Ontologias sobre segurança da informação em biomedicina: tecnologia, processos e pessoas

Luciana Emirena dos Santos Carneiro, Maurício Barcellos Almeida

Escola da Ciência da Informação – Universidade Federal de Minas Gerais – UFMG
Avenida Antônio Carlos, 6627– Campus Pampulha - 31.270-901–Belo Horizonte – MG

lucianaemirena@gmail.com, mba@eci.ufmg.br

Abstract. *An issue concerning the organizational information security is the lack of standards to describe incidents. One of the first initiatives to face attacks and failures may be the creation of a uniform vocabulary. Ontologies are an alternative to organize such vocabulary. This paper advocates that information security guidelines are effective insofar as they are able to encompass three perspectives – namely, technology, people, and processes – and that such perspectives are present within ontologies development process. We describe the preliminary terminological stage of an information security ontology, part of an ongoing research, as well as its future uses.*

Resumo. *Uma questão sobre segurança da informação nas organizações é a falta de padronização para descrever incidentes. Um vocabulário uniforme é o primeiro passo responder as tentativas de ataque e falhas. Ontologias são uma alternativa para organizar tal vocabulário. Esse artigo advoga que políticas de segurança da informação são efetivas na medida em que abrangem três perspectivas – tecnologia, pessoas, e processos – e que tais perspectivas estão presentes no processo de desenvolver ontologias. Descreve-se estágio terminológico preliminar de ontologia para segurança da informação, parte de pesquisa em andamento, bem como suas possibilidades de uso.*

1. Introdução

A evolução dos sistemas de informação tem possibilitado às empresas ganhos em mobilidade e conectividade. A descentralização promovida pelas redes, entretanto, tem exigido mais atenção à gestão e ao controle, em um conjunto de esforços que se convencionou chamar de "segurança da informação".

Os investimentos em segurança da informação tem sido crescentes, mas existem dificuldades em definir: o que deve ser protegido, qual o nível de proteção necessário, e quais as ferramentas utilizar no ambiente corporativo. A TI tem meios para solucionar parte do problema de segurança, mas o elemento humano ainda representa grande parte das ocorrências e falhas de segurança [Colwill, 2010].

O presente artigo apresenta pesquisa em andamento na qual se busca os requisitos para definir segurança da informação na perspectiva de tecnologia, pessoas, e processos. Usa-se uma abordagem baseada em ontologias para classificar informações sobre segurança, cujos resultados correspondem ao estágio terminológico preliminar de uma ontologia de domínio sobre segurança da informação na área de saúde, a qual ainda requer decisões de natureza ontológica, criação de restrições, validação, implementação, dentre outros. Tais ações estão planejadas para a sequencia da pesquisa.

O restante do artigo está dividido conforme segue. A seção 2 apresenta uma visão geral da segurança da informação e a seção 3 detalha a segurança do ponto de vista das três perspectivas mencionadas. A seção 4 descreve a metodologia de pesquisa, a seção 5 apresenta resultados parciais e a seção 6 apresenta considerações finais.

2. Segurança da informação: uma visão geral

Segurança da informação é uma questão multifacetada, composta por diversas variáveis interagindo em um único ambiente. Uma empresa demanda confidencialidade da informação sem, entretanto, perder a disponibilidade frente aos riscos, ameaças e vulnerabilidades. A segurança da informação abrange a totalidade dos elementos de negócio corporativos: a busca de melhorias em processos que garantem a qualidade e competitividade; o aprendizado e a produção de conhecimento organizacional; a criação de modelos e o uso das informações; detecção e prevenção, assim como documentação de potenciais riscos, ameaças e vulnerabilidades.

A TI é quesito fundamental em qualquer solução para a segurança da informação. Os sistemas, contudo, são projetados, implementados e operados por pessoas. São pessoas que proporcionam segurança física, concedem acesso aos sistemas, causam, relatam e gerenciam a resposta das empresas frente às violações e incidentes de segurança [Lacey, 2009].

Segundo Sveen, Torres e Sarriegi (2009), o desenvolvimento de um plano estratégico de segurança da informação efetivo depende dos aspectos: i) pessoas, como formadoras da cultura organizacional; ii) processos, como condutores do fluxo informacional; e iii) tecnologias, ferramentas que sustentam processos e necessidades dos usuários.

