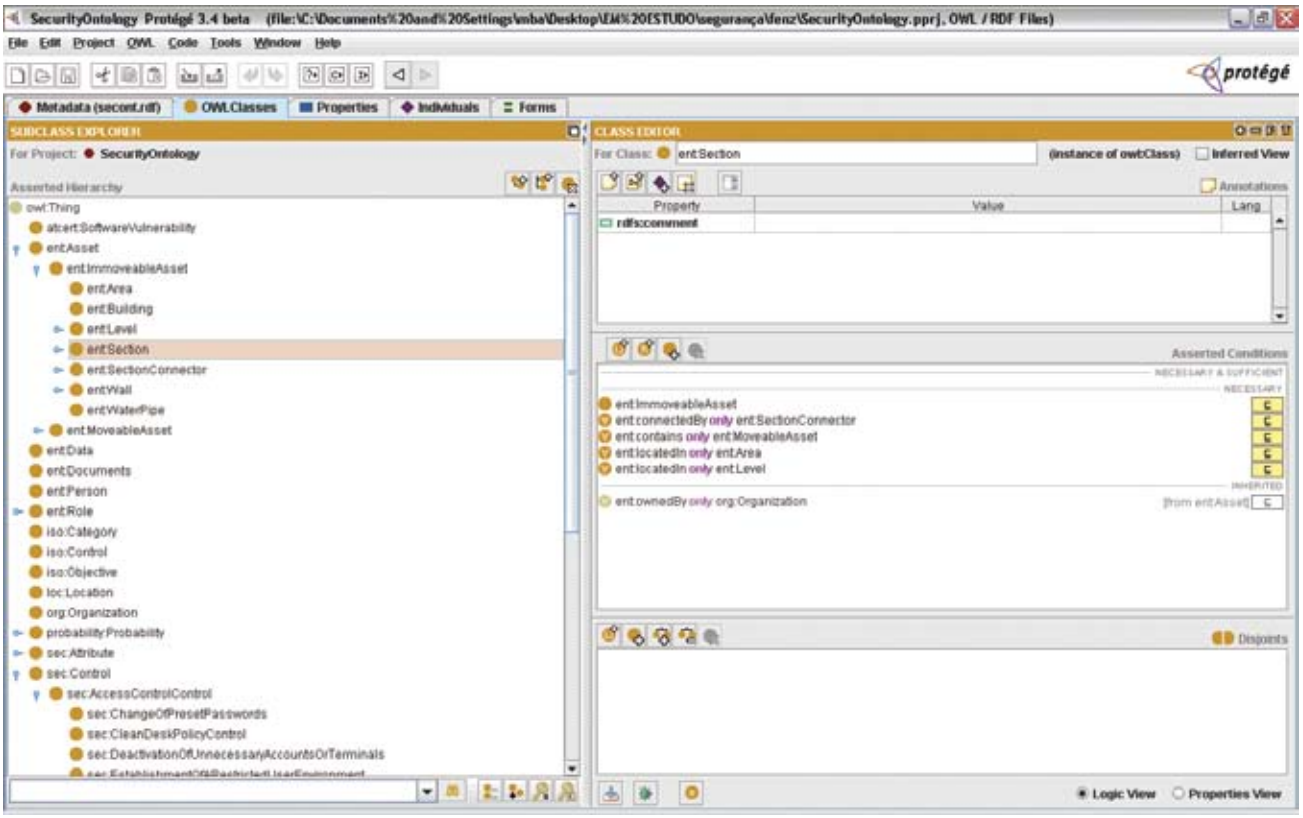

Figura 1 – Ontologia de incidentes em um editor de ontologias (Fenz et al., 2007).

4.2 Construção de ontologia organizacional para segurança da informação

Existem aplicações com base em ontologias para segurança da informação, conforme comprovam as iniciativas apresentadas na seção 4.1. Tais iniciativas estão relacionadas com a criação de um vocabulário consensual, de alto nível, com termos sobre segurança da informação. Pretende-se apresentar uma abordagem que enfatize duas ações principais: i) agrupamento dos termos sobre segurança em uso no dia-a-dia da

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

organização e dos termos obtidos em ontologias de alto nível, os quais representam padrões aceitos no domínio; ii) integração do vocabulário sobre segurança a um vocabulário mais amplo, representativo da informação registrada e compartilhado por todos os membros da organização. As duas contribuições podem ser operacionalizadas em uma ontologia.

