UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Lorena Melo Guimarães Rosa

Utilização de Elementos Ontológicos para Representação de Conhecimento em Segurança da Informação

Uberlândia, Brasil

2017

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Lorena Melo Guimarães Rosa

Utilização de Elementos Ontológicos para Representação de Conhecimento em Segurança da Informação

Dissertação de Mestrado apresentada à Faculdade de Computação da Universidade Federal de Uberlândia, Minas Gerais, como requisito parcial exigido à obtenção do grau de Mestre em Ciência da Computação.

Orientador: Prof. Pedro Frosi Rosa, PhD

Coorientador: Prof. Flávio de Oliveira Silva, PhD

Universidade Federal de Uberlândia – UFU

Faculdade de Computação

Programa de Pós Graduação em Ciência da Computação

Mestrado em Ciência da Computação

Uberlândia, Brasil

2017

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

R788u
2017

Rosa, Lorena Melo Guimarães, 1985-
Utilização de elementos ontológicos para representação de conhecimento em segurança da informação / Lorena Melo Guimarães Rosa. - 2017.
68 f. : il.

Orientador: Pedro Frosi Rosa.
Coorientador: Flávio de Oliveira Silva.
Dissertação (mestrado) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Ciência da Computação.
Disponível em: http://dx.doi.org/10.14393/ufu.di.2018.1119
Inclui bibliografia.

1. Computação - Teses. 2. Ontologias (Recuperação da informação) - Teses. 3. Sistemas de recuperação da informação - Teses. 4. Sistemas operacionais distribuídos (Computadores) - Teses. I. Rosa, Pedro Frosi. II. Silva, Flávio de Oliveira, 1970- III. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Ciência da Computação. IV. Título.

CDU: 681.3

Maria Salete de Freitas Pinheiro – CRB6/1262

UNIVERSIDADE FEDERAL DE UBERLANDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Os abaixo assinados, por meio deste, certificam que leram e recomendam para a Faculdade de Computação a aceitação da dissertação intitulada **"Utilização de Elementos Ontológicos para Representação de Conhecimento em Segurança da Informação"** por **Lorena Melo Guimarães Rosa** como parte dos requisitos exigidos para a obtenção do título de **Mestre em Ciência da Computação**.

Uberlândia, 22 de fevereiro, 2017

Orientador: Prof. Dr. Pedro Frosi Rosa
Universidade Federal de Uberlândia

Banca Examinadora: Prof. Dr. João Henrique de Souza Pereira
Universidade Federal de Uberlândia

Prof. Dr. José Gonçalves Pereira Filho
Universidade Federal do Espírito Santo

Dedico esta dissertação ao meu esposo Fábio e meu filho Gabriel, pelo apoio incondicional e constante incentivo que sempre me impulsiona em direção às vitórias dos meus desafios.

Agradecimentos

Agradeço primeiramente à Deus, que através de seu amor incondicional me deu forças todos os dias de minha vida para nunca desistir e me mostrou, mais uma vez, que tudo posso naquele que me fortalece. Ao meu querido esposo Fábio, pessoa essencial na minha vida. Sempre ao meu lado, em todos os momentos dessa caminhada, me fazendo acreditar que eu podia chegar ao fim. Devido ao seu apoio, companheirismo, paciência e amizade foi possível a concretização deste trabalho. Obrigada por ter feito do meu sonho o nosso sonho! Ao meu filho Gabriel, minha razão de viver. Mesmo tão pequeno se mostrou muito compreensivo nos momentos que estive ausente para me dedicar a este trabalho. Com você aprendi que sou mais forte e que posso alcançar todos os meus objetivos. Muito obrigada pelo privilégio de ser sua mãe. Aos meus pais Maristela e Sérgio(*in memoriam*), por me terem dado educação, valores e por me terem ensinado o caminho dos estudos. Ao Professor William Chaves de Souza Carvalho meu infinito agradecimento. Muito mais que um professor se mostrou um grande amigo nessa jornada, sempre disposto a me ajudar com seu conhecimento indiscutível, mas sobretudo com palavras de incentivo e de ânimo para que eu nunca desistisse. Obrigada por tudo! Ao meu orientador, Professor Dr. Pedro Frosi Rosa, minha gratidão por todo conhecimento compartilhado comigo neste tempo, foi um aprendizado que levarei por toda minha vida. E também, obrigada por sempre ter acreditado e confiado em mim ao longo desta jornada. Você se tornou uma referência para mim, não somente de um excelente profissional, mas também referência de uma pessoa íntegra, generosa e sempre disposta a ajudar o próximo. Ao meu coorientador Professor Dr. Flávio de Oliveira Silva agradeço pela confiança, pela oportunidade de trabalhar ao seu lado e por me ajudar na condução deste trabalho. Ao CNPq meu muito obrigada pelo apoio financeiro que possibilitou a minha dedicação exclusiva neste trabalho. À todos os professores do mestrado que de alguma forma contribuíram para minha formação, obrigada!

Resumo

O tema de segurança da informação é algo fundamental nos dias atuais visto que na sociedade em que vivemos temos uma grande variedade de conteúdos que estão disponibilizados em vários meios e estão sujeitos a diversas formas de ameaças, físicas ou virtuais, que podem comprometer a segurança das informações e das pessoas as que pertencem. Além disso, a necessidade de atenção ao tema de segurança da informação está cada vez maior diante da quantidade de dados que as pessoas manipulam diariamente. Aliado a isso, outro grande desafio das organizações é a dificuldade de interligar seus sistemas e o compartilhamento de conhecimento entre os diversos elementos de sua infraestrutura de rede e de negócios. Isso faz com que o esforço necessário para realizar alterações em regras de negócio sejam aumentados, o que se reflete também no aumento do custo e/ou prazo de execução. Esta pesquisa apresenta uma abordagem de representação de conhecimento sobre casos de incidentes de ameaça interna baseada em ontologia para apoiar a criação, o compartilhamento e a análise de indicadores deste tema. A ontologia foi submetida aos motores de inferência Pellet e Racer que analisaram sua consistência interna, consistência dos conceitos, hierarquia das classes e existência de classes equivalentes. A pesquisa também identificou pontos de atenção que pesquisadores podem usar como guia para a criação de ontologias.

Palavras-chave: Ontologia, Segurança da Informação, Motor de Inferência.

Resumo

The issue of information security is fundamental in today's society we live in have a wide variety of content that is available in various media and are subject to various forms of threats, physical or virtual, which can compromise the security of the information and of the people to which they belong. In addition, the need for attention to the issue of information security is increasingly the amount of data that people manipulate daily. Ally to, another major challenge for organizations is the difficulty of interconnecting their systems and sharing of knowledge among the various elements of its infrastructure of network and business. This causes the effort required to make changes to rules increase, which is also reflected in the increase in cost and / or of execution. This research presents a knowledge representation approach on ontology-based internal threat incidents to support the creation, the sharing and analysis of indicators of this theme. The ontology was submitted to the Pellet and Racer inference engines that analyzed their internal consistency, consistency of concepts, class hierarchy and existence of equivalent classes. The search points of attention that researchers can use as a creation of ontologies.

Key Words: Ontology, Information Security, Inference Engine.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ACK	*Acknowledgement*
AF	*Addess Family*
ALM	*Application Layer Multicast*
API	*Application Programming Interface*
ASCII	*American Standard Code for Information Interchange*
CERT	*Computer Emergency Response Team*
CORBA	*Common Object Requester Broker Architecture*
DARPA	*Defense Advanced Research Projects Agency*
DIG	*DL Implementation Group*
DL	*Description Logic*
DS Field	*Differenciated Services Field*
DSCP	*Differentiated Services Code Point*
DTS	*Domain Title Service*
DTS	*Domain Title Service*
DTSA	*Domain Title Service Agent*
DTSA	*Domain Title Service Agent*
DTSCP	*Domain Title Service Control Protocol*
EJB	*Enterprise JavaBeans*
EPUSP	Escola Politécnica da Universidade de São Paulo
ETArch	*Entity Title Archicture*
ETCP	*Entity Title Control Protocol*
FACOM	Faculdade de Computação
HDTV	*High Definition Television*

HTTP	*Hypertext Transfer Protocol*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IEEE	*Institute of Electrical and Electronics Engineers*
IHL	*IP Header Length*
IMS	*IP Multimedia Subsystems*
IoT	*Internet of Things*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
JEE	*Java Enterprise Edition*
JMS	*Java Message Services*
MDTSA	*Master Domain Title Service Agent*
NE	*Network Element*
NGN	*Next Generation Networks*
OIL	*Ontology Inference Layer*
OSI	*Open Systems Interconnection*
OWL	*Ontology Modeling Language*
PoA	*Point of Attachment*
PSM	*Problem Solving Methods*
QoE	*Quality of Experience*
QoS	*Quality of Service*
RDF	*Resource Description Framework*
RFC	*Request for Comments*
RTP	*Real-time Transport Protocol*
RTSP	*Real Time Streaming Protocol*
SDN	*Software Defined Networking*
SIP	*Session Initiation Protocol*

SOA	*Service Oriented Architecture*
SOAP	*Simple Object Access Protocol*
SP	*Service Provider*
TCP	*Transmission Control Protocol*
TI	Tecnologia da Informação
ToS	*Type of Service*
UDP	*User Datagram Protocol*
UFU	Universidade Federal de Uberlândia
UML	*Unified Modeling Language*
USP	Universidade de São Paulo
VoD	*Video on Demand*
VoIP	*Voice over IP*
W3C	*World Wide Web Consortium*
XML	*eXtensible Markup Language*

Sumário

1 Introdução

Na sociedade informatizada que vivemos, o papel da segurança da informação é fundamental. É cada vez mais comum nesta sociedade o uso de sistemas informatizados para realização das mais variadas atividades com a integração de suas bases de dados por meio de redes. Porém, esta variedade de conteúdos está sujeita a diversas formas de ameaças, físicas ou virtuais, que comprometem a segurança das informações e das pessoas as que pertencem.

