Proposição de uma Ontologia de Apoio à 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 - Brasil

[2]Faculdade de Ciência da Informação (FCI)
Universidade de Brasília (UnB) - Brasília - DF - Brasil

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

Abstract. *Information Security Risk Management processes consume information from various sources such as data related to assets and their vulnerabilities, system logs, management decisions. Resources that can assist in handling information in this complex context are real and relevant needs to be considered. In this article, an ontology is presented as a proposal to formalize, share, manipulate and process concepts and information related to the field of information security risk management. It discusses the main concepts of risk management and of the information security management, the developing process of proposed ontology, and its evaluation process, where the stipulated requirements and parameters were validated and verified. The most important contributions of this work are also presented in the last section.*

Resumo. *Processos de Gerenciamento de Riscos de Segurança da informação utilizam informações de fontes variadas, tais como dados sobre ativos e suas vulnerabilidades, logs de sistemas, decisões gerenciais etc. Recursos que possam auxiliar na manipulação de informações neste complexo contexto são necessidades reais e relevantes a serem consideradas. Neste artigo, é apresentada uma ontologia como proposta de representação para formalizar, compartilhar, manipular e processar conceitos e informações relacionadas ao domínio de gestão de riscos de segurança da informação. São discutidos os principais conceitos relacionados à gestão de riscos e à gestão de segurança da informação, o processo de desenvolvimento da ontologia proposta, e também o seu processo de avaliação, onde foram validados e verificados os requisitos e parâmetros estipulados. São apresentadas ainda, na última seção, as contribuições mais relevantes desse trabalho.*

1. Introdução

Promover e gerir a segurança da informação tem sido um grande desafio para as organizações, vista a alta criticidade deste tipo de ativo e dos ativos de suporte relacionados, e consideradas as constantes ameaças que os cercam [Sêmola 2003]. Diante dessa situação, considerando que tal desafio vai além da resolução de questões inerentemente relacionadas à tecnologia da informação (TI), as ações gerenciais que

compreendem processos, tecnologias e pessoas são importantíssimas para a efetividade da segurança da informação.

Assim, tem sido bastante discutida a questão da gestão da segurança da informação (GSI) em ambientes corporativos, públicos e privados. Em especial, tais discussões levaram à publicação das normas da família ISO 27000 que constituem, conforme [ISO 2009], o estado da arte internacional nesta área. Essas normas definem um modelo para sistemas de gerenciamento de segurança da informação (SGSI) com vistas a proteger os ativos de informação e permitir à organização continuar realizando sua missão.

No âmbito de um SGSI, um processo de gestão de riscos de segurança da informação (GRSI) caracteriza-se como um dos elementos mais importantes para a efetividade do próprio SGSI, visto que tal processo permite a identificação das necessidades e prioridades de segurança da informação da organização, com base em análises e avaliações que se guiam pelos critérios e requisitos definidos pela própria organização. Segundo [ABNT 2008], administrar os riscos de segurança da informação aos quais se está sujeito contribui de maneira significativa para o sucesso da organização e de seus negócios.

Ocorre, no entanto, que a operacionalização e manutenção de um processo de GRSI opera sobre uma grande quantidade de conceitos. 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 da organização. Além disso, a GRSI atua sobre uma grande quantidade de informações e a utilização de mecanismos que permitam a sua manipulação de forma eficiente e eficaz são extremamente relevantes [AS/NZS 2004].

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 [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 de 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 de GSI, e a criação e estruturação de uma base de conhecimento a respeito da segurança da informação na organização, além de possibilitar a comunicação e interoperabilidade entre agentes de software e agentes humanos sobre uma mesma representação de dados.

Diante o exposto, foi desenvolvida uma ontologia para gestão de riscos de segurança da informação denominada InfoSecRM. Esta caracteriza-se como uma ontologia de domínio, visto que dispõe dos conceitos básicos relacionados ao domínio de GRSI e de GSI, em particular obedecendo ao disposto nas normas supracitadas, além de outras regulamentações nacionais. Por meio de sua utilização, pode-se documentar e operar o processo de GRSI e subsidiar decisões gerenciais relacionadas à GSI. Neste

artigo, apresenta-se tal ontologia, estendendo e aprofundando o conteúdo de [Gualberto et al 2012a].

2. Segurança da Informação

A segurança da informação diz respeito à proteção da informação, de modo a preservar determinadas propriedades (confidencialidade[1], integridade[2] e disponibilidade[3]) e aspectos (autenticidade[4], legalidade[5] etc) da informação, evitando que as vulnerabilidades dos ativos relacionados sejam exploradas por ameaças e possam trazer consequências para os negócios de uma organização.