Apresenta-se, a seguir, um conjunto de procedimentos e uma breve descrição sobre como construir ontologias para classificação de informação registrada (documentos). O processo foi dividido em duas etapas, apresentadas de forma genérica: 1- Ontologia e 2- Recursos corporativos.

Etapa 1 – Ontologia

i. Aquisição de conhecimento: o objetivo dessa etapa é obter, com os membros de um setor, informações sobre suas atividades, sobre documentos que utilizam, sobre conceitos e relações relevantes para o entendimento das práticas organizacionais. As técnicas mais utilizadas para isso são as entrevistas e a análise de documentos.
ii. Conceitualização: os dados são organizados em uma taxonomia corporativa composta por classes representativas de conceitos, bem como por relações entre as classes; em ontologias, classes representam uma categoria de objetos similares, denominados instâncias.
iii. Construção da ontologia[11]: a ontologia é então construída por meio de um editor de ontologias e em duas camadas: a primeira, de alto nível (reaproveitamento de outras ontologias, como as da seção 4.1); a segunda, com termos específicos do ambiente de trabalho, levantados na fase de aquisição de conhecimento e organizados na fase de conceitualização.

Etapa 2 – Recursos corporativos

i. Organização dos documentos: a partir de princípios da arquivística, organizam-se os documentos, conforme sua origem, registram-se a tipologia de documentos e seu ciclo de vida e elegem-se os documentos vitais[12] para as atividades corporativas.
ii. Padronização dos documentos: a partir de princípios da Organização, Sistemas e Métodos (OSM), os documentos são padronizados formalmente e é acrescentada uma folha de rosto a cada um, na qual são registrados dados como autor, data de emissão, data de revisão, autorização, dentre outros.
iii. Classificação dos documentos: os membros dos setores são orientados e treinados para classificar documentos, conforme as classes definidas na ontologia, assim que estes são produzidos; a classificação é feita na folha de rosto e pode ocorrer, a partir de um sistema de informação automatizado, que a consulta à ontologia seja um documento em formato digital ou em papel.

Com esses procedimentos, apresentados de forma simplificada, os documentos, que correspondem a uma grande parte da informação registrada na organização, são classificados e relacionados entre si. A ontologia permite a inserção de atributos, os quais podem apresentar características especiais de um documento, como por exemplo, sua confidencialidade, temporalidade, dentre outros. Além de permitir a classificação, a ontologia pode armazenar, ainda, as *instâncias* de tipos de documentos, ou seja, referências aos próprios documentos utilizados na rotina organizacional.

A ontologia resultante é um modelo consultado por um sistema, que pode ser, por exemplo, de gestão de documentos. Sugere-se que a interface de classificação seja integrada a outra interface já em uso, de forma que o usuário não tome a tarefa como um trabalho adicional. A ontologia passa a ser a referência única para qualquer sistema de informação em uso na organização em questões que dizem respeito à segurança da informação.

11 Para um levantamento abrangente sobre ferramentas, linguagens e metodologias para a construção de ontologias ver Almeida (2003).

12 Documentos vitais são aqueles essenciais para atestar uma atividade em um contexto organizacional, ou seja, documentos sem os quais os processos não teriam início, continuidade, e os agentes não contariam com instrumental para exercer avaliações e gestão.

5. Considerações Finais

Este artigo apresentou considerações sobre segurança da informação, destacando iniciativas governamentais, normativas e tecnológicas. Sem pretensão de abranger toda a pesquisa em segurança da informação, apresentou-se apenas o suficiente para uma visão geral da área. Introduziu-se, então, a ontologia como importante instrumento para projetos de segurança nas organizações, e descreveu-se um breve roteiro para a sua construção.

Vários benefícios podem ser contabilizados com o uso de ontologias em projetos de segurança: i) criar modelos conceituais que tornam possível a organização saber mais sobre o domínio de incidentes de segurança; ii) facilitar a interoperabilidade entre diferentes ferramentas de segurança; iii) criar um padrão para estruturar dados sobre segurança e possibilitar que termos diversos sejam mapeados para a ontologia; iv) possibilitar a reutilização de dados sobre segurança, por meio da importação e exportação de ontologias; v) auxiliar os administradores de sistemas nas decisões sobre gestão de segurança, com possibilidades de consultas e de inferências automáticas.