A necessidade por segurança da informação está cada vez maior diante da quantidade de dados que as pessoas manipulam diariamente. Isto implica no aumento da demanda por segurança digital em função das preocupações a respeito do uso não autorizado de informações sigilosas e das respectivas consequências. O uso de senhas é a maneira mais comum de controlar o acesso a informações privilegiadas e envolve dois mundos muito diferentes, o mundo tecnológico e o humano, porém a interação entre eles tem gerado inúmeros problemas (SILVA; STEIN, 2007).

Como os requisitos para uma senha segura esbarram nas capacidades cognitivas de seus usuários, dando origem a inúmeros problemas, as organizações contam com suas políticas de segurança da informação para abranger de forma adequada as mais variadas áreas, incluindo os recursos de infra-estrutura, logística, computacionais e humanos.

O estudo da ameaça interna apresenta alguns dos desafios mais complexos na segurança da informação (CAPPELLI; MOORE; TRZECIAK, 2012). As organizações começaram a reconhecer a importância de detectar e prevenir ameaças internas, mas há uma surpreendente falta de padrões dentro do domínio de Segurança da Informação para auxiliar no desenvolvimento, descrição, teste e compartilhamento de informações (WEST-BROWN et al., 2003). Para muitas organizações, o estabelecimento de um programa de prevenção de ameaças internas e o início de busca por atividades de potenciais intrusos mal-intencionados são uma nova atividade empresarial uma vez que o uso intensivo das redes de comunicação é um caminho de mão única(ALLEN, 2001).

Aliado a isso, outro grande desafio das organizações é a dificuldade de interligar seus sistemas, uma vez que a arquitetura e tecnologias utilizadas na sua implementação fazem com que o custo de alteração para interconexão seja impeditivo, em termos de custo ou prazo de execução (CHOI; SONG; HAN, 2006; CHEN; CHEN; SU, 2009). Além disto, a heterogeneidade dos elementos dos sistemas de informação dificulta a resposta das empresas aos requisitos de mercado, impactando negativamente sua competitividade (PEREIRA et al., 2011), (PEREIRA; KOFUJI; ROSA, 2009).

Quando se fala nos componentes de um sistema de informação é comum que eles tenham

certo grau de distribuição e isso implica a existência de alguns requisitos para a comunicação entre as suas diversas partes. No entanto, estes componentes também podem possuir níveis variáveis de autonomia, comunicando entre si de maneiras diferentes (De Nicola; MISSIKOFF; NAVIGLI, 2009).

A falta de padronização do processo de desenvolvimento e de troca de informações é um fator crítico que leva as organizações a vivenciarem dificuldades crescentes para integrar as diversas fontes de informações (CHEN; CHEN; CHU, 2009; FARQUHAR; FIKES; RICE, 1997; FIKES; FARQUHAR, 1999). Neste sentido, o *Institute of Electrical and Electronics Engineers* (IEEE) considera um sistema ou produto interoperável quando este pode interagir com outros sistemas ou produtos, sem que haja algum esforço especial por parte de um cliente (XU; WU; CAI, 2011).

Este conceito indica que a interoperabilidade pode ser obtida com sucesso quando padrões e políticas são definidos para que haja a troca integrada de informações, a qual é uma exigência da crescente disponibilidade de tecnologias de informação e comunicação, como, por exemplo, as redes, os computadores, a web, aplicativos móveis, sistemas embarcados (FU; COHN, 2008). Ainda em 1991, o DARPA *Knowledge Sharing Effort* (NECHES et al., 1991) identificou este problema, vislumbrou uma nova maneira de construir sistemas interoperáveis e fez a seguinte proposta:

> Atualmente, a construção de sistemas baseados em conhecimento geralmente implica a construção de novas bases de conhecimento a partir do zero. No entanto, isso pode ser feito de outra maneira, por meio da montagem de componentes reutilizáveis. Assim, os desenvolvedores de sistemas só precisariam se preocupar com a criação do conhecimento e com a execução das tarefas específicas do seu sistema. Dessa maneira, este novo sistema poderia interoperar com sistemas pré-existentes, utilizando-os para executar alguns dos seus propósitos. Desta forma, conhecimento declarativo, técnicas de resolução de problemas e outros serviços seriam compartilhados entre os sistemas. Esta abordagem facilitaria a construção de sistemas maiores, melhores e mais baratos (CORCHO; FERNANDEZ-LOPEZ; GOMEZ-PEREZ, 2006).

Desde a ideia da DARPA, progressos consideráveis foram feitos no desenvolvimento das bases conceituais para construir tecnologias que permitam reusar e compartilhar componentes de conhecimento, o que tem sido satisfatoriamente obtido com o uso de ontologias (SCHOLAR et al., 2006). Ontologias e métodos de resolução de problemas (PSMs) foram criados para permitir compartilhar e reusar conhecimento e padrões de raciocínio em diversos domínios (BUCCELLA; CECHICH; BRISABOA, 2003; CHANDY, 1985). Nesta evolução, o fato mais importante foi o surgimento da web semântica. De acordo com (BERNERS-LEE; FISCHETTI, 1999), a Web Semântica é

uma extensão da Web atual em que é atribuído um significado bem definido para a informação, permitindo que computadores e pessoas trabalhem melhor cooperativamente (ABDOLI; KAHANI, 2009). Esta cooperação pode ser conseguida por meio do uso de componentes de conhecimento compartilhados (DING; FENSEL, 2001); o que fez com que ontologias e PSMs se tornassem instrumentos fundamentais para o desenvolvimento da Web Semântica; sendo que seu poder de representatividade já foi usado, inclusive, para criar uma ontologia de *malwares* baseada em *fuzzy logic* (TAFAZZOLI; SADJADI, 2008).

Assim, a criação de *frameworks*, soluções, padrões e processos que visam aumentar a interoperabilidade dos sistemas passou a ser fundamental para a prestação de serviços eficientes e de qualidade, em que seja possível integrar sistemas e compartilhar informações(FLAHIVE et al., 2005; GREGOR et al., 2016).

Uma abordagem para a criação de tecnologias interoperáveis se baseia no uso de ontologias. Por exemplo, nas áreas de Medicina e Biomedicina as ontologias têm sido usadas para estruturar o grande volume de dados gerados. Estas áreas têm investido em pesquisa sobre a interoperabilidade utilizando ontologia (FARINELLI; ALMEIDA, 2013). Neste sentido, a portaria 2.073 (SAúDE, 2011) recomenda o uso da ontologia para lidar com interoperabilidade entre Sistemas de Informação da área médica no Brasil.

A ontologia pode ajudar na interoperabilidade sobretudo graças à sua inerente heterogeneidade semântica (SUN, 2011). Mesmo que os sistemas de informação utilizem a mesma sintaxe, eles podem associar significados diferentes às coisas, o que impede a troca de informação. Com o uso de ontologias é possível especificar, sem ambiguidade, os vocabulários subjacentes dos sistemas de informação (FARINELLI; ALMEIDA, 2013).

1.1 Motivação

No escopo desta pesquisa, a motivação do desenvolvimento da ontologia de Ameaça Interna é apoiar a criação, o compartilhamento e a análise de indicadores de ameaça interna.

Este domínio de negócio foi escolhido como estudo de caso para desenvolvimento da ontologia porque a segurança da informação é uma preocupação inerente a todas organizações, seja qual for sua área de atuação final.

1.2 Objetivos

O trabalho tem como objetivo criar uma ontologia que represente e permita compartilhar um conjunto organizado de conhecimento sobre incidentes relacionados a segurança da informação e que possa ser utilizada como base para a criação e manutenção de sistemas

de informação que compartilhem indicadores de ameaças internas à segurança. A construção do modelo usa a metodologia SABIO (FALBO, 1997) juntamente com as ontologias fundacionais UFO (GUIZZARDI, 2005a) (GUIZZARDI; GUIZZARDI, 2008).