3. Fatores intervenientes em segurança da informação

A concepção sobre o que é segurança da informação tem evoluído e não mais se restringe apenas à questão técnica. A segurança da informação está atrelada ao negócio da empresa através da necessidade de proteção dos ativos informacionais. Esses ativos informacionais não incluem apenas informações valiosas em repositórios da empresa, ou em suas marcas, mas também o valor fornecido pelo know-how, expertise, habilidades e relacionamentos incorporados na rede corporativa, dentro e fora de seus limites físicos. Os ativos informacionais envolvem assim pessoas, executando processos, em geral, como uso de tecnologia.

3.1. Segurança e pessoas

Incluir pessoas nos estudos de segurança significa dar atenção devida à subjetividade inerente ao seres humanos, suas relações e seu comportamento informacional nas organizações que tanto influencia a gestão e a tecnologia.

O elemento “pessoas” gera vulnerabilidade, uma vez que a falta de conhecimento ou treinamento resulta em condutas inapropriadas às ações de segurança. Colaboradores das organizações, intencionalmente ou por negligência, são a maior ameaça à segurança da informação [Van Niekerk e Solms, 2010]. A segurança depende tanto do conhecimento humano quanto de sua cooperação. A falta de conhecimento é tratada através da educação ou treinamento, enquanto a falta de cooperação é abordada através da promoção de uma cultura de que incentive preocupação com a segurança.

As organizações não podem proteger a integridade, confidencialidade e disponibilidade das informações em ambiente de sistemas em rede, sem garantir que cada pessoa envolvida compreenda suas responsabilidades, e seja treinada para realizá-las.

3.2. Segurança e processos

A adoção de políticas, procedimentos, normas e diretrizes relativas à segurança em organizações, busca tornar claro o comportamento esperado e as regras a seguir. Nesse sentido, uma série de fatores contribuem para segurança ineficaz: falta de especificação e de documentação, incapacidade interna de criar políticas efetivas, e a falta de mecanismos de execução [Kraemer, Carayon e Clem, 2009]. Incidentes decorrentes da ineficácia dos controles são minimizados através de rotinas e instruções acessíveis.

Um fator-chave no sucesso de uma política de segurança é a implantação dos controles de segurança, incluindo o acompanhamento, sanções e recompensas de colaboradores, proporcionais aos potenciais riscos envolvidos [Sianes, 2006].

3.3. Segurança e tecnologia

A necessidade de proteção dos ativos informacionais das empresas faz com que a tecnologia ganhe uma posição de destaque. Existem diversos tipos de controles para auxiliar na gestão da segurança, na limitação dos incidentes e na violação de segurança [Sveen, Torres e Sariegi, 2009]: check-lists, análise de risco, avaliação e métodos de detecção, dispositivos biométricos e de bloqueio, antivírus, firewalls, criptografia, permissões na rede, auditorias, dentre outros.

A ISO/IEC-15408-1 (2005) é a principal referência para avaliação de atributos de segurança em produtos de TI. Esta norma estabelece um critério comum para a avaliação, possibilitando que o resultado seja significativo para audiências variadas.

No âmbito da Internet, cabe destacar o papel do Computer Emergency Response Team / Coordination Center (CERT/CC), cujo objetivo é centralizar a coordenação de respostas à incidentes de segurança.

4. Metodologia de pesquisa

Diversas iniciativas de uso de ontologias em segurança da informação estão disponíveis na literatura [Raskin et al, 2001] [Martiniano e Moreira, 2007] [Fenz et al, 2007] [Ekelhart et al, 2006]. Apresenta-se a seguir um conjunto de procedimentos utilizado em uma organização de saúde para criar a ontologia relativa à segurança. O processo foi divido em três etapas: i) organização da informação registrada; ii) organização da informação especializada; iii) terminologia para ontologia.

Etapa (1) – organização da informação registrada em documentos e em sistemas

- Organização: classificam-se os documentos a partir de seu conteúdo e de sua proveniência, registra-se sua tipologia e seu ciclo de vida, elegem-se os vitais;
- Padronização: acrescenta-se uma folha de rosto a cada documento, na qual são registrados dados como autor, data de emissão, etc;
- Treinamento: os colaboradores são orientados sobre como classificar documentos assim que este é produzido;

- Relatórios: são gerados a partir de registros e dados provenientes de sistemas utilizados no setor, os quais são tratados da mesma forma que os documentos.