Apesar das vantagens com o uso de ontologias, cabe destacar a influência do fator humano. Tal influência é marcante pelo fato de que grande parte dos problemas de segurança é gerada por ações, intencionais ou não, de pessoas em suas atividades rotineiras. A classificação da informação registrada em uma ontologia pelos próprios usuários, a partir de suas necessidades, é uma primeira resposta ao problema do fator humano. Ao tornar as pessoas parte do processo, orientá-las, treiná-las e deixar que decidam sobre a classificação das informações que manipulam rotineiramente, pode-se esperar por colaboração nas iniciativas de segurança da informação. Sem essa participação, fomentada pela abordagem distribuída de conhecimento consensual da teoria das ontologias, nenhum sistema tecnológico de segurança poderá ser considerado eficiente, a partir de uma abordagem sistêmica.

Referências

ARAÚJO, L. A. D. *A correspondência eletrônica do empregado e o poder diretivo do empregador*. *In*: Revista de direito constitucional ALMEIDA, M.B.; BAX, M.P. Uma visão geral sobre ontologias: pesquisa sobre definições, tipos, aplicações, métodos de avaliação e de construção. *Ciência da Informação*. v. 26, n. 1. p. 39-45, set./dez. 2003.

BAKER, W. *Information security*; volume I. (2004). Available from Internet: <http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf >. Access: 02 May 2006.

CIAO-Critical Infrastructure Assurance Office. *Practices for Securing Critical Information Assets*. (2000). Available from Internet: <http://www.infragard.net/library/pdfs/securing_critical_assets.pdf> . Access: 02 Dec. 2007.

ECCLES, R.G.; NOHRIA, N. *Assumindo a responsabilidade*; redescobrindo a essência da administração. Rio de Janeiro: Campus, 1994. 287p.

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). Available from Internet: <http://www.springerlink.com/index/w530v5081301j833.pdf>. Access: 30 July 2007.

FENZ, S. et al. I*nformation security fortification by ontological mapping of the ISO/IEC 27001 Standard*. (2007). Available from Internet: <http://www.ifs.tuwien.ac.at/node/4274 >. Access: 19 Nov. 2007.

FOWLER, S. *GIAC Security essentials certification*. (2003). Available from Internet: <http://www.sans.org/reading_room/whitepapers/auditing/846.php>. Access: 13 April 2005.

GAO-General Accounting Office of United States. *GAO Audit Guide*. (1988). Available from Internet: <http://www.gao.gov/index.html>. Access: 15 Nov. 2007.

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

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

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>. Access: 13 Dec. 2006.

ISACF-Information Systems Audit and Control Foundation. *COBIT-Control Objectives for Information and Related Technology*. (2000). Available from Internet: <http://www.isaca.org/>. Access: 01 Dec. 2007.

ISSEA-International Systems Security Engineering Association. *SSE/CMM-System Security Engineering/Capability Maturity Model, V3.0*. (2003). Available from Internet: <http://www.sse-cmm.org/>. Access: 02 Dec. 2007.

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

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

ISOO-*The Information Security Oversight Office*; Marking classified national security information. (2003). Avalaible from Internet: <http://www.archives.gov/isoo/training/marking-booklet.pdf>. Access: 12 Jan. 2006.

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

KRAUSS, L. I. *SAFE*; 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.

LII-Legal Information Institute of Cornell University. *U.S. Code collection*; 3452 Definitions. (2005). Available from Internet: <http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542----000-.html>. Access: 8 Dec. 2007.

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

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

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

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

NCSC-National Computer Security Center. *Glossary of computer security itens*. (1988). Available from Internet: <http://packetstormsecurity.org/docs/rainbow-books/NCSC-TG-004.txt >. Access: 15 Nov. 2007.

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

NIST/CSD-Nacional Institute of Standards and Technology/Common Criteria/Computer Security Division. *Common Criteria for Information Technology Security Evaluation*. (1998). Available from Internet: <http://csrc.nist.gov/nissc/1999/proceeding/papers/p15.pdf >. Access: 01 Dec. 2007.

OECD-Organization for Economic Cooperation and Development. *Guidelines for the Security of Information Systems*. (1992). Available from Internet: <http://www.oecd.org/ >. Access: 01 Dec. 2007.

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

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

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

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

WILSON, T.D. *The nonsense of 'knowledge management'* . (2002). Available from Internet: <http://informationr.net/ir/8-1/paper144.html#non95>. Access: 03 April 2006.

WOOD, C. C. *Principles of Secure Information Systems Design*. (1990). Available from Internet: <http://portal.acm.org/citation.cfm?id=85089.85091>. Access: 22 Sept. 2007.

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