1.3 Estrutura do Documento

Este documento foi estruturado em cinco capítulos, estruturados como se segue. No primeiro capítulo são apresentados, na forma de introdução, o contexto e objetivo da pesquisa; o segundo capítulo apresenta trabalhos relacionados ao tema da pesquisa; o terceiro capítulo, por sua vez, é responsável por descrever trabalhos relacionados ao tema da pesquisa. Já o capítulo quatro descreve a metodologia e o desenvolvimento da ontologia de ameaça interna; e, por fim, no capítulo cinco são feitas as considerações finais, envolvendo os desafios da pesquisa e enumeração de trabalhos futuros.

2 Fundamentos e Conceitos

Este capítulo apresenta os fundamentos e conceitos essenciais à compreensão do trabalho. Nele são abordados tópicos referentes à Segurança da Informação, definição de ontologia, metodologia de desenvolvimento de ontologia, Ontologia Fundacional, além dos motores de inferência e do ambiente de criação de ontologias utilizado nesta pesquisa.

2.1 Segurança da Informação

A ampliação do uso dos sistemas informatizados em várias atividades e a integração destes sistemas e de suas bases de dados são fatos muito relevantes na sociedade. Porém, este grande volume de informações está sujeito a várias formas de ameaças, físicas ou virtuais, que comprometem sua segurança e das pessoas ou organizações a que pertencem. A tecnologia da informação se propõe a ser parte da solução deste problema, porém, não consegue resolvê-lo em sua totalidade. As organizações adotam políticas de segurança para preservar seus ativos (recursos materiais ou informações), que devem abranger as mais variadas áreas do contexto organizacional, passando pelos recursos computacionais, infra-estrutura e logística, além dos recursos humanos (SILVA; STEIN, 2007).

As políticas de segurança são apresentadas como códigos de conduta aos quais os usuários devem respeitar e seguir. Contudo, não se tem uma discussão adequada sobre o nível de receptividade das pessoas a estas políticas, nem se apresentam questões sobre o impacto, usualmente considerável, por elas causado sobre o ambiente e sobre o comportamento daqueles que as devem seguir.

O uso não autorizado de informações sigilosas e suas consequências têm contribuído para o aumento da demanda por segurança da informação. Este tema envolve a interação entre dois mundos bastante diferentes, e por vezes conflitantes, e que juntos geram muitos problemas: o mundo da tecnologia e o mundo dos seres humanos (SILVA; STEIN, 2007).

Pessoas sem as devidas autorizações que tentam burlar a segurança a uma informação de propriedade particular, por qualquer que seja a razão, são chamadas de *hackers*. Ataques de *hackers* têm acontecido com uma frequência cada vez maior a empresas particulares, departamentos governamentais ou até mesmo indivíduos.

A definição de Segurança da Informação pode ser representada como a proteção contra o uso ou acesso não autorizado à informação ou a proteção contra a negação do serviço a

usuários autorizados (SILVA; STEIN, 2007). A Segurança da Informação não é restrita a somente sistemas de computação e informações em formato eletrônico, mas sim a todos os aspectos de proteção da informação em qualquer formato. O nível de proteção à informação deve corresponder ao valor e aos prejuízos que poderiam decorrer do uso inadequado da mesma e deve envolver toda infraestrutura necessária, como processos, sistemas, serviços, tecnologias, e outros.

Apesar de não poder eliminar por inteiro o risco de uso inapropriado ou mal-intencionado de qualquer informação, muitos esforços já foram feitos no sentido de aprimorar os sistemas. A Segurança da Informação se tornou uma preocupação importante da sociedade moderna, pois todos têm o direito de esperar que seus dados privados sejam mantidos intactos e disponibilizados apenas a pessoas autorizadas.

A proliferação de meios de acesso à informação, com a contribuição significativa da internet, possibilitou formas fáceis e de rápido de acesso aos conteúdos, mas ao mesmo tempo expôs ainda mais a fragilidade e os riscos que os usuários e os sistemas estão sujeitos. Por exemplo, no Brasil, a iniciativa que teve como objetivo a inclusão digital e que foi iniciada pelo poder público por meio do Programa Sociedade da Informação, priorizava o tema da segurança para prestação de serviços ao governo. Também é observada a preocupação no desenvolvimento de sistemas seguros, como um item obrigatório, em outras áreas, como no comércio eletrônico e nas páginas de instituições financeiras por meio da internet (SILVA; STEIN, 2007).

Diante disto, a segurança se faz necessária nas arquiteturas e modelos da informação em todos os níveis. Contudo, observa-se um número crescente de ocorrências de incidentes relativos à segurança da informação, como fraudes digitais, furtos de senhas, vírus e outros meios de ameaças que têm se multiplicado consideravelmente. Devido a este cenário, a segurança da informação, em seu sentido mais abrangente, envolve requisitos voltados à garantia de origem, uso e trânsito da informação, buscando certificar todas as etapas do seu ciclo de vida. Estes objetivos podem ser resumidos na forma dos seguintes itens: confidencialidade; integridade; disponibilidade; e, autenticidade.

As organizações e indivíduos estão cada vez mais cientes do risco de ataque às suas informações e tem buscado alternativas para evitá-lo. Porém, mesmo assim ainda presenciamos noticiários com fatos de intrusos que tiveram acessos a dados sem autorização. Por exemplo, em novembro de 2005, um estagiário do INSS de São Paulo foi preso acusado de inserir dados falsos nos sistemas da previdência através do uso de senhas de colegas de trabalho (GloboOnline, 2005). Segundo a reportagem, em dois anos o estagiário acumulou 3 milhões de reais. Outro exemplo foi em 2004, onde um estudante foi preso devido acusação de invadir contas bancárias pessoais do Banco do Brasil, Bradesco, Caixa Econômica Federal e Itaú (FolhaOnline, 2004).

O comportamento humano desempenha um papel importante em incidentes de

Tabela 1 – Custo para correção de uma falha de Segurança

Estágio	Custo Relativo
Projeto	1.0
Implementação	6.5
Testes	15.0
Manutenção	100.0

segurança. Sistemas de segurança da informação são comparados a uma corrente com muitos elos representando os componentes envolvidos, como os equipamentos, software, protocolos de comunicação de dados e o usuário humano (sendo este considerado o elo mais fraco).

Não adianta as organizações investirem em firewalls, encriptação e dispositivos de acesso seguro se o elo mais fraco, que é o ser humano, não se desenvolver para ajudar nesta busca da segurança da informação. Porém, pouco tem sido feito para identificar os fatores que levam a comportamentos potencialmente inseguros e menos ainda para tentar resolver tais problemas.

Além disso, as organizações precisam entender que pensar em segurança durante a concepção de um software é melhor para todos. Além de ser mais barato implementar meios de segurança durante as fases iniciais de um sistema do que quando este sistema já se encontra em produção, pode-se evitar ataques que levam a perda de informações confidenciais. Isto pode ser visto na tabela 1 que apresenta o custo relativo para a correção de falhas de segurança em software, em cada etapa do processo de desenvolvimento. Observa-se que quanto mais tarde são encontradas as falhas de segurança maior é o custo para correção.

Enfim, com o crescimento dos incidentes relacionados à segurança da informação surge o alerta para a necessidade de fundamentos e ações para solucionar este problema, as quais vão além do campo da tecnologia. Esta é capaz de colaborar com soluções para alguns dos problemas, mas não todos. Não se conhece solução meramente tecnológica para problemas sociais. Sendo um conceito eminentemente social, a segurança da informação necessita de uma visão igualmente embasada em conceitos sociais, além dos tecnológicos, para sua correta cobertura. Um ponto essencial e que deve ser trabalhado é a analise dos papéis representados pelos usuários e suas interações diante dos sistemas de informação (SILVA; STEIN, 2007).

2.2 Ontologia: perspectiva filosófica e técnica

Embora ontologia tenha uma definição clara na filosofia, há uma confusão terminológica substancial nas diferentes áreas da ciência da computação sobre o que o termo

supostamente denota. Assim, é necessário esclarecer a terminologia e estabelecer a caracterização formal de como o termo é usado na ciência da computação; além de tratar sobre a relação entre a definição de ontologia e as noções de conceituação e linguagem. O dicionário Webster remete o termo ontologia a duas definições (COMPANY, 2014):

1. Um ramo da metafísica preocupado com a natureza e com as relações do ser; e,
2. Uma teoria particular sobre a natureza do ser ou dos tipos de coisas que tem existência.

O termo ontologia foi cunhado no século XVII, em paralelo pelos filósofos Rudolf Göckel em sua obra Philosophicum Lexicon e por Jacob Lorhard na sua *Ogdoas Scholastica* (GUIZZARDI, 2005b). Etimologicamente, *ont-* vem do particípio presente do verbo grego *einai* (ser) e da palavra *logos* (conhecimento). Daí, ontologia (ont- + logia) pode ser traduzida como o estudo da existência. O termo, no entanto, foi popularizado nos círculos filosóficos apenas no século XVIII com a publicação em 1730 da Philosophia Ontologia por Christian Wolff (GUIZZARDI, 2005b), (TOIT, 1974).

