InfoSecRM: Uma Ontologia para Auxiliar na Compreensão do Domínio de Gestão de Riscos de Segurança da Informação

Éder S. Gualberto[1], **Rafael T. de Sousa Jr**[1], **Flávio E. G. de Deus**[1], **Cláudio G. Duque**[2]

[1]Departamento de engenharia Elétrica – Universidade de Brasília (UnB)
Caixa Postal 4.386 – 70.910-900 – Brasília – DF – Brazil

[2]Faculdade de Ciência da Informação (FCI)
Universidade de Brasília (UnB) – Brasília – DF – Brazil

{edergual}@gmail.com, {rafael,flavioelias,klauss}@unb.br

Abstract. *This paper presents a domain ontology for information security risks management (ISRM), called InfoSecRM. Its conceptualization presents the concepts involved in a ISRM process, as well as their relationships amid this type of process activities. This representation specifies the architecture of related information, and helps the learning and understanding of the ISRM domain.*

1. Introdução

A implementação e manutenção de um processo de Gestão de Riscos de Segurança da Informação (GRSI) opera sobre uma grande quantidade de conceitos, tais como ativos, vulnerabilidades, riscos, incidentes etc. Conceitos estes que manifestam muitos relacionamentos entre si, tornando seu entendimento e aprendizado, por parte dos colaboradores e intervenientes (*stakeholders*), fator crítico à aquisição e ao compartilhamento de conhecimento relativo à segurança da informação em organizações.

O conhecimento em segurança vale-se de variadas fontes de informação e estruturar estas informações de modo a permitir o processamento, o compartilhamento e a utilização deste conhecimento é uma tarefa complexa, define [Schumacher 2003]. Assim, paradigmas que promovam a automação deste processo e possibilitem a definição da arquitetura da informação relacionada são representações extremamente úteis às modelagens deste tipo domínio.

Neste cenário, a utilização de ontologias permite, ao mesmo tempo, a representação das relações semânticas entre os conceitos envolvidos em um processo de GRSI, e a criação e estruturação de uma base de conhecimento a respeito da segurança da informação em uma organização. Além disso, auxilia o aprendizado e a comunicação entre os envolvidos em um processo de GRSI, visto apresentar as definições dos termos utilizados, as atividades intrínsecas a este tipo de processo e a sua sequência.

Diante o exposto, foi desenvolvida uma ontologia para gestão de riscos de segurança da informação denominada *InfoSecRM*. Essa caracteriza-se como uma ontologia de domínio, visto que dispõe dos conceitos básicos relacionados ao domínio de GRSI e de Gestão de Segurança da Informação (GSI). Por meio da utilização dessa, pode-se documentar e operar o processo de GRSI e subsidiar decisões gerenciais relacionadas à GSI.

2. A Ontologia desenvolvida

A *InfoSecRM* tem como ideia base o conceito de risco associado a um cenário de incidentes de segurança da informação, que é uma descrição fictícia de um potencial conjunto de incidentes a que uma organização pode estar sujeita. A este cenário são associados os ativos, as vulnerabilidades inerentes a esses, as ameaças que podem explorar essas últimas, os controles, assim como incidentes que já tenham ocorrido neste contexto, consequências, probabilidade de ocorrência e medida de impacto. Com base nestes é estimado o nível do risco associado. A representação do núcleo da *InfoSecRM* pode ser observada na figura 1.

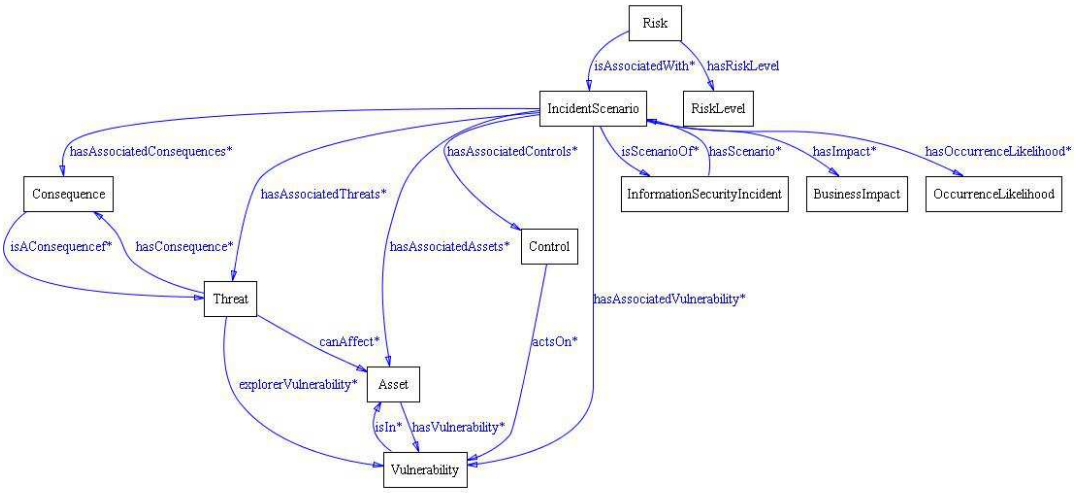

Figure 1. Idéia Central da *InfoSecRM*

Para a elaboração da *InfoSecRM* foram utilizadas as perspectivas de três abordagens: a metodologia *methontology*, como o processo que define o arcabouço das atividades a serem realizadas, o método 101, para definir o "como fazer" de algumas destas atividades e a metodologia proposta por Fox e Gruninger no projeto TOVE, de onde foram utilizadas as idéias de cenários de motivação e de questões de competência.

Esta ontologia foi modelada em OWL, por meio do framework Protégé 3.4.7. Para sua verificação foi utilizada a máquina de inferência Pellet 1.5.2 e alguns critérios como acurácia, usabillidade, expressividade etc, além de compará-la a outras ontologias cujo domínio modelado é relacionado à segurança da informação. Já para as atividades de validação, a *InfoSecRM* foi utilizada na introdução de um processo de gestão de riscos de segurança da informação em uma organização com vistas a responder às questões de competência definidas para esta ontologia por meio das instanciações realizadas, e também foi comparada com documentos de referência sobre o domínio de GRSI.

References

Schumacher, M. (2003). *Secuurity Engineering with patterns - Origins, Theoretical and New Applications*, chapter Toward security core ontology, pages 87–96. Simpreger Verlag.