Etapa (2) – organização da informação especializada fornecida por pessoas

- Aquisição de conhecimento: obtém-se com os colaboradores e especialistas as informações sobre suas atividades, documentos que utilizam, conceitos e relações relevantes para o entendimento de suas práticas;
- Técnicas: são utilizadas técnicas bem consolidadas, como entrevistas, grade repertórios, ordenamento de cartões, dentre outras;
- Relatórios: o material obtido, sejam de cunho administrativo ou científico, é registrado em sínteses de entrevistas e planilhas;

Etapa (3) – elaboração da terminologia

- Organização preliminar: os dados obtidos são organizados em uma lista composta por termos obtidos nas etapas 1 e 2;
- Estágio terminológico: a lista é organizada agrupando-se substantivos candidatos a conceitos, e verbos candidatos a relações na ontologia; cabe destacar que tais correspondências – verbo ⇔ relação, e substantivo ⇔ classe – são mais simples do que aquelas requeridas para construir a ontologia, mas atendem a demanda por organização preliminar do vocabulário nessa etapa da pesquisa.

Os processos organizacionais e as práticas dos colaboradores registradas em documentos e em sistemas, os quais correspondem à grande parte da informação da organização, são classificados e relacionados entre si. O estágio terminológico, produto parcial da pesquisa em andamento, é parte da atividade de desenvolvimento de ontologia. A atividade de desenvolvimento de ontologias abrange etapas de aquisição e modelagem correspondem à formas de incrementar a comunicação humana [Almeida e Barbosa, 2009]. A ontologia será, após sua consecução, a referência única para classificar dados em uso na organização relativos a segurança da informação.

5. Resultados parciais

Os termos obtidos pela metodologia descrita na seção 4 caracterizam a organização preliminar de dados e resultam no que se denominou aqui de "estágio terminológico". A Tabela 1 resume as entidades consideradas básicas e traz uma descrição de seu significado obtida no âmbito da organização de saúde.

Tabela 1 – Exemplos de termos e definições da ontologia de segurança

Entidade	Descrição
Organização	Organização é uma entidade social composta por recursos materiais e humanos, e caracterizada por objetivos, procedimentos de controle e limites. Ex. pública, privada.
Atributo de segurança	Atributo de segurança caracteriza um ativo e diz respeito a requisitos de segurança sobre tal ativo. Pode ser um atributo de confidencialidade, ou de integridade.
Ativo	Ativo é um bem da organização, seja físico ou imaterial, utilizado

	pelos seus membros para alcançar os objetivos estipulados. Ex. um, um sistema, um documento.
Controle	Controle é um procedimento sistematizado para atenuar vulnerabilidades, bem como para estabelecer medidas preventivas e corretivas com vistas à proteção de ativos.
Ameaça	Ameaça é uma possibilidade de dano aos ativos da organização, que afeta atributos de segurança e explora vulnerabilidades. Ex. de origem humana ou natural.
Vulnerabilidade	Vulnerabilidade é a situação caracterizada por falta de medidas de proteção e que possui um grau de severidade associado. Pode ser administrativa, técnica ou física.

A Figura 1 apresenta a organização de termos correspondente ao estágio terminológico preliminar, resultado parcial de pesquisa. Enfatiza-se que o estágio de pesquisa aqui apresentado requer ainda considerações para que se possa obter a ontologia. A organização de termos e definições se restringe, nessa etapa, a uma visão terminológica que ainda carece de considerações adicionais de natureza ontológica. O conjunto terminológico é composto por 165 termos representativos de conceitos no domínio da segurança da informação, bem como classes. Os termos estão distribuídos da seguinte forma: 13 tipos de ativo (por ex., móvel, sistema), 3 tipos de organização (por exemplo, pública), 11 tipos de atributos de segurança (por ex. confiabilidade), 51 tipos de ameaça (por ex., controle de operações em servidores), e 40 tipos de vulnerabilidades (por ex. término de contrato de trabalho de colaborador).