Desde a Idade Antiga, o homem já se preocupavam com a questão: "qual é a essência das coisas através das mudanças?" (SMITH, 2009). Muitas respostas diferentes para esta pergunta foram propostas por diversos filósofos gregos, tais como Parmênides de Eléia, o precursor da ontologia, e Aristóteles, autor de Metafísica, em que ele descreve ontologia como a ciência do ser enquanto ser, ou a essência de todas as coisas (SMITH, 2003; HACKING, 2007).

Em seu estudo sobre a essência das coisas, Aristóteles distingue diferentes modos de se estabelecer um sistema de categorias [1] para classificar qualquer coisa referente a qualquer coisa no mundo (SMITH, 2003). Por exemplo, quando se diz que "um computador está sobre a mesa" utiliza-se um modo diferente do (verbo) ser de quando se diz que "o computador é cinza". A primeira declaração é classificado dentro da categoria de lugar, enquanto a segunda pertence à categoria de qualidade (TOIT, 1974).

Nesta perspectiva, o objetivo da ontologia é estudar as características mais gerais da realidade e dos objetos reais (ATKIN, 2010), isto é, o estudo das características genéricas de cada modo de ser (GOMEZ-PREREZ, 2004). Ao contrário das várias disciplinas científicas específicas – física, química, biologia etc – (D'AQUIN; NOY, 2012; USCHOLD et al., 1998) que lidam apenas com as entidades que se enquadram dentro de seu respectivo domínio, a ontologia trata das relações entre as categorias (LAWSON, 2004). Isso inclui as relações que acontecem entre entidades pertencentes a domínios distintos da ciência, e também por entidades reconhecidas pelo senso comum (SMITH, 2003; MAEDCHE; STAAB, 2001).

[1] Substância, qualidade, quantidade, relação, ação, paixão, lugar e tempo.

> Ontologias visam desenvolver teorias que tratem, por exemplo, de persistência e mudança, identidade, classificação e instanciação, causalidade etc. Questões ontológicas incluem questões como: que tipos de entidades existem? O que diferencia os objetos de eventos e como eles estão relacionados? Quais são as propriedades de uma coisa e como elas se relacionam com a coisa em si? Qual é a essência de um objeto? A essência precede a existência? Um objeto é igual à soma de suas partes? (GRUNINGER; LEE, 2002; SMITH, 2003)

> Estas são questões gerais, porém factuais e fundamentais para a ciência, independentemente se o assunto for as propriedades dos átomos, órgãos humanos ou requisições de seguro, ou mesmo se o objetivo for desenvolver teorias de eventos físicos, mentais ou sociais[2] (CHRUDZIMSKI, 2002).

> Finalmente, na axiomatização de teorias científicas alguns dos seguintes conceitos ontológicos aparecem de forma explícita: parte; composição; sistema; relações; limite; causalidade; estado; evento; mudança; propriedade; direito; possibilidade; processo; espaço; e, tempo. No entanto, os axiomas específicos dessas teorias geralmente não dizem nada – ou muito pouco – sobre esses conceitos fundamentais e genéricos (GRUNINGER; LEE, 2002; SMITH, 2003; TOIT, 1974).

As ciências simplesmente os tomam emprestados e utilizam-nos num estado intuitivo, informal e pré-sistemático. Em outras palavras, apesar destes conceitos genéricos serem comuns a várias ciências, nenhuma disciplina científica única se dá ao trabalho de arregimentá-los num corpo único (ALLEN; MARCH, 2006). O mesmo acontece com a utilização destes conceitos em ciência da computação e, em particular, na modelagem conceitual.

> Conceitos como parte e todo, instanciação e classificação, atribuição e relações, causalidade, interação etc estão representados nas primitivas de várias linguagem de modelagem conceitual ou, no mínimo, são utilizados no discurso da literatura de ciência da computação. No entanto, há uma falta de suporte teórico na área para definir com precisão o significado desses conceitos (GRUNINGER; LEE, 2002; ALLEN; MARCH, 2006; TOIT, 1974).

No início do séc. XX, o filósofo Edmund Husserl cunhou o termo Ontologia Formal como uma analogia à Lógica Formal. A Lógica Formal lida com estruturas lógicas formais tais como verdade, validade e consistência, independentemente de sua veracidade; e, a Ontologia Formal lida com estruturas ontológicas como teoria das partes, teoria dos conjuntos, tipos e instanciação, identidade, dependência e unidade, ou seja, com os aspectos formais dos objetos independentemente da sua natureza particular (BEYER,

[2] Existem muitos princípios ontológicos que são utilizados na investigação científica, por exemplo, na seleção de conceitos e hipótese, na reconstrução axiomática de teorias científicas, na concepção de técnicas e na avaliação dos resultados científicos.

2013).

O desdobramento da ontologia formal como uma disciplina filosófica visa o desenvolvimento de um sistema de categorias gerais e os seus vínculos, e isso pode ser usado no desenvolvimento de teorias científicas e teorias da realidade baseada no senso comum de domínios específicos. Enquanto os cientistas lidam com questões específicas, o ontologista se ocupa com questões transversais a todos os domínios (CORCHO; FERNANDEZ-LOPEZ; GOMEZ-PEREZ, 2006).

A primeira ontologia desenvolvida para sistematizar a natureza do ser ou dos tipos de coisas que têm existência foi o conjunto de teorias da substância e Acidentes desenvolvida por Aristóteles nas suas obras Metafísica e Categorias. Desde então, teorias ontológicas foram desenvolvidas por diversos filósofos; e, além disso, ontologia filosófica é atualmente uma área ativa em filosofia.

Por fim, mais recentemente, diversos sistemas ontológicos foram construídos em projetos relacionados à ciência da computação e sob os auspícios de uma nova disciplina chamada Ontologia Aplicada (CORCHO; FERNANDEZ-LOPEZ; GOMEZ-PEREZ, 2006; CORAZZON, 2013). Esta pesquisa utiliza teorias ontológicas formais que podem ser desenvolvidas e aplicadas na solução de problemas nas áreas de informática e ciências da informação e, em particular, de modelagem conceitual.

Para responder à pergunta "o que é uma ontologia para um engenheiro?", é interessante supor que existam semelhanças entre a forma com que a realidade é percebida por pessoas e por computadores, e ambos podem ser estruturados em ontologias (GRUBER, 1993). De acordo com essa ideia, se um computador é exclusivamente dedicado a responder a perguntas sobre turismo, seu universo poderia ser estruturado por meio da classificação das viagens tais como viajar de trem, viagem de avião etc.

No entanto, para esta classificação ser realmente uma ontologia para o computador, ela deve ser capaz de raciocinar com base nela. Isso leva ao estabelecimento da primeira diferença importante entre uma ontologia a partir da perspectiva filosófica e a partir do ponto de vista da ciência da computação (KIM; MANLEY; YANG, 2006).

Do ponto de vista ciência da computação, as ontologias devem ser codificadas em uma linguagem interpretável pela máquina (STAAB et al., 2001; CORCHO; FERNANDEZ-LOPEZ; GOMEZ-PEREZ, 2006). Quando um engenheiro define o que é uma ontologia, ele muda a perspectiva da pessoa para o computador. Assim, se o computador não puder compreendê-la, ela não pode ser considerada uma ontologia.

Além disso, para um engenheiro, as ontologias geralmente são mais específicas do que para um filósofo. Finalmente, devido ao uso do termo ontologia em ciência da computação, sua definição neste contexto precisa levar em conta características de reutilização e compartilhamento, que não são essenciais em ontologias filosóficas. Em

suma, para um engenheiro (STAAB et al., 2001):

> Uma ontologia é uma especificação explícita e formal de uma conceitualização compartilhada. Conceituação refere-se a um modelo abstrato de algum fenômeno no mundo mediante a identificação dos conceitos relevantes de tal fenômeno. Explícita significa que o tipo de conceitos utilizados bem como as restrições à sua utilização são explicitamente definidos. Formal refere-se ao fato de que a ontologia deve ser interpretável pela máquina. Compartilhada reflete a noção de que uma ontologia captura conhecimento consensual, isto é, ele não é específico de um indivíduo, mas aceito por um grupo.

Em seu trabalho de 1991, Neches et alli (NECHES et al., 1991) deram outra definição, com foco na forma de uma ontologia:

> Uma ontologia define os termos básicos e relações que compõem o vocabulário de uma área temática, bem como as regras par a a combinação de termos e relações a fim de definir extensões para o vocabulário.

2.3 Componentes principais de uma ontologia

Existem diversos formalismos e linguagens de representação do conhecimento que podem ser utilizados para a formalização e implementação de ontologias. Cada um deles possui componentes diferentes que podem ser usados para estas funções. Todavia, eles compartilham o seguinte conjunto mínimo de componentes.

