Uma Ontologia para Gestão de Segurança da Informação

Paulo Fernando da Silva, Henrique Otte, José Leomar Todesco, Fernando A. O. Gauthier

Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento (EGC) – Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brasil

{paulofernando@furb.br, otte@stela.org.br, tite@inf.ufsc.br, gauthier@egc.ufsc.br

Abstract. *This article presents some problems of knowledge management in management information security organizations and suggests ontologies as part of solving these problems. The article describes the construction of a specific ontology for information security using the methodology NeOn and discusses the use of this ontology in the management information security environment.*

Resumo. *Este artigo apresenta alguns problemas de gestão do conhecimento em organizações de consultoria de gestão de segurança da informação e sugere ontologias como parte da solução destes problemas. O artigo descreve a construção de uma ontologia para gestão de segurança da informação utilizando a metodologia NeOn e discute o uso desta ontologia no cenário de gestão de segurança da informação.*

1. Introdução

A gestão de segurança da informação é realizada por consultores internos ou externos em uma organização com o objetivo de identificar o grau de segurança de um ambiente corporativo e propor controles tecnológicos ou administrativos para a redução dos riscos de incidentes de segurança da informação neste ambiente.

Geralmente o conhecimento necessário para a realização de um projeto de gestão de segurança da informação está descrito em normas técnicas, como a ISO 27001 (conhecimento explícito), ou internalizado na mente dos consultores de segurança da informação (conhecimento tático), sendo que neste segundo caso a qualidade do projeto de gestão de segurança da informação depende da experiência e prática do consultor. Este fator torna-se um problema na medida em que empresas de consultoria em segurança da informação não conseguem manter a mesma qualidade de atendimento em todo o seu corpo de consultores, ou seja, um consultor com mais experiência ou conhecimentos específicos poderá desempenhar um trabalho diferenciado frente a outros consultores [Kim, 2007].

Considerando também o problema da dispersão de conhecimento (em diversas normas técnicas, políticas, boas práticas e na mente dos consultores) nas organizações de consultoria em gestão de segurança da informação, a construção de uma especificação explícita e formal para o gerenciamento deste conhecimento seria um grande avanço rumo à gestão do conhecimento nestas organizações.

As ontologias visam à definição de semântica para representação do conhecimento em um dado contexto [Bachimont, 2002]. Uma ontologia aplicada à gestão de segurança da informação poderia contribuir para a gestão do conhecimento em empresas de consultoria de gestão de segurança da informação, servindo de auxílio para os processos de aquisição, representação, armazenamento e compartilhamento de conhecimento obtido a partir de normas e consultores de segurança da informação.

O objetivo inicial deste artigo é mostrar a construção de uma ontologia para gestão de segurança da informação seguindo a metodologia NeOn de desenvolvimento de ontologias. Futuramente espera-se que esta ontologia possa ser utilizada na gestão de conhecimento em organizações de consultoria de segurança da informação.

A seção 2 deste artigo apresenta os conceitos de segurança da informação que serviram de base para a construção da ontologia. A seção 3 descreva a construção da ontologia a partir dos conceitos de segurança da informação. A seção 4 descreve resultados obtidos até o momento com o desenvolvimento da ontologia, e a seção 5 apresenta as conclusões e extensões do projeto.

2. A Gestão de Segurança da Informação

Vários elementos compõem a Gestão de Segurança da Informação. Estes elementos permitem a realização de análises de risco, definição de controles de segurança da informação e a melhoria contínua do ambiente. Um elemento essencial na gestão de segurança da informação é o ativo de informação. Ativo de informação é qualquer informação que possua valor para a organização, bem como qualquer outro elemento de infraestrutura que forneça suporte a esta informação, como: hardwares, softwares e ambientes físicos [Campos, 2007].

Para a realização de uma análise de risco de segurança da informação existe a necessidade da definição de Ameaças e Vulnerabilidades relacionadas ao ambiente a ser avaliado. Ameaça é o agente ou condição que realiza um incidente de segurança da informação [ABNT, 2006]. Grupos comuns de ameaças podem ser: invasores internos, invasores externos, eventos naturais e programas maliciosos (*malwares*).

Vulnerabilidades são falhas em potencial existentes nos ativos de informação. As vulnerabilidades podem ser agrupadas de diversas maneiras. Uma forma simples de agrupar ou categorizar as vulnerabilidades ocorre dividindo-as em: deficiências físicas ou deficiências lógicas [ABNT, 2007].

Os conceitos discutidos acima serão modelados em uma ontologia para gestão de segurança da informação (seção 3 deste artigo) com o objetivo de se estabelecer uma conceituação clara e explícita dos mesmos.