O termo **Ativos**, como definido em [ABNT 2006], refere-se a "qualquer coisa que tenha valor para a organização". Os ativos possuem fragilidades, denominadas **vulnerabilidades** [ISO 2009], que podem ser exploradas por **ameaças** (que segundo [ISO 2009], são as causas potenciais de incidentes de segurança da informação), causando danos e impactos à organização e seus sistemas. **Impactos**, conforme explicitado em [ISO 2009], "dizem respeito a mudanças adversas nos níveis dos objetivos de negócio alcançados".

A definição de impacto auxilia a diferenciar o conceito de evento de segurança da informação daquele de incidente de segurança da informação, pois conforme exposto em [ABNT 2005], um **evento de segurança da informação** caracteriza-se por uma "ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação", ao passo que **incidente de segurança da informação** diz respeito apenas aquele(s) evento(s) que tenham grande probabilidade de impactar o negócio e a segurança da informação de uma organização.

Quanto ao termo **Risco**, conforme se depreende de [AS/NZS 2004], refere-se a um evento hipotético (com probabilidade de ocorrência não nula), cuja concretização pode afetar de forma positiva ou negativa uma organização. Já o risco de segurança da informação é mais específico, consoante ao exposto em [ABNT 2008] e [Alberts and Audrey 2002], e considera apenas a probabilidade de impacto negativo, assim pode-se determinar **risco de segurança da informação** como a combinação da probabilidade de uma determinada ameaça explorar uma vulnerabilidade de um ativo (evento) com o impacto de suas potenciais consequências.

---

[1] Propriedade que a informação apresenta, de estar disponível apenas para àqueles que estão autorizados a obtê-la [ABNT 2006].

[2] Propriedade que a informação apresenta, de estar completa e fiel ao estado original [ABNT 2006].

[3] Propriedade que a informação apresenta, de estar disponível e utilizável numa eventual requisição de uma entidade autorizada [ABNT 2006].

[4] Aspecto comprovante de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade [GSI-PR 2008].

[5] Aspecto comprovante do valor legal (onde todos os ativos relacionados estão de acordo com os requisitos de conformidade) que uma informação pode ter em um processo de comunicação [Sêmola 2003].

No processo de gestão de riscos de segurança da informação, conforme proposto em [ABNT 2008], o risco de segurança da informação é conceituado por meio da definição de **cenários de incidentes de segurança da informação**, que são descrições de um potencial conjunto de incidentes a que uma organização pode estar sujeita. A este cenário são associados os ativos, as vulnerabilidades a eles inerentes, as ameaças que podem explorar tais vulnerabilidades, os controles (existentes e potenciais), assim como as consequências, probabilidade de ocorrência e medida de impacto.

A preservação das propriedades e dos aspectos da informação anteriormente mencionados depende do estabelecimento de uma ação gerencial explícita, que é a chamada GSI. A GSI tem como objetivo principal fazer com que as ações e decisões relativas à segurança da informação estejam alinhadas aos objetivos e estratégias do negócio da organização e que estas sejam promovidas por meio de um conjunto de controles (tais como procedimentos, estruturas organizacionais, políticas etc) com objetivos específicos. Um Sistema de Gestão de Segurança da Informação visa justamente permitir que a organização que o implementa alcance seus objetivos relativos à segurança da informação. A própria norma ABNT NBR ISO/IEC 27001, [ABNT 2006] versa que um Sistema de Gestão de Segurança da Informação baseia-se numa análise de riscos para estabelecer, programar, operar, monitorizar, rever, manter e melhorar a Segurança da Informação.

Já um processo de Gestão de Riscos de Segurança da Informação pode ser aplicado nas mais variadas esferas de uma organização, abrangendo essa organização como um todo, ou somente atuando em uma de suas divisões, ou apenas em um projeto específico. Em qualquer situação, esse ambiente onde o processo será desenvolvido deve ser bem definido, de modo a permitir as decisões específicas e corretas que impliquem em ações eficientes. Ou seja, o escopo de aplicação da gestão de riscos deve ser transparente e delineado. A definição de onde ou em que será implantada a gerência de riscos de segurança da informação é um dos itens mais importantes no que tange ao princípio de estabelecer uma base para um processo de gestão contínuo, conforme definido em [Alberts and Audrey 2002].

Em [ABNT 2008] é indicado um processo de GRSI, cujas principais atividades são: definição de contexto, apreciação de riscos (que prevê subatividades de identificação, estimativa e avaliação de riscos), tratamento de riscos e aceitação de riscos, além de uma comunicação efetiva entre as partes envolvidas, e um monitoramento e revisões contínuas ao longo do processo. Cada uma destas atividades deve ter suas entradas, ações e resultados registrados, pois esses registros são parte dos requisitos para uma GSI efetiva e consequentemente para uma boa governança de TI e para uma boa governança corporativa.