2.3.1 Classes

Classes representam conceitos, em sentido amplo. Por exemplo, no domínio de viagens, conceitos podem ser: locais (cidades, aldeias, praias etc); hospedagem (hotéis, albergues, pousadas, *camping* etc); e, meios de transporte (aviões, trens, carros, barcos, motos e navios). Numa ontologia, classes normalmente são organizados em taxonomias que permitem a utilização de mecanismos de herança.

Pode-se representar uma taxonomia de locais de entretenimento (teatro, cinema, concertos etc) ou pacotes de viagem (viagem econômica, viagens de negócios etc) No paradigma de representação do conhecimento baseado em quadros, também é possível definir metaclasses, que são classes cujas instâncias são classes. Metaclasses permitem a criação de diferentes gradações de significado, uma vez que é possível estabelecer diferentes camadas de classes na ontologia.

2.3.2 Relações

Relações representam um tipo de associação entre conceitos do domínio. Elas são formalmente definidas como qualquer subconjunto do produto cartesiano de n conjuntos, isto é, $R \subset C_1 \times C_2 \times \ldots \times C_n$. Ontologias geralmente contêm relações binárias. O primeiro argumento é conhecido como o domínio da relação e o segundo argumento é o seu contradomínio. Por exemplo, na relação binária **localChegada**, o conceito Viagem é o seu domínio e o conceito Local é seu contradomínio. Relações podem ser instanciadas a partir do conhecimento do domínio. Por exemplo, para expressar que o voo JJ3242Feb-15-2016 chega em Uberlândia deve-se escrever: (localChegada JJ3242-Feb-15-2016 Uberlândia).

Relações binárias por vezes são usadas para expressar os atributos do conceito. Geralmente, atributos são distinguidos de relações porque seu contradomínio é um tipo de dados, como por exemplo, *string*, *number* etc, enquanto que o contradomínio das relações é um conceito. O código a seguir define o atributo **numeroVoo**, que é uma *string*. Também é possível expressar relações de maior predicado, como "uma estrada liga duas cidades diferentes".

De acordo com Gruber (Gruber, 1993), axiomas formais servem para modelar sentenças que sempre são verdadeiras. Elas normalmente são usadas para representar conhecimento que não pode ser formalmente definido por outros componentes. Adicionalmente, axiomas formais são utilizados para verificar a consistência da própria ontologia ou a consistência do conhecimento armazenado na base de conhecimento. Axiomas formais são muito úteis para inferir novos conhecimentos. Um axioma no domínio Viagem seria de que não é possível viajar da América do Norte para a Europa de trem.

2.3.3 Instâncias

Instâncias são usadas para representar elementos ou indivíduos em uma ontologia. Um exemplo de instância do conceito JJ3242 é o voo JJ3242 que chega em Uberlândia em 15 de Fevereiro de 2016 e custa R$ 937,00.

2.4 SABIO - Uma metodologia de desenvolvimento de Ontologia

A comunidade de Engenharia Ontológica entende que os processos para construção de ontologias podem ser melhorados através de práticas da Engenharia de Software, pois, assim como software, ontologias precisam ser construídas com base em atividades padronizadas, ferramentas e métodos apropriados (FALBO, 1997). A ausência destes itens podem levar a problemas como inconsistência e falta de clareza do modelo ontológico desenvolvido.

Por isso, antes que se inicie a construção de uma ontologia é importante que se escolha uma metodologia que servirá de base para guiar os passos durante o desenvolvimento. Neste trabalho a metodologia escolhida foi a SABIO (*Systematic Approach for Building Ontologies*). Em (FALBO, 1997) são descritos todos os detalhes desta metodologia e seus passos.

SABIO foi originalmente concebido para apoiar na construção de ontologias de domínio [3] e incorporar melhores práticas comuns da Engenharia de Software e Engenharia Ontológica. Ele inclui uma linguagem gráfica para expressar ontologias, uma classificação de axiomas e o uso de questões de competência.

Conforme apresentado em (COSTA, 2008), os itens abaixo representam as etapas propostas pelo SABIO durante o desenvolvimento de uma ontologia:

1. Identificação de propósito e especificação de requisitos;
2. Captura da ontologia;
3. Fomalização da ontologia;
4. Integração com ontologias existentes; e,
5. Avaliação e documentação da ontologia.

2.4.1 Identificação de propósito e especificação de requisitos

O primeiro passo proposto por SABIO é a identificação do propósito pelo qual a ontologia está sendo criada e qual seu uso esperado. Estas respostas se dão através da definição das competências da ontologia, ou seja, delimitando o que será e o que não será escopo da ontologia. Por isso, neste momento é necessário que sejam definidas as questões de competência as quais a ontologia seja capaz de responder (COSTA, 2008).

2.4.2 Captura da ontologia

Neste momento é feita a conceituação dos itens do domínio que a ontologia objetiva formalizar, de acordo com o escopo definido segundo a competência da ontologia. Devem ser identificadas e organizadas as entidades relevantes do domínio utilizando uma forma clara e não ambígua para facilitar a comunicação entre as partes, assim como os axiomas também devem ser identificados com o intuito de definir a semântica dos termos envolvidos para restringir sua interpretação. Os axiomas devem ser orientados pelas questões de competências e devem ser suficientes para expressá-las e representar suas soluções (COSTA, 2008).

[3] Ontologias de Domínio tem o objetivo descrever um domínio específico.

2.4.3 Fomalização da ontologia

Esta etapa tem por objetivo transcrever para uma linguagem formal a conceituação escolhida no passo anterior através de alguma meta-ontologia, escolha de uma linguagem formal e criação da ontologia. É necessário que esta linguagem formal expresse de forma não-ambígua as entidades do domínio e axiomas para futuras interpretações do conhecimento expresso pela ontologia (COSTA, 2008).

2.4.3.1 Integração com ontologias existentes

Esta etapa tem por objetivo verificar se existe alguma conceituação já estabelecida de conceitos do domínio que está sendo formalizado e avaliar se é possível fazer a reutilização na ontologia que está sendo construída.

2.4.4 Avaliação e documentação da ontologia

Por fim, deve ser analisado se a ontologia construída está de acordo com escopo definido no primeiro passo. Para isto, a ontologia deve ser comparada com as questões de competências definidas e se ela atende alguns critérios de qualidade, como clareza, coerência etc.

Além disso, é preciso que seja feita toda a documentação da ontologia, como o escopo, descrição dos conceitos e a própria ontologia formal.

2.5 UFO - Uma ontologia Fundacional

Uma ontologia fundacional é um sistema de categoria independente de domínio que tem como objetivo ser usada como referência para melhorar a qualidade de modelos conceituais, uma vez que ajudam a reduzir ambiguidades e aumentam a clareza na interpretação ao fazer definição de primitivas de modelagem de semânticas do mundo real (GUIZZARDI; GUIZZARDI, 2008) (COSTA, 2008).

Neste trabalho vamos apresentar a UFO (*Unified Foundational Ontology*) que é uma ontologia fundacional originalmente desenvolvida por (GUIZZARDI, 2005a). O cerne da UFO é a UFO-A onde são definidos os principais conceitos, como por exemplo, coisas, objetos etc. Na UFO-B são definidos os eventos, como eventos, processos etc. E a UFO-C faz a definição das coisas intencionais e sociais. A seguir serão apresentados os principais conceitos de cada um dos conjuntos citados anteriormente da UFO.

2.5.1 UFO-A: Uma Ontologia de Objetos

A UFO-A, apresentada na figura 1, faz a definição de conceitos de objetos e suas propriedades e relacionamento. Na UFO-A existe uma distinção importante entre o que

é Universal e o que é Indivíduo. Os conceitos Universais são padrões que podem ser instanciados por vários indivíduos e são independentes de tempo e espaço. Já os Indivíduos são entidades que possuem identidade única.