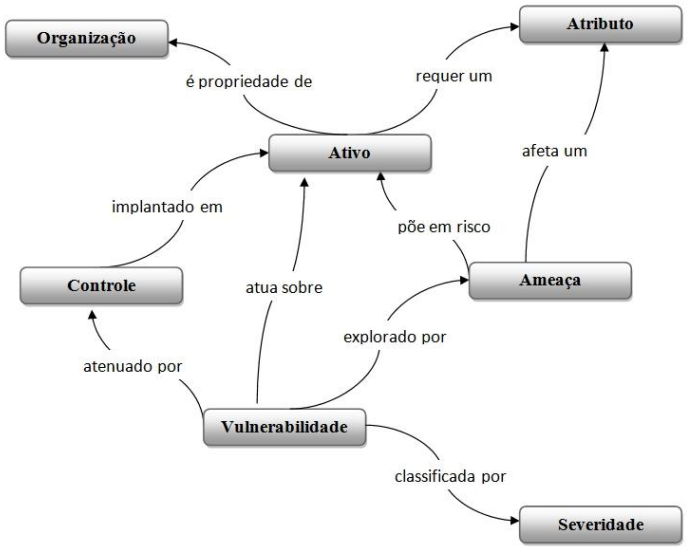

Figura 1: Organização preliminar de termos básicos em forma de rede semântica

6. Considerações finais

O presente artigo aborda a necessidade de se tratar a Segurança da Informação sob a ótica da tríade "pessoas – processos – tecnologias" no contexto corporativo. Através das

ontologias pretende-se registrar, classificar e relacionar as informações de segurança informacional através de uma abordagem sócio-técnica em instituições de saúde.

Entende-se que através do mapeamento das práticas de segurança da informação dos colaboradores da área biomédica, seu registro e documentação, e conseqüente classificação e relacionamento das entidades apuradas, promover-se-á um mecanismo de criação de conhecimento organizacional e desenvolvimento para processos e sistemas.

O desenvolvimento de ontologias é uma oportunidade para unir perspectivas e integrar pessoas, processos e tecnologias de forma equitativa. Fomenta a criação, aquisição e compartilhamento de conhecimento, bem como a aprendizagem organizacional. Os resultados esperados apontam para um produto de informação, uma base de conhecimento, que auxiliará o desenvolvimento de sistemas e políticas no contexto empresarial em que for aplicada.

Na continuidade da pesquisa, pretende-se reavaliar ontologicamente os dados organizados no estágio preliminar de termos, buscando alinhamento com ontologias de alto nível e, em última instância, a redução da ambigüidade.

7. Referências

Almeida, M. B.; Barbosa, R. R. (2009). Ontologies in knowledge management support - a case study. In: Journal of American Society of Information Science and Technology. vol. 60, n.10, p. 2032-2047.

Colwill, C.(2010). Human factors in information security: The insider threat e Who can you trust these days? In: Information Security Technical Report, p. 01-11.

Ekelhart, A. et al.(2006) Security ontology; simulating threats to corporate assets, http://www.springerlink.com/index/w530v5081301j833.pdf, July.

Fenz, S. et al.(2007) Information security fortification by ontological mapping of the ISO/IEC 27001 Standard, http://www.ifs.tuwien.ac.at/node/4274, November.

Lacey, D.(2009). Managing the human factor in information security. Wiley.

Kraemer A. S.; Carayon, P.; Clem, J. (2009) Human and organizational factors in computer and information security: Pathways to Vulnerabilities. In: Computer e Security, v.28, p. 509-520.

Martiniano, L. A. F.; Moreira, E. S. (2007) An OWL-based security incident ontology, http://protege.stanford.edu/conference/2005/submissions/posters/poster-martimiano.pdf, November.

Raskin, V. et al. (2001) Ontology in information security; a useful theoretical foudation and methodological tool, http://portal.acm.org/ft_gateway.cfm?id=508180, August.

Sveen, F. O.; Torres, J. M.; Sarriegi, J. M. (2009). Blind Information Security Strategy. In: International Journal of Critical infrastructure Protection, v.2, p.95-109

Sianes, M. (2005). Compartilhar ou proteger conhecimentos? In: Gestão Estratégica da Informação e Inteligência Competitiva. São Paulo.

Van Niekerk, J. F.; Von Solms, R. (2010). Information Security Culture: A management perspective. In: Computer & Security, n.4,v.29, p.476.