3. Ontologias

Descrever e representar conceitos e propriedades relevantes em um domínio específico é uma das principais funcionalidades de uma ontologia. Por meio deste tipo de representação, facilita-se o compartilhamento de conhecimento em um domínio, visto estabelecer-se sobre um vocabulário, além de permitir aquisição de novos conhecimentos com base em axiomas e regras definidas para a ontologia proposta.

Segundo [Guarino 1998], uma ontologia pode ser entendida como um artefato de engenharia, baseado em vocabulário formal específico, cujo uso permite a descrição de um domínio que se quer representar. Consoante a esta definição, uma formalização do conceito de ontologia pertinente é a proposta por [Stumme and Maedche 2003] e complementada por [Ehrig et al. 2004], representada pela 10-upla abaixo:

$$O := (C, T, \leq_C, \leq_T, R, A, \sigma_A, \sigma_R, \leq_R, \leq_A). \quad (1)$$

Na equação 1 acima, C refere-se ao conjunto de conceitos, R ao conjunto de relacionamentos e T ao conjunto de tipos de dados, sendo estes três conjuntos disjuntos. Os conceitos estão organizados segundo uma hierarquia $\leq_C$, as relações segundo uma hierarquia $\leq_R$ e os atributos segundo uma hierarquia $\leq_T$. Os relacionamentos têm assinatura σ_R: R $\rightarrow$ C x C, ou seja, se dão entre elementos da classe de conceitos. A é o conjunto dos atributos de tipos de dados associados a conceitos, com assinatura σ_A : A $\rightarrow$ C x T e organizados segundo a taxonomia $\leq_A$.

Assim, com base na explicação da equação 1, explicitam-se alguns entendimentos: o conjunto de conceitos são representações de objetos (entidades) do mundo real, que possuem propriedades relativas a outros objetos (propriedades relacionais ou relacionamentos) e propriedades descritivas (atributos com valores de determinados tipos de dados) que os descrevem (representando estados, eventos ou processos destas entidades). As instâncias de um conceito representam um objeto particular e a sua descrição (atributos e relacionamentos) dentro de um conjunto de objetos do mesmo tipo. O conjunto de instanciações associado à ontologia constitui uma base de conhecimento relativa aquele domínio.

Em [Fensel 2000], aponta-se que a definição de ontologia dada em [Gruber 1995] melhor representa a essência de uma ontologia como sistema de organização do conhecimento, que privilegia a conexão de conceitos e a representação dos relacionamentos complexos entre eles, conforme conceitua [Brascher and Carlan 2010]. Conforme explicitado em [Borst 1997], em uma extensão do definido em [Gruber 1995], uma ontologia diz respeito a uma "especificação formal e explícita de uma conceitualização compartilhada". **Conceitualização** é concebida aqui como um modelo abstrato que representa um determinado contexto no mundo, por meio dos conceitos mais relevantes a este domínio. Enquanto **compartilhada** caracteriza esta conceitualização com um conhecimento consensual, comum ao grupo envolvido no domínio especificado. Ao passo que **explícita** refere-se à característica de os objetos representados pelo conjunto de conceitos, assim como os relacionamentos e atributos a eles associados, estarem definidos de forma conhecida e comum ao grupo envolvido. E **formal** ao fato de a especificação ser declarativamente definida (por meio de lógica descritiva, por exemplo) e assim ser compreensível a agentes e sistemas.

Tanto no que tange a domínios relacionados à segurança da informação [Donner 2003] [R Andersson and Hallberg 2003] [Raskin et al. 2001], quanto na sua utilização de

uma forma geral [Noy and McGuinners 2001], podem-se citar os seguintes principais benefícios da utilização de ontologias:

- A formalização de um fenômeno, por meio da organização e sistematização de conceitos relacionados ao domínio em questão, seus relacionamentos e atributos, propiciando um compartilhamento do entendimento comum a pessoas e agentes de software;
- Uma compreensão mais clara do domínio modelado, devido à definição formal e explícita, além da aquisição de conhecimento (geração automática) possibilitada por meio das regras de inferência e axiomas;
- A manutenção do conhecimento no modelo obtido (seja pela reuso ou extensão) também é facilitada pela especificação formal e explícita empregada nas ontologias;
- O compartilhamento de conhecimento e informações também é favorecido, devido ao domínio alvo ser modelado com base em uma conceitualização compartilhada e permitir a instanciação dos conceitos e propriedades especificados;
- A utilização de ontologias permite separar conhecimento de um domínio do conhecimento operacional, assim uma mesma ontologia pode ser utilizada em variadas aplicações, além de admitir a interoperabilidade entre elas.