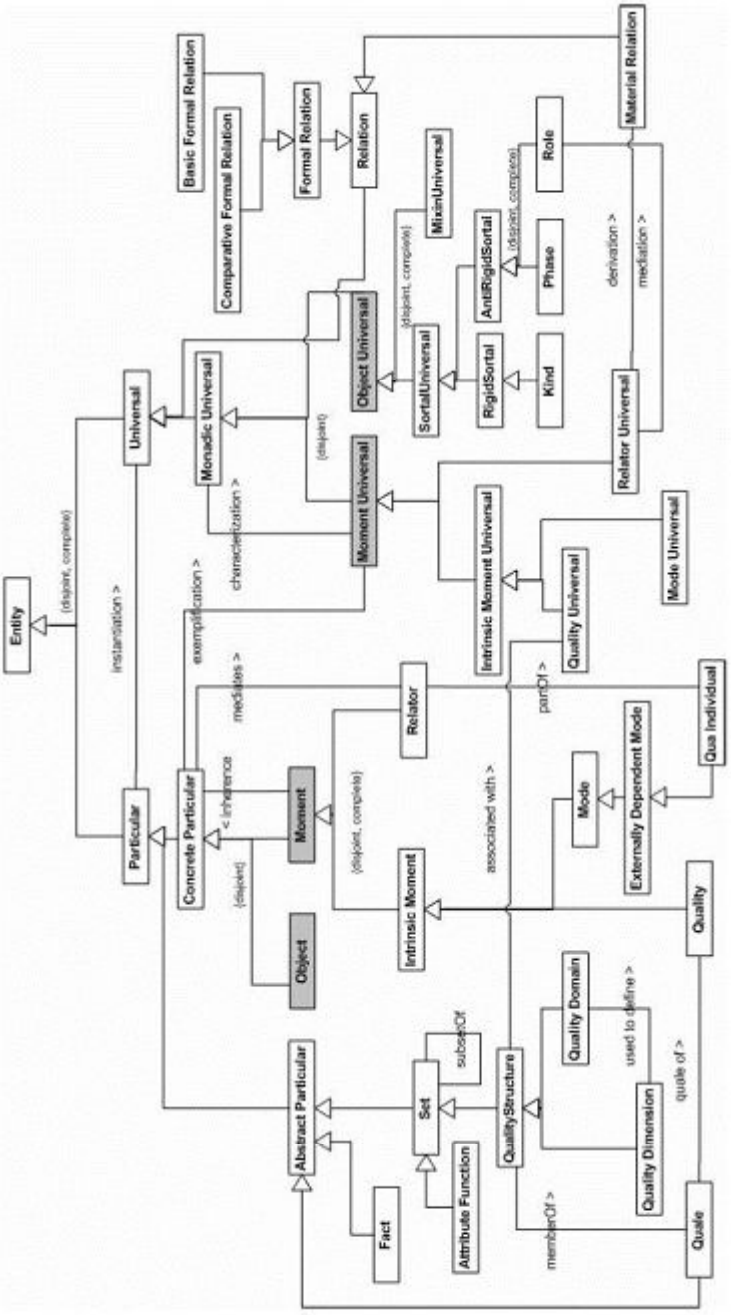


Figura 1 – Fragmento da UFO A

Os Substanciais são indivíduos independentes, tais como uma pessoa ou uma casa. O Modo é uma instanciação de uma propriedade, como uma cor ou uma doença, ou seja, ele só pode existir em outros indivíduos, por exemplo, uma doença só pode existir em um ser vivo. Um Modo intrínseco é dependente de somente um indivíduo (ex.: uma temperatura, uma massa); já um Modo relacional é dependente de vários indivíduos (um emprego, um casamento) (GUIZZARDI; GUIZZARDI, 2008).

O Modo externamente dependente é um modo intrínseco de um indivíduo, mas que existencialmente tem dependência de vários outros. Por exemplo, uma pessoa ao casar-se com outra adquire algumas responsabilidades, que são Modos existencialmente dependente dela e externamente dependente da outra pessoa.

Considerando a categoria de Universais, a UFO-A faz a uma importante distinção entre Universais Substanciais e Universais de Modo, onde os primeiros podem ser, por exemplo, massa, planeta e pessoa e os segundos uma cor, carga elétrica e dor de cabeça.

Relações são entidades que fazem conexão com outras entidades e podem ser: Relações Formais e Relações Materiais. As Relações Formais se dão diretamente entre duas ou mais entidades sem a necessidade de intervenção de outra entidade. Já as Relações Materiais entre duas ou mais entidades só existem se tiver uma entidade mediadora (que são chamadas de *relators*). Exemplo de Relações Materiais são "trabalhar em" e "sendo tratado em" (COSTA, 2008).

Por fim, é definido o conceito de Situação que representa entidades complexas constituídas por vários objetos (inclusive de outras Situações) e que apresentam uma parte da realidade que pode ser compreendida como um todo. Por exemplo "Maria trabalha na empresa X e estuda na faculdade Y" (GUIZZARDI; GUIZZARDI, 2008).

2.5.2 UFO-B: Uma Ontologia de Eventos

Diferentemente da UFO A, que é uma ontologia de Objetos, a UFO B é uma ontologia de Eventos. A diferença entre estes indivíduos está relacionada em suas ações no tempo. Um Objeto mantém sua identidade ao longo do tempo, ou seja, não possui partes temporais. Já os Eventos, são compostos por partes temporais, estendendo-se no tempo acumulando partes temporais. Desta forma, genuinamente falando, os eventos não sofrem mudanças no tempo, pois suas partes não mudam sua identidade ao longo do tempo. Pode-se citar como exemplo de Eventos: uma consulta médica; uma conversa; e, uma festa de casamento (GUIZZARDI; GUIZZARDI, 2008). A figura 2 apresenta um fragamento da UFO B.

Os eventos são dependentes da participação (*Participation*) de seus integrantes e podem alterar a realidade, mudando de um estado pré-evento para outra pós-evento. Por exemplo, o evento Aula somente existe com participação dos alunos e professor. Além disso a Aula altera o estado do conhecimento dos alunos, acrescentando novos conhecimentos ao final do evento.

Um Event (ou *Perdurant*) representa um evento e pode ser dividido entre:

1. *Atomic*: eventos que não podem ser subdivididos em outros eventos;
2. *Complex*: evento composto pelo agrupamento de outros eventos.

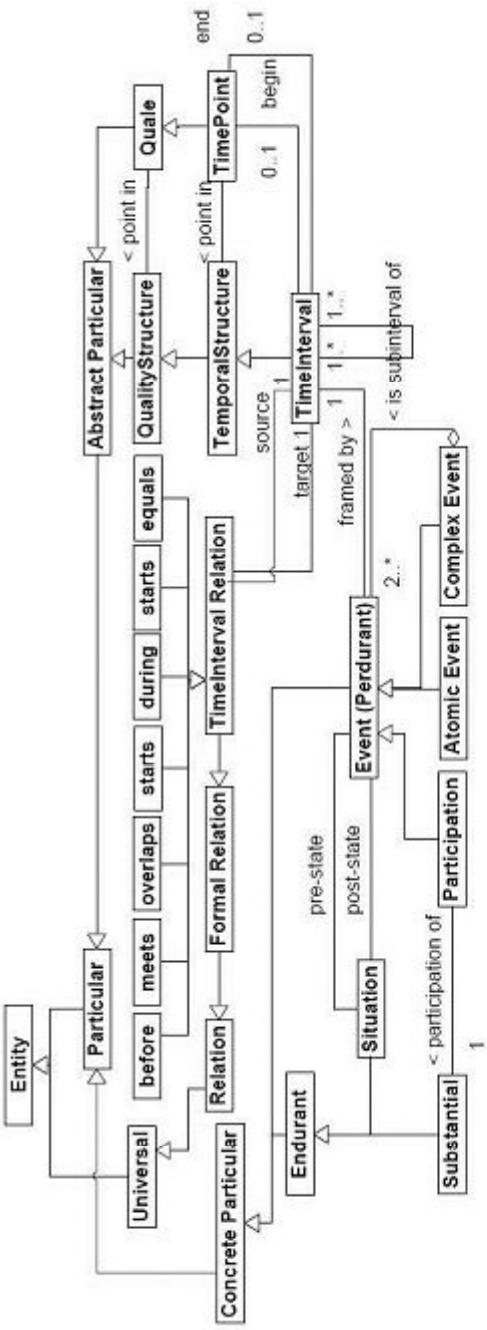


Figura 2 – Fragmento da UFO B

A UFO B considera que os modos espaciais de eventos são definidos em termos dos modos espaciais de seus participantes. Já as propriedades temporais dos substanciais são definidas em termos dos *events* nos quais participam. Projetando estas propriedades em uma estrutura de qualidade obtém-se o valor (*qualia*) dos modos temporais de eventos.

Os intervalos temporais (*time intervals*) compõem o espaço conceitual e podem ser representados por um conjunto de números reais. Por outro lado, os intervalos temporais são compostos por instantes (*time point*), que podem ser representados por números reais.

2.5.3 UFO-C: Uma Ontologia de Entidades Sociais

A UFO-C apresentada na figura 3 é uma ontologia de entidades sociais (de objetos e eventos), construída sobre a UFO-A e UFO-B. Seus conceitos são baseados nos *substantial individual (object)* e nos *moment individual (moment)* da UFO-A, e no conceito de *event* da UFO-B. Um *object* pode ser classificado entre: *Resource (Non-agentive objects)* e *Social Object*.

1. *Resource (Non-agentive objects)*: são utilizados pelos agentes com um objetivo e normalmente são controlados por um algum *agente*. Exemplo: carro, caneta etc.

2. *Social Object*: como exemplo de *Social Object* pode-se citar dinheiro, linguagem e normas (*normative descriptions*). Uma *normative descriptions* define uma ou mais regras/normas reconhecidas por pelo menos um agente social e que tem a capacidade de definir *universals nominais*, como *Social Moment* , *social objects* e *social roles*. Exemplo de *normative descriptions*: políticas de uma organização, estatuto de uma igreja, Constituição Brasileira etc.

   Os *Agents* são classificados em:

   a) *Human Agent*: agentes biológico ou humanos;

   b) *Artificial Agent*: entidades computacionais;

   c) *Institutional Agent*: organizações e unidades de uma organização.