3. Ontologia para Segurança da Informação Utilizando Metodologia NeOn

A partir de conceitos gerais de gestão de segurança da informação, foram modeladas classes de indivíduos para uma ontologia de segurança da informação. Estas classes foram modeladas utilizando-se a ferramenta NeOn e a metodologia NeOn de construção de ontologias [Suárez-Figueroa, 2008]. A Figura 1 apresenta as classes resultantes a partir dos conceitos de segurança da informação levantados. Pode-se observar a criação

das classes Ameaça, Vulnerabilidade e AtivoInformação, bem como suas respectivas sub-classes.

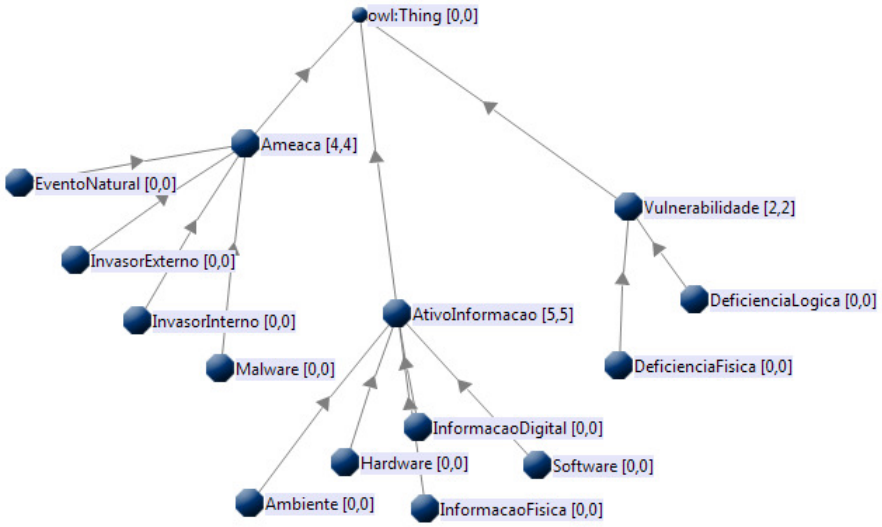

Figura 1. Modelagem das classes da ontologia

Após a definição das classes de indivíduos da ontologia, é necessário estabelecer a relação entre elas. Conforme os conceitos de gestão de segurança da informação, um incidente ocorre quando uma ameaça explora uma vulnerabilidade existente em um ativo de informação. Outro conceito importante é o fato de que ativos de informação podem estar localizados dentro de outros ativos de informação, por exemplo, um documento digital importante para a organização está localizado em um servidor, que por sua vez está localizado em um *Data Center* (ambiente físico).

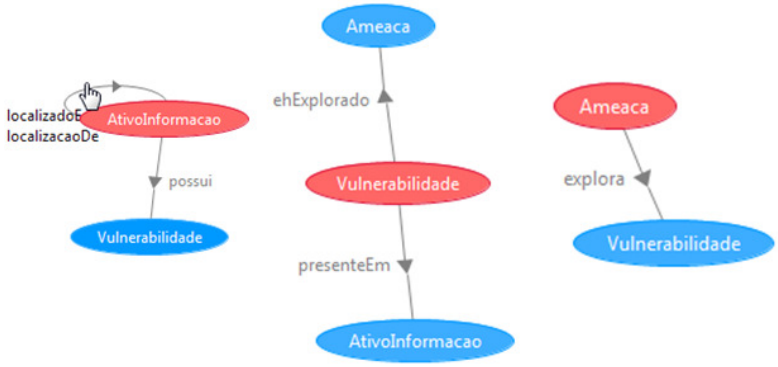

Figura 2. Visualização dos relacionamentos

Com base no exposto acima, foram criados os seguinte relacionamentos na ferramenta NeOn: *localizadoEm, localizaçãoDe, possui, presenteEm, ehExplorado, explora*. A Figura 2 apresenta a relação entre as classes de indivíduos com base nos relacionamentos criados, onde se pode observar que um ativo de informação está localizado em outro ativo de informação ao mesmo tempo em que também é a localização de outro ativo de informação. Uma vulnerabilidade está presente em um

ativo de informação e é explorada por uma ameaça. E uma ameaça possui o relacionamento de explorar um ativo de informação.

Além das definições de relacionamentos, também foram modeladas restrições entre as classes da ontologia. Por exemplo, o relacionamento *localizadoEm* não pode ocorrer entre as classes Hardware e Software, pois não faz sentido um hardware estar localizado em um software. O mesmo ocorre entre as classes Ambiente e Hardware, por exemplo. Existem restrições também entre o relacionamento de Ameaça com Vulnerabilidade, por exemplo, uma vulnerabilidade física não pode ser explorada por uma ameaça da classe *Malware*, bem como uma vulnerabilidade lógica não pode ser explorada por uma ameaça da classe EventoNatural.