4. O processo de desenvolvimento da InfoSecRM

Para a elaboração da InfoSecRM foram utilizadas as perspectivas de três abordagens: a **metodologia methontology** [Fernandez-Lopez et al. 1997] como o processo que define o arcabouço das atividades a serem realizadas, **o método 101** [Noy and McGuinners 2001] para definir o "como fazer" de algumas destas atividades (na conceituação por exemplo, onde os passos são bem detalhados) e a **metodologia proposta por Fox e Gruninger no projeto TOVE** [Grüninger and Fox 1995], com a utilização das idéias de cenários de motivação e de questões de competência por ela proposta. Para a implementação da InfoSecRM foi utilizada a linguagem OWL-DL e a composição se fez com o *framework* Protégé 3.4.

A InfoSecRM teve como idéia base o conceito de risco associado a um cenário de incidente de segurança da informação, conforme analisado em [Gualberto et al 2012b]. Assim, um **risco** está associado a um **cenário de incidente de segurança da informação**, que é uma descrição 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 tais vulnerabilidades, os **controles**, assim como as **consequências**, **probabilidade de ocorrência** e medida de **impacto**. Com base nestes elementos é estimado o **nível de risco**. A representação do núcleo da InfoSecRM descrito pode ser observada na figura 1.

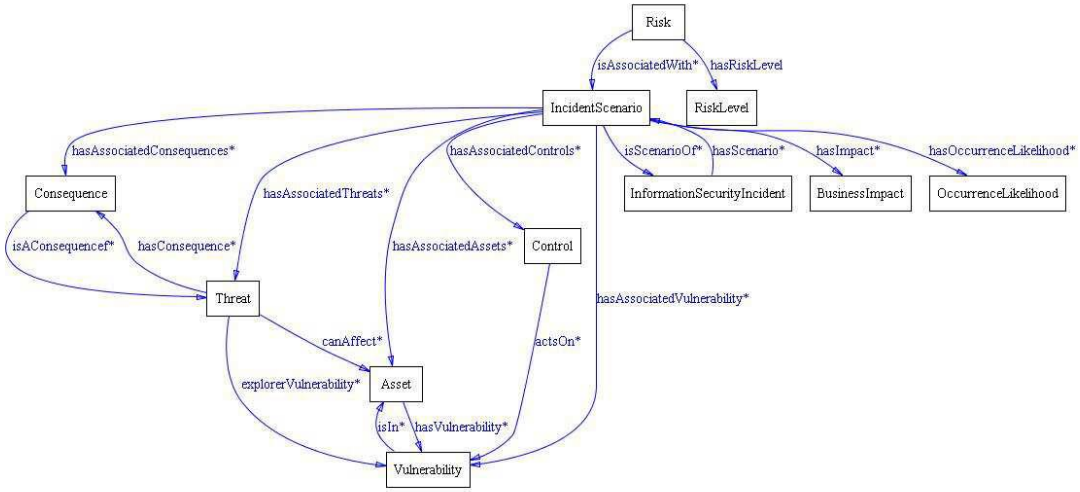

Figura 1. Representação do núcleo de conceitos e relacionamentos que formam a base da InfoSecRM

Além da idéia central, outro elemento importante na concepção da InfoSecRM, foi o processo de gestão de riscos de segurança da informação definido na norma ISO 27005 [ABNT 2008].

Com base nas duas ideias citadas, na composição da InfoSecRM foram elencados os termos mais importantes a serem representados pela ontologia, definidas classes e suas hierarquias, e as propriedades de cada classe e suas restrições. A InfoSecRM possui 88 classes (82 classes nomeadas e 6 definidas), 68 relacionamentos e 9 atributos, encontrando-se completa em [Gualberto 2011]. Seguem as definições relativas a um exemplo de classe desta ontologia:

Classe Risk - Representam os riscos (foco do processo de gestão de riscos) associados a indivíduos da classe "**IncidentScenario**". Possui as seguintes propriedades:

isARiskAssociatedWith - identifica o cenário de incidente de segurança da informação associado ao risco.

hasRiskLevel - identifica o nível de risco de um indivíduo da classe **Risk**, atribuído quando da atividade de estimativa de risco (pode ser alto, médio ou baixo).

hasPriority - identifica a prioridade dada a um risco, na atividade de avaliação de risco, para que este seja tratado (pode ser uma prioridade alta, média ou baixa).

hasTreatment - indica o tratamento dado a um risco quando da atividade de tratamento de risco.

hasRiskAcceptanceStatus - representa se um risco foi ou não aceito durante a atividade de aceitação de risco.

hasResponsible - associa a responsabilidade do risco a um colaborador ou fornecedor.

hasDescription - apresenta uma frase (string) de descrição do risco.