O *Agent* é um *substantial* que pode ter tipos especiais de *moments*: os *Intentional Moments*. A intencionalidade é percebida como a capacidade de certas propriedades de alguns *individuals* se referir a possíveis situações na realidade. Todo *intentional moment* possui um conteúdo proposicional (*Goal*) e um tipo.

Actions são *events* intencionais que instanciam um plano (*Plan*) que é uma ação universal (*Action Universal*) cujo objetivo é satisfazer a *proposition* de alguma intenção (*intention*). As *actions* podem ser executadas somente por *agents* e tem a participação de objetos físicos (*Resources*) . Exemplo: a ministração de uma aula; a compra de uma

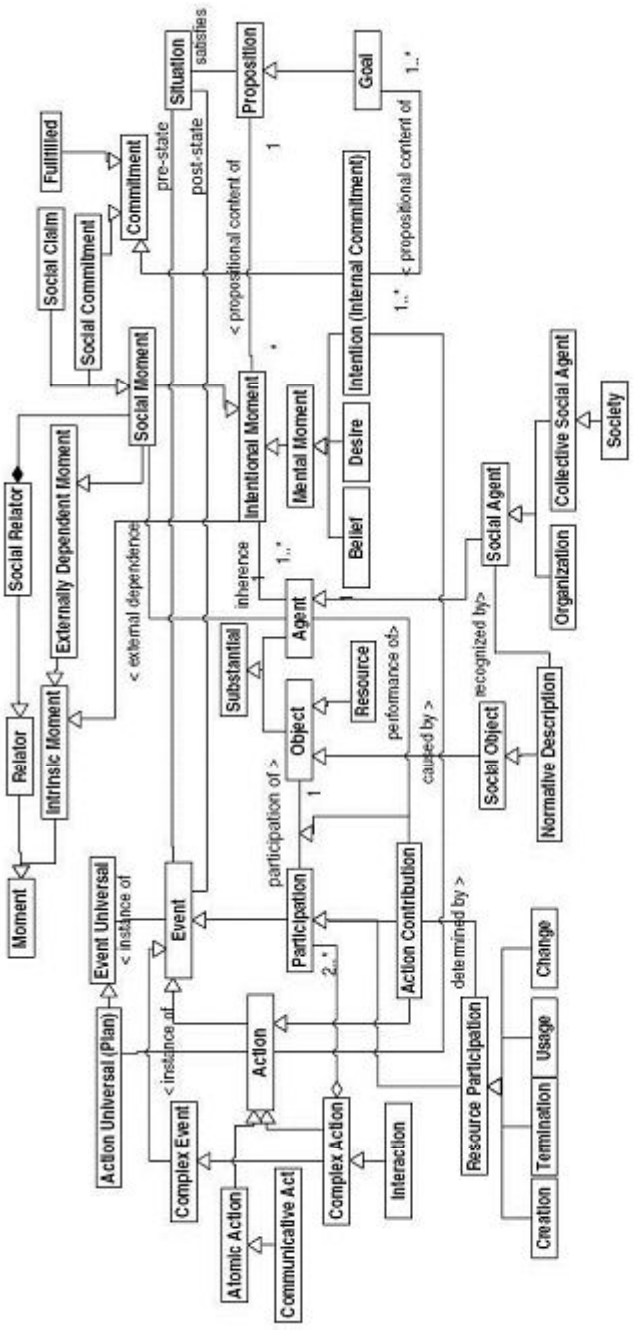


Figura 3 – Fragmento da UFO C

casa; uma conversa etc. Uma *communicative act* (ato de discurso) é uma *atomic action*. As *actions* podem ser classificadas como atômicas (*atomic*) ou complexas (*complex* - composta por mais de duas ou mais participações). Essas participações (*participations*) podem ser intencionais ou eventos não-intencionais. Nem toda participação de um *agente* é considerada uma *action*, mas somente as participações intencionais, chamadas de *Action Contributions* (COSTA, 2008).

Uma dependência de recurso pode ser causada por uma participação de recurso e a consequência de uma aquisição de recurso entre agentes. Em uma aquisição de recurso de um agente B para um agente A, A dá permissão do recurso **r** para B. Para isso acontecer, A deve ter o direito de conceder permissão para o agente B e, além disso, o direito de conceder o direito do tipo de permissão (por exemplo usar ou alterar) (GUIZZARDI; GUIZZARDI, 2008).

A troca de *communicative acts* cria os chamados *Social moments* que são tipos de *intentional moments*. Por exemplo, suponha o aluguel de uma casa por Maria. Quando Maria assina o contrato de aluguel com uma imobiliária, a imobiliária (*agente*) executa uma ação comunicativa (*communicative act*), criando, assim, um *Social Commitment* (compromisso de entregar o imóvel na data prevista) com a Maria. Além disso, cria também uma reivindicação social (*social claim*) da imobiliária para com Maria, relativa a esse conteúdo proposicional.

Um *Commitment* (interno ou social) pode ser cumprido (*Fulfilled*) ou Não-Cumprido (*Unfulfilled*), sendo um *Unfulfilled* classificado em:

1. *Pending*;
2. *Dismissed*;
3. *Broken*.

O *social commitment* leva à criação de um *internal commitment*, que por sua vez conduz um *agente* para a realização de uma *action*. Um *Commitment* (interno ou social) é cumprido por um *agente* se esse agente executar uma ação e o estado posterior dessa ação seja uma situação que satisfaça a *proposition* desse *commitment*.

2.6 Motores de inferência

Os motores de inferência ou *reasoners* são *software* que inferem conhecimentos adicionais e mostram relações implícitas a partir do mapeamento de uma base de conhecimento existente[4] (ZÚÑIGA, 2001; ABBURU, 2012). Com esta inferência os

[4] Coleção de conceitos e relações entre estes conceitos, fatos e regras

reasoners tornam-se capazes de responder consultas a partir do conhecimento provido e inferido, bem como checagem de consistência de ontologias (ZABLITH, 2008).

Além disso, eles também são aptos a realizar a classificação (computação de todas as classes as quais um determinado indivíduo pertence) e a realização (encontrar as classes mais específicas às quais um indivíduo pertence) de indivíduos. Atualmente, existem vários reasoners implementados e em constante aprimoramento tais como Racer (HAARSLEV; MÖLLER, 2001; HAARSLEV; MÜLLER, 2001), Pellet (SIRIN et al., 2007; KHAN; KUMAR, 2014) e Fact++ (BOBILLO; DELGADO; GÓMEZ-ROMERO, 2012). Cada um deles tem uma maneira diferente de tratar as informações na ontologia, mas algumas características são desejáveis a todos:

1. Dinamismo: Consiste em dar suporte ao acréscimo de informações na base de conhecimento, sempre atualizando as inferências de forma a manter a corretude das informações;
2. Multiplicidade: Conseguir trabalhar num domínio que possa conter uma ou mais ontologias, dando suporte a conceitos externos;
3. Suporte à linguagem padrão de ontologias (OWL); e,
4. Trabalhar eficientemente com grandes volumes de informação.

As duas próximas subseções apresentam os detalhes dos motores de inferência utilizados no desenvolvimento desta pesquisa.

2.6.1 Pellet

Pellet é um motor de inferência OWL-DL originalmente desenvolvido no Laboratório Mindswap da Universidade de Maryland. Ele é baseado em algoritmos de *tableaux* desenvolvidos para lógicas de descrição (DL) expressivas; e suporta a expressividade OWL-DL completa, incluindo raciocínio sobre nominais (classes enumeradas) (SIRIN et al., 2007; KHAN; KUMAR, 2014).

Dentre as principais vantagens do Pellet pode-se citar a portabilidade, facilidade de integração com os principais *frameworks* para desenvolvimento de ontologias – visto que foram desenvolvidos em Java –, e o bom desempenho se comparado a outros motores de inferência. O motor de inferência Pellet fornece muitos serviços diferentes de raciocínio.

Ele também incorpora várias técnicas de otimização descritas na literatura de DL e contém várias otimizações para nominais, resultados de consultas conjuntivas e raciocínio incremental. O pacote Pellet já possui uma versão do motor de inferência que funciona como um pequeno servidor *web* utilizando o protocolo DIG (DL

Implementation Group) para interagir com outras aplicações (PARSIA; SIRIN, 2000). Através dessa interface *web*, é possível fazer com que o Protégé utilize diretamente motor de inferência Pellet, bastando apenas que a ontologia utilize somente construtores suportados pelo DIG.

A integração direta entre o Protégé e o Pellet é feita através da interface DIG. Assim que o Pellet é instalado no sistema, ele cria um executável que realiza o raciocínio em arquivos RDF e outro executável que funciona como um pequeno servidor web que utiliza a interface DIG para se comunicar com outros programas, como o Protégé. A integração do Protégé com o Pellet através da interface DIG dá maior dinamismo ao desenvolvimento dentro do Protégé e facilita o desenvolvimento e a verificação de consistências na ontologia.

2.6.2 RACER

Racer é um motor de inferência para OWL DL e está livremente disponível para propósito de pesquisa e pode ser acessado pelos protocolos padrões HTTP ou TCP. Assim, outros programas clientes que precisem de serviços de inferência podem se comunicar com o Racer via protocolos TCP. Como exemplo de inferências disponível no Racer pode-se citar a verificação da consistência da ontologia e a criação da árvore inferida de classes (HAARSLEV; MÖLLER, 2001; HAARSLEV; MÜLLER, 2001).

Ele suporta expressividade da Lógica Descritiva e pode ler bases de conhecimento OWL tanto de arquivos locais como também de servidores *web* remotos. Ele suporta a API OWL e a interface DIG e segue múltiplas estratégias de otimização para melhor realizar as inferências (ILIE; MOLNAR, 2013; CHEN; HAARSLEV; WANG, 2005).

Racer pode ser implementado em projetos industriais baseados nos padrões W3Cs: RDF e OWL, e é uma importante ferramenta para pesquisa e desenvolvimento. Racer é um sistema baseado na representação do conhecimento que implementa um cálculo *Tableau* altamente otimizado usado para uma Lógica Descritiva muito expressiva.

3 Trabalhos Correlatos

Este capítulo tem por objetivo fazer uma análise de trabalhos correlatos a esta pesquisa. Serão apresentadas alguas ontologias de segurança.

3.1 Ontologia de Ataque de Segurança para Web Service

Web Services tornaram-se uma parte significativa da Web por causa de recursos atraentes como a simplicidade de uso, independência de plataforma e suporte a XML / SOAP.

No entanto, esses recursos o tornam vulnerável a muitas ameaças de segurança, ainda mais quando se fala de Web Services semânticos, que são capazes de publicar dados semânticos sobre suas propriedades funcionais e não funcionais, acrescentam ainda mais problemas de segurança. Agora, torna-se mais fácil atacar um Web Service porque seus dados semânticos estão disponíveis publicamente.

Para registrar e prevenir esses ataques, especialmente ataques distribuídos, novos *firewalls* distribuídos e sistemas de detecção de intrusão (F/IDS) devem ser aplicados. No entanto, estes F/IDS podem ser desenvolvidos por diferentes fornecedores e eles não têm mecanismos para cooperar uns com os outros. Este problema pode ser resolvido se vários F/IDS compartilham um vocabulário comum, que pode ser baseado em ontologias, para permitir que eles interajam uns com os outros.

O trabalho de (VOROBIEV; HAN, 2006) descreve as ameaças de segurança aos Web Services e afirma que elas precisam ser analisadas e classificadas sistematicamente para permitir o desenvolvimento de mecanismos defensivos melhor distribuídos usando F/IDS. A ontologia foi escolhida, porque elas permitem que diferentes partes evoluam e compartilhem uma compreensão comum de informações que podem ser racionalizadas e analisadas automaticamente. Foi desenvolvida a Ontologia de Ataque de Segurança para Web Service e ilustrados os benefícios de usá-la com um exemplo.

3.2 Uma Ontologia de Segurança da Informação

O trabalho de (HERZOG; SHAHMEHRI; DUMA, 2007) apresenta uma ontologia de segurança da informação disponível publicamente, baseada em OWL, que modela ativos, ameaças, vulnerabilidades, contramedidas e suas relações.

A ontologia pode ser usada como um vocabulário geral, roteiro e dicionário extensível do domínio da segurança da informação. Com base nela, os usuários podem concordar em

uma linguagem comum e definição de termos e relacionamentos.

Além de disponibilizar informações, a ontologia também é útil para raciocinar sobre as relações entre suas entidades, por exemplo, ameaças e contramedidas. A ontologia ajuda a responder perguntas como: Que contramedidas detectar ou impedir a violação de integridade de dados? Quais contramedidas impedem ataques de estouro de buffer?

A ontologia é composta por 88 classes de ameaças, 79 classes de ativos, 133 classes de contramedidas e 34 relações entre essas classes. No trabalho de (HERZOG; SHAHMEHRI; DUMA, 2007) é possível acessar o conteúdo da ontologia, bem como seus usos, potencial de extensão, implementação técnica e ferramentas para trabalhar com ela.

3.3 Ontologia de Segurança para Aplicações Móveis

A mobilidade é uma área emergente que surge com várias tecnologias e partes interessadas. Lidar com os requisitos de segurança para aplicações móveis significa adquirir todo o conhecimento e as tecnologias disponíveis para a concepção e implantação de uma medida confiável e utilizável.

Para ajudar os desenvolvedores a enfrentar esse desafio, o trabalho de (BEJI; El Kadhi, 2009) propõe uma solução de base de conhecimento através da conceituação de uma ontologia de segurança. A ontologia foi implementada em linguagem semântica OWL-DL com a ferramenta Protégé. Em (BEJI; El Kadhi, 2009) é possível verificar a estrutura da ontologia e os possíveis uso na segurança no mundo móvel.

3.4 Usando uma ontologia fundacional para reengenharia de uma Ontologia de Software Enterprise

O conhecimento sobre as organizações de software é consideravelmente relevante para engenheiros de software. O uso de um vocabulário comum para representar os conhecimentos úteis sobre organizações de software envolvidas em projetos de software é importante por várias razões, como apoiar a reutilização de conhecimento e permitir a comunicação e interoperabilidade entre ferramentas.

As ontologias de domínio podem ser usadas para definir um vocabulário comum para compartilhamento e reutilização de conhecimento sobre algum domínio. As ontologias fundacionais podem ser usadas para avaliar e re-projetar ontologias de domínio, dando a estas semânticas do mundo real. O trabalho de (BARCELLOS; De Almeida Falbo, 2009) apresenta uma avaliação de uma Ontologia de Software Enterprise que foi reengenharia utilizando a Ontologia da Fundação Unificada (UFO) como base.

3.5 Ontologia de Segurança: Simulação de Ameaças aos Ativos Corporativos

A análise e mitigação de ameaças essenciais para a segurança corporativa consomem tempo, são complexas e demandam conhecimento especializado. Em (EKELHART et al., 2006) é apresentada uma abordagem para a simulação de ameaças aos ativos corporativos, levando em conta toda a infraestrutura.

Usando esta abordagem é possível calcular medidas eficazes e seus custos sem conhecimento de especialistas e decisões de segurança subsequentes serão baseadas em critérios objetivos. A ontologia utilizada para a simulação é baseada na de Landwehr.

3.6 Ontologia do Gerenciamento de Nível de Serviço do Padrão ITIL

Com o objetivo de fornecer serviços com maior qualidade às organizações, em especial as organizações de TI, vêm utilizando boas práticas de gerenciamento de serviços consolidadas no mercado. O ITIL se destaca neste tema, pois ele proporciona grandes benefícios às organizações de TI e seus clientes.

O ITIL leva em conta o conceito de Gerenciamento de Nível de Serviço que é responsável por realizar o processo de negociação e definição dos serviços a serem utilizados pelo negócio, o tornando, assim, muito importante para as organizações. Ele leva em consideração os requisitos do usuário para sugerir o serviço mais adequado e o fornecimento do serviço por parte do provedor (qualidade do fornecimento) (COSTA, 2008).

No trabalho de (COSTA, 2008) são apresentadas ontologias de Gerenciamento de Nível de Serviço que visam representar os conceitos envolvidos neste domínio, possibilitando um entendimento comum e compartilhado deste conhecimento, além de possibilitar automatização do processo através da geração de informações gerenciais.

Além disso, (COSTA, 2008) também apresenta um estudo de caso onde as ontologias desenvolvidas são aplicadas a uma plataforma sensíveis ao contexto.

3.7 Outras Abordagens de Uso de Ontologias

A utilização de ontologias para representação, compartilhamento e estruturação de conhecimento também contempla problemas de resolução mais trivial, porém não menos importante, que aqueles pretendidos pela ETArch. Esta seção apresenta o uso de

Ontologia em uma gama de domínios e tarefas inerentes à Ciência da Computação como ferramenta para operacionalização de processos.

A exposição de trabalhos correlatos que utilizam Ontologia em outras abordagens começa pela descrição do seu uso em uma arquitetura corporativa. Uma arquitetura corporativa é uma descrição abrangente de todos os elementos-chave e relacionamentos que compõem uma organização através de várias visões. Cada visão expressa os elementos e as relações de um sistema a partir da perspectiva de preocupações específicas do sistema relevantes para um ou mais dos seus *stakeholders*. Como resultado, cada visão precisa ser expressa na linguagem de descrição de arquitetura que melhor se adeque às suas preocupações.

A arquitetura corporativa permite que empresas implementem integração empresarial para lidar com o ambientes de negócio dinamicamente em mudança. Entretanto, nas arquiteturas empresariais existentes, a falta de semântica equitativamente compreensível para humanos e sistemas é algo comum e que causa problemas de comunicação. Esses problemas impedem as empresas de implementar a integração