Após a definição das classes, dos relacionamentos e das restrições, a ontologia foi populada com vários indivíduos representativos das classes. Conforme apresenta a Figura 3, foram criados indivíduos para todas as subclasses de ativos de informação, ameaças e vulnerabilidades previamente modeladas.

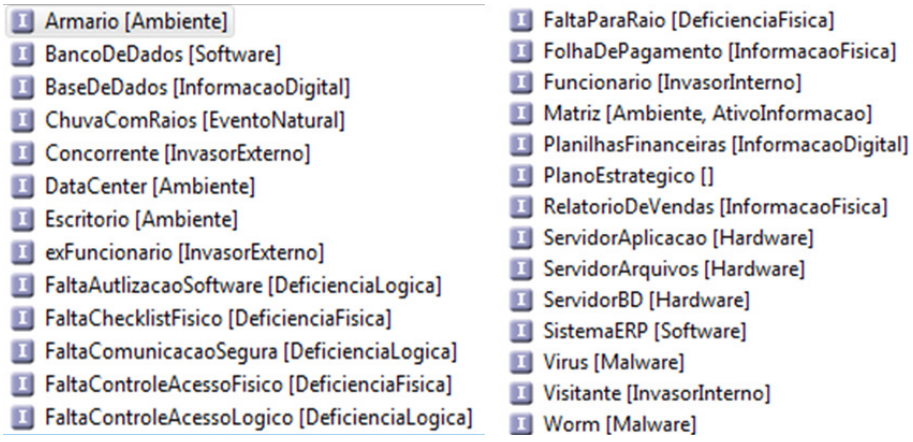

Figura 3. Criação dos indivíduos da ontologia

Uma vez que os indivíduos estão cadastrados, estes já recebem influência dos relacionamentos e das restrições modeladas na ontologia, ou seja, a ontologia já fornece semântica para os indivíduos, a partir dos relacionamentos das classes e das restrições.

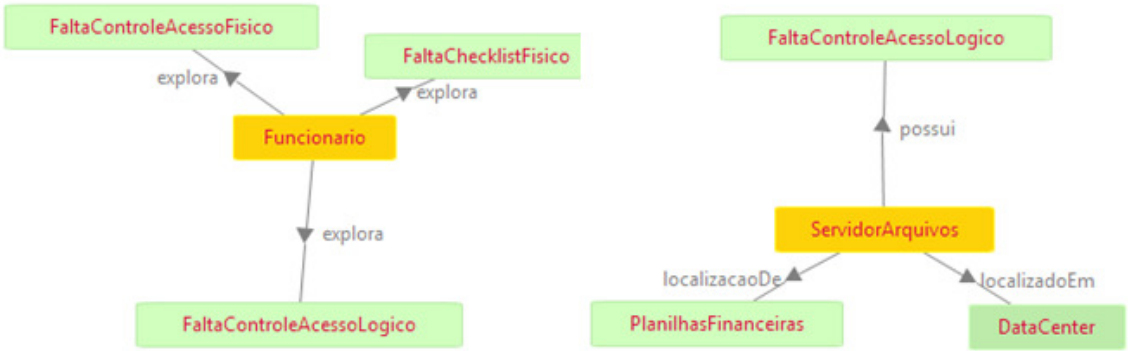

Figura 4. Visualização dos relacionamentos

A Figura 4 (extraída diretamente da ferramenta NeOn) apresenta um exemplo de relacionamento de indivíduos inferido através da ontologia modelada. Através da ontologia e dos indivíduos cadastrados pode-se concluir que o funcionário é uma

ameaça no cenário de segurança da informação que explora as vulnerabilidades de falta de controle de acesso físico, falta de *checklist* físico e falta de controle de acesso lógico. Da mesma forma o servidor de arquivos é um ativo de informação que possui a vulnerabilidade de falta de controle de acesso lógico, também é a localização de outro ativo de informação que é a planilha financeira e está localizado no Data Center da empresa.

Esta seção apresentou a modelagem de uma ontologia para gestão de segurança da informação e a criação de indivíduos representativos para as classes desta ontologia.

4. Resultados e Discussão

Com uma ontologia para gestão de segurança da informação desenvolvida sob a metodologia NeOn de desenvolvimento de ontologias é possível aplicar qualquer ferramenta de inferência compatível com o padrão OWL. Outra vantagem é a possibilidade de integração desta ontologia com outras ontologias de outros domínios, por exemplo: esta ontologia que se fundamenta na ISO 27001 poderia ser integrada com outras ontologias desenvolvidas com base em outras normas da ISO (ex. ISO 9001), formando assim uma ontologia maior e integrada.

Para demonstrar os resultados e possibilidade a partir do desenvolvimento de uma ontologia para segurança da informação, fez-se uso de uma ferramenta compatível com o NeOn para inferência e consulta sobre ontologias no padrão OWL – o SPARQL.