Figura 2. Hierarquia da classe Risk

A classe **Risk** (classe nomeada) possui a hierarquia representada na figura 2. As suas subclasses (classes definidas) identificam quais atividades já foram realizadas sobre um determinado risco. Por exemplo: a classe **TreatedRisk** possui as condições necessárias e suficientes, indicadas na equação 2:

$$\text{TreatedRisk} \equiv \text{Risk} \cap \forall\, \text{isAssociatedWith.}\, \text{IncidentScenario} \cap \exists\, \text{hasLevel.}\, \text{RiskLevel} \cap \exists\, \text{hasPriority.}\, \text{RiskPriority} \cap \exists\, \text{hasTreatment.}\, \text{Treatment} \quad (2)$$

Denota-se, das condições expressas acima, que os riscos inferidos como indivíduos da classe **TreatedRisk** já passaram pela atividade de tratamento de risco. Desta forma, são riscos que estão associados a um cenário (identificaram-se os ativos, vulnerabilidades, ameaças, controles e incidentes relacionados), tiveram o seu nível de criticidade estimado (com base em seu impacto e probabilidade de ocorrência), foram priorizados para tratamento segundo os objetivos de negócio da organização e tiveram os controles, previstos como tratamento, implementados.

5. Avaliação da InfoSecRM e análise dos benefícios de sua utilização

O processo de avaliação de ontologias consiste em atividades de verificação e de validação, que, segundo define [Obrst et al. 2007], referem-se respectivamente a: avaliar se a ontologia implementa os requisitos corretamente (avaliar quanto à forma) e avaliar se a ontologia modela de fato o domínio alvo (avaliar se a ontologia correta foi construída).

As atividades de verificação foram guiadas pela abordagem indicada em [Lozano-Tello and Gomez-Perez 2004] e em [Sirin et al. 2007], onde é proposto avaliar ontologias segundo um conjunto de critérios pré-definidos, e também pela abordagem proposta em [Maedche et al. 2002] e discutida em [Obrst et al. 2007], que indica a comparação entre ontologias de um domínio relacionado como forma de verificação (com base em uma análise quantitativa).

Considerando o exposto por [Vrandecic 2009], onde é afirmado que a validação requer uma colaboração entre os profissionais responsáveis pelo desenvolvimento da ontologia e os profissionais do domínio mapeado, para as atividades de validação, adotou-se a abordagem proposta em [Obrst et al. 2007], que avalia a capacidade da ontologia criada de responder a algumas das questões de competência. Nesse sentido, a ontologia foi utilizada nas atividades de um processo de GRSI em uma gerência operacional do departamento de TI de uma organização governamental, com vistas a

instanciar suas classes e relacionamentos, e assim, permitir as pesquisas pelas questões de competência. Esta abordagem é similar à adotada em [Silva et al. 2011], porém foi realizada com dados reais de um processo de GRSI de uma organização

Para a validação, ainda foi adotada a abordagem denominada *Data-driven*, proposta em [Brewster et al. 2004], que consiste em comparar a ontologia desenvolvida com um conjunto de dados ou documentos sobre o domínio modelado.

5.1. Verificação

A ontologia foi verificada quanto aos critérios: acurácia, adaptabilidade, transparência, granularidade, adequação organizacional, classificação, consistência, expressividade, precisão, satisfação, usabilidade e utilidade, propostos em [Vrandecic 2009] e [Lozano-Tello and Gomez-Perez 2004].

Para a verificação do critério expressividade, por exemplo, observou-se que a InfoSecRM possui interseção e disjunção entre classes, quantificação universal e existencial, negação, regras transitivas, inversas e funcionais, hierarquia de classes e de propriedades, definição de classes por enumeração, restrições de cardinalidade e utilização de tipos de dados. Em outras palavras, identificou-se, por meio da máquina de inferência Pellet 1.5.2, que a ontologia verificada possui expressividade SHOIN(D) que é a maior expressividade que a OWL-DL pode proporcionar.

Já com relação à verificação por comparação entre ontologias, considerando a abordagem, proposta por [Maedche et al. 2002], de comparar a InfoSecRM com outras ontologias, adotou-se como métrica a indicada em [Ning and Shihan 2006], que é realizada com base nos indicadores: Quantidade de classes nomeadas, Média de propriedades do tipo objeto (relacionamentos), Nível da ontologia quanto a hierarquias - relacionamento *is-a* (é um) e Classe com maior número de relacionamentos *is-a* da ontologia.

Foram utilizadas para este comparativo as ontologias propostas em [Martimiano 2006] e [Azevedo 2008], respectivamente, OntoSec e CoreSec. A OntoSec representa parte do domínio de segurança da informação, porém seu foco é na gestão de incidentes de segurança da informação. Já a CoreSec tem como domínio a segurança da informação, propondo uma representação com conceitos de alto nível, facilitando a sua utilização em avaliação de riscos e gestão de segurança da informação.

Por meio destes indicadores, pode-se observar que a estrutura da InfoSecRM assemelha-se mais à CoreSec do que à OntoSec, o número de classes nomeadas (respectivamente, 82, 89 e 59) e os conceitos representados indicam esta semelhança. No entanto, é importante frisar que, enquanto o domínio modelado pela InfoSecRM refere-se apenas à gestão de riscos de segurança da informação, o domínio modelado pela CoreSec tinha como objetivo abranger toda a gestão de segurança da informação.

Observou-se também que a InfoSecRM apresenta maior média de propriedades do tipo objeto por classes nomeadas (0.82, frente a 0.47 da OntoSec e 0.45 da CoreSec). Este número é um indicador de que a conceitualização proposta por esta ontologia representa bem as relações semânticas entre os conceitos do domínio representado, como pode ser observado nas propriedades que relacionam os conceitos: ativo,

vulnerabilidade, ameaças, consequência, incidente, cenário de incidente e riscos, por exemplo.

Com relação à quantidade de níveis e à classe com maior número de relacionamentos *is-a*, verificou-se que ontologia proposta neste trabalho possui seis níveis em sua hierarquia, enquanto a OntoSec e a CoreSec possuem 5. Neste sexto nível, estão representadas as subclasses das classes **Datamedium**, **Network** e **Host**, que são subclasses da classe **Hardware**, que é uma subclasse da classe **PhysicalAsset**, que por sua vez é uma subclasse da classe **Asset**. A classe **Asset** é a classe na InfoSecRM que possui mais subclasses, ou seja, mais relacionamentos do tipo **is-a**. Este grau de especialização desta classe justifica-se em parte devido ao fato de o inventário de ativos e a sua valoração para uma organização serem atividades críticas ao processo de GRSI.

Uma constatação importante de ser citada é que na OntoSec e na CoreSec a maioria dos relacionamentos se concentra na classe que representa os incidentes de segurança (**Securityincident**). Na InfoSecRM, esta tendência de centralização em incidentes de segurança da informação também é perceptível, no entanto a dinâmica empregada considera estes incidentes como pertencentes a cenários de incidentes e estes por sua vez como associados a riscos, daí a maioria dos relacionamentos da ontologia descrita neste trabalho concentrar-se nas classes **Risk** e **IncidentScenario**.

5.2. Validação

A InfoSecRM foi utilizada nas atividades de um processo, ainda de nível inicial, de GRSI em uma gerência operacional do departamento de TI de uma organização governamental. Esta organização ainda não possui política de segurança da informação ou outros documentos que possam balizar as ações deste processo em todas as suas áreas e com a participação de todos os colaboradores. Assim, o processo limitou-se à área que gerencia a infraestrutura de TI e às questões onde os colaboradores participantes tinham autonomia e autoridade para fazê-lo.

Os conceitos e relacionamentos representados na InfoSecRM foram instanciados representando as ações do processo de GRSI com as limitações descritas acima. Por meio de consultas na linguagem de consulta SPARQL às instanciações realizadas, pôde-se responder às questões de competência definidas durante o desenvolvimento desta ontologia. Apresenta-se aqui um exemplo de questão de competência:

Quais são os riscos de nível alto a que uma organização está sujeita?

```
SELECT ?Risk
WHERE {?Risk:hasRiskLevel:High_Risk}
```

As respostas a questões de competência, como a citada, permitem, não apenas verificar que os conceitos necessários à representação do domínio de GRSI foram modelados pela ontologia, como também auxiliar os usuários da InfoSecRM a buscar informações nas bases de conhecimento geradas sobre a estrutura que ela representa. Assim, foi possível observar que a utilização da InfoSecRm permitiu auxiliar na implementação da GRSI, ao armazenar as informações e indicar as atividades e escopo deste processo, apresentando-se como uma estrutura padronizada por meio da qual se

pode operar sobre os conceitos de segurança da informação relacionados à gestão de riscos e permitir o compartilhamento das informações relacionadas.

A ontologia desenvolvida ainda auxiliou no aprendizado, por alguns colaboradores, dos conceitos envolvidos em um processo de gestão de riscos de segurança da informação. A ontologia permite uma representação intuitiva dos conceitos do domínio de GRSI, suas respectivas propriedades e atributos, além de incluir pequenas descrições para cada um destes elementos representados. Este tipo de conceitualização, juntamente com os *plug-ins* de visualização utilizados, torna a percepção do domínio modelado mais clara.

Durante as atividades de validação, a InfoSecRM foi ainda comparada com documentos sobre o domínio modelado. Para esta abordagem de validação foram utilizadas as normas ABNT 27002 [ABNT 2005], ABNT 27001 [ABNT 2006] e ABNT 27005 [ABNT 2008]. Estas normas foram utilizadas como os documentos sobre o domínio representado por se tratarem de integrantes da família de normas ISO 27000, corpo normativo que se destina a auxiliar organizações a implementar e operar um sistema de gerenciamento de segurança da informação (SGSI). Como já exposto, um processo de GRSI é um fator crítico a um SGSI, pois por meio do GRSI pode-se implementar e monitorar os controles de segurança da informação de uma organização, além de promover ações que os melhorem continuamente.

Por meio da comparação da InfoSecRM às normas citadas, pode-se notar que os aspectos mais relevantes do contexto de gerenciamento de riscos de segurança da informação foram representados, principalmente no que tange ao conceito de riscos e cenários de incidentes de segurança da informação, e ao processo de GRSI em si.

6. Conclusões e Trabalhos Futuros

A InfoSecRM, ontologia de domínio desenvolvida neste trabalho, apresenta uma conceitualização do conhecimento relacionado à GRSI. Por meio dessa ontologia, podem ser instanciados os conceitos envolvidos (como riscos, cenários de incidentes, impacto etc) e também as atividades propostas para um processo de gestão de riscos (como análise de riscos, avaliação de riscos, tratamento de riscos etc). As representações dessa ontologia auxiliam não só a tomada de decisões neste domínio, como a própria implementação e continuidade deste processo. Assim, as principais contribuições deste trabalho foram:

- Uma conceitualização formal, desenvolvida e avaliada segundo um processo bem definido, que apresenta uma representação das informações relacionadas à gestão de riscos de segurança da informação. Por meio desta representação, promove-se a aquisição e o compartilhamento de informações e conhecimento neste domínio;
- Promoção do processo de GRSI em organizações por meio da utilização da InfoSecRM, que como visto pode contribuir na implementação de uma gestão de riscos e na tomada de decisões, e ser utilizada na criação e estruturação de uma base de conhecimento de riscos de segurança da informação;
- Reuso de Conhecimento e informações, visto que a ontologia desenvolvida pode ser utilizada em processos de GRSI de organizações, em treinamentos de

colaboradores em GRSI, para o desenvolvimento de novas ontologias (de aplicação, por exemplo) e como base para aplicações.

Diante das contribuições e resultados obtidos, identificaram-se as seguintes oportunidades de trabalhos futuros:

- Desenvolver um sistema que permita auxiliar em processos de GRSI, indicando os conceitos trabalhados e as informações necessárias nos moldes do realizado neste trabalho, tendo como base a InfoSecRM. Por meio deste, fornecer uma interface ainda mais intuitiva e com uma estrutura mais robusta para usuários menos familiarizados com conceitos de segurança da informação e com a utilização de ontologias.
- Expandir os conceitos da InfoSecRM de forma a representar também o indicado nas outras normas da família ISO 27000.
- Desenvolver ontologias de aplicação, a partir da InfoSecRM, para cenários mais específicos relacionados à GRSI, como por exemplo, as atividades de inventário de ativos.

7. Referências

ABNT (2005). *ABNT NBR ISO/IEC 27002 - Código de prática para a gestão de segurança da informação*. Associação Brasileira de Normas Técnicas, Rio de Janeiro.

ABNT (2006). *ABNT NBR ISO/IEC 27001 - Sistemas de gestão de segurança da informação - requisitos*. Associação Brasileira de Normas Técnicas, Rio de Janeiro.

ABNT (2008). *ABNT NBR ISO/IEC 27005 - Gestão de riscos de segurança da informação*. Associação Brasileira de Normas Técnicas, Rio de Janeiro.

Alberts, C.; Audrey, D. (2002). *Managing Information Security Risks: The OCTAVE Approach*. Addison Wesley.

Andersson, R.; Hunstad, A.; Hallberg, J. (2003). *Evaluation of the Security of Components in Distributed Information Systems*. Swedish Defence Research Agency, Linkoeping. Command and Control Systems.

AS/NZS (2004). *AS/NZS 4360:2004 - Risk Management*. Australian/New Zealand Standard, Autralia: GPO Box 5420, Sydney / New Zealand: Private Bag 2439,Wellington 6020.

Azevedo, R. R. (2008). *Coresec: Uma ontologia para o domínio de segurança da informação*. Master's thesis, Universidade Federal de Pernambuco, Recife.

Borst, W. (1997). *Construction of Engineering Ontologies*. PhD thesis, University of Tweente, Enschede, NL–Centre for Telematica and Information Technology.

Brascher, M.; Carlan, E. (2010). *Passeios no Bosque da Informação: Estudos sobre Representação e Organização da Informação e do Conhecimento*, chapter Sistemas de organização do conhecimento: antigas e novas linguagens, pages 147–176. IBICT, Brasília.

Brewster, C.; Alani, H.; Dasmahapatra, S.; Wilks, Y. (2004). *Data-driven ontology evaluation*. In Proceedings of the Language Resources and Evaluation Conference (LREC 2004), pages 164–168, Lisbon, Portugal. European Language Resources Association.

Donner, M. (2003). *Toward a security ontology*. IEEE Security and Privacy magazine, 1(3):6–7.

Ehrig, M.; Haase, P.; Hefke, M.; Stojanovic, N. (2004). *Similarity for ontologies - a comprehensive framework.* FZI Research Center for Information Technologies at the University of Karlsruhe.

Fensel, D. (2000). *Ontologies: Silver Bullet for Knowledge Management and Eletronic Commerce*. Springer.

Fernandez-Lopez, M.; Gomez-Perez, A.; Juristo, N. (1997). *Methontology: from ontological art towards ontological engineering.* In Proceedings of the AAAI97 Spring Symposium, pages 33–40, Stanford, USA.

Gualberto, E. S. (2011). InfoSecRM: Uma Ontologia para Gestão de Riscos de Segurança da Informação. Dissertação de Mestrado em Engenharia Elétrica, Universidade de Brasília.

Gualberto, E. S.; Sousa Jr, R. T.; Deus, F. E. G.; Duque, C. G. (2012a). InfoSecRM: Uma Abordagem Ontológica para a Gestão de Riscos de Segurança da Informação. In: Anais do VIII Simpósio Brasileiro de Sistemas de Informação - SBSI 2012. Porto Alegre: Sociedade Brasileira de Computação, 2012. v. 13. p. 1-12.

Gualberto, E. S.; Sousa Jr, R. T.; Deus, F. E. G.; Duque, C. G. (2012b). InfoSecRM: Uma Ontologia para Auxiliar na Compreensão do Domínio de Gestão de Riscos de Segurança da Informação. In: Anais do Computer on the Beach 2012. São José: UNIVALI CTT. Mar, 2012. v. 1. p. 129-130.

Gruber, T. R. (1995). *Toward principles for the design of ontologies used for knowledge sharing.* International Journal of Human-Computer Studies, 43(5/6):907–928.

Grüninger, M.; Fox, M. (1995). *Methodology for the Design and Evaluation of Ontologies.* In IJCAI'95, Workshop on Basic Ontological Issues in Knowledge Sharing, April 13, 1995.

GSI-PR (2008). *Gabinete de Segurança Institucional da Presidência da República. Norma Complementar GSI nº 2, de 14 de outubro de 2008*. Gabinete de Segurança Institucional da Presidência da República.

Guarino, N. (1998). *Formal ontologies and information systems*. First International Conference (FOIS), 1:3–15.

ISO (2009). *ISO/IEC 27000 - Information Security Management Systems*. International Organization for Standardization.

Lozano-Tello, A.; Gomez-Perez, A. (2004). *ONTOMETRIC: A method to choose the appropriate ontology.* Journal of Database Management, 15(2):1–18.

Maedche, A.; Maedche, E.; Staab, S. (2002). *Measuring similarity between ontologies.* In Proceedings of the European Conference on Knowledge Acquisition and Management (EKAW, pages 251–263. Springer.

Martimiano, L. A. F. (2006). *Sobre a estruturação de informação de segurança computacional: o uso de ontologia*. Tese de Doutorado, Instituto de Ciências Matemáticas e de Computação - ICMC, Universidade de São Paulo - USP, São Carlos.

Ning, H.; Shihan, D. (2006). *Structure-based ontology evaluation.* In e-Business Engineering, 2006. ICEBE '06. IEEE International Conference on, pages 132–137.

Noy, N. F.; McGuinners, D. L. (2001). *Ontology development 101: A guide to create your first ontology*. Knowledge Systems Laboratory - Stanford University.

Obrst, L.; Ceusters,W.; Mani, I.; Ray, S.; Smith, B. (2007). The evaluation of ontologies. In Baker, C. J. and Cheung, K.-H., editors, Revolutionizing Knowledge Discovery in the Life Sciences, chapter 7, pages 139–158. Springer.

Raskin, V.; Hempelmann, C. F.; Triezenberg, K. E.; Nirenburg, S. (2001). Ontology in information security: a useful theoretical foundation and methology tool. In Proceedings of the workshop and New Security Paradigms.

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

Silva, P. F.; Otte, H.; Todesco, J. L.; Gauthier, F. A. O. (2011). *Uma ontologia para gestão de segurança da informacão.* Ontobras/Most - Internacional Workshop on Metamodels Ontologies and Semantic Technologies.

Sirin, E.; Parsia, B.; Grau, B.; Kalyanpur, A.; Katz, Y. (2007). *Pellet: A practical OWL-DL reasoner*. Web Semantics: Science, Services and Agents on the World Wide Web, 5(2):51–53.

Sêmola, M. (2003). *Gestão da segurança da informação: visão executiva da segurança da informação*. Elsevier, Rio de Janeiro.

Stumme, G.; Maedche, A. (2003). *Fca-merge: Bottom-up merging of ontologies.* 17th Intl. Conf. on Artificial Inelligence (IJCAI '01, 19:225–230.

Vrandecic, D. (2009). *Ontology Evaluation*, pages 293–313. International Handbook on Information Systems. Springer.