A partir do SPARQL é possível realizar questionamentos complexos sobre a ontologia e seus indivíduos. A Figura 5 demonstra a execução de uma consulta SPARQL sobre a ontologia modelada e os indivíduos criados neste projeto.

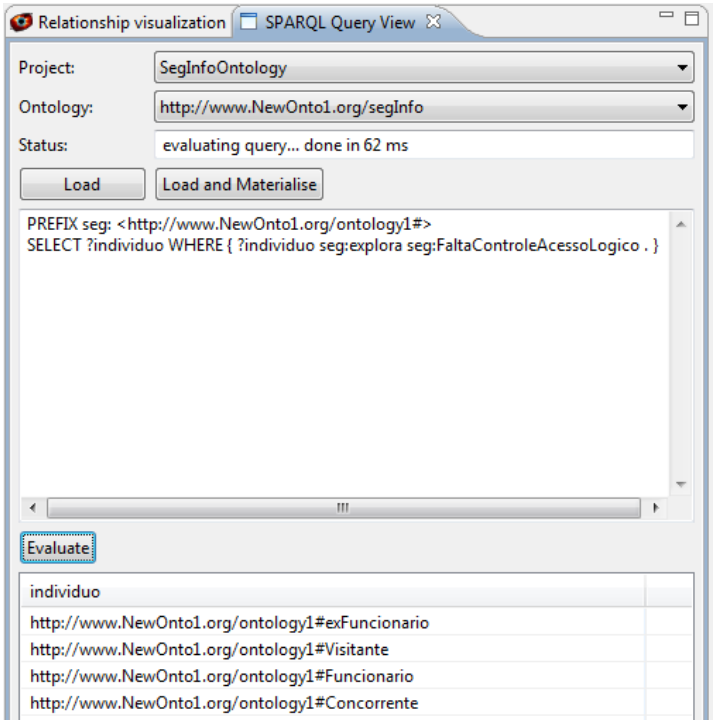

Figura 5. Visualização dos relacionamentos

Foi questionado à ontologia quais são os indivíduos que exploram a falta de controle de acesso lógico, como resultado o SPARQL apresentou os indivíduos: ex-funcionário, visitante, funcionário e concorrente. A partir deste exemplo seria possível realizar qualquer tipo de questionamento com base nas classes e relacionamentos modelados.

O uso do SPARQL neste exemplo foi feito através de um console de consulta, porém no desdobramento deste projeto o SPARQL e outras ferramentas de inferência sobre ontologia poderão ser utilizados em forma de biblioteca dentro de um ambiente mais amplo de suporte à gestão do conhecimento de segurança da informação em empresas de consultoria de gestão de segurança da informação.

5. Conclusão

Este artigo apresentou a concepção, modelagem, população e teste de uma ontologia para gestão de segurança da informação, desenvolvida sob a metodologia NeOn de desenvolvimento de ontologias. Esta ontologia servirá de base para o desenvolvimento de uma ferramenta de suporte à gestão do conhecimento em organizações de consultoria de segurança da informação. A ontologia de gestão de segurança da informação auxiliará na aquisição, representação, armazenamento e compartilhamento de conhecimento relacionado com gestão de segurança da informação.

Como extensão deste trabalho sugere-se: a ampliação da ontologia, com a adição de classes para o suporte de controles de segurança da informação tecnológicos e administrativos; a aplicação desta ontologia em uma arquitetura para gestão do conhecimento em organizações de consultoria de gestão de segurança da informação.

References

ABNT NBR ISO/IEC 27001:2006, Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos.

ABNT NBR ISO/IEC 27002:2007, Tecnologia da informação - Técnicas de segurança - Código de pratica para a gestão de segurança da informação.

Campos, André L. N. Sistemas de Segurança da Informação: controlando os riscos. São Paulo: Visual Books, 2007.

Suárez-Figueroa, M. C.. K. Dellschaft, E. Montiel-Ponsoda, B. Villazón-Terrazas, Z. Yufei, G. Aguado de Cea, A. García, M. Fernández-López, A. Gómez-Pérez, M. Espinoza, M. Sabou. NeOn Deliverable D5.4.1. NeOn Methodology for Building Contextualized Ontology Networks. NeOn Project. http://www.neon-project.org. February 2008.

Kim, Sung-kwan. Silvana Trimi: IT for KM in the management consulting industry. J. Knowledge Management 11(3): 145-155 (2007)

Bachimont, Bruno. Antoine Isaac. Raphaël Troncy, Semantic Commitment for Designing Ontologies: A Proposal, Proceedings of the 13th International Conference on Knowledge Engineering and Knowledge Management. Ontologies and the Semantic Web, p.114-121, October 01-04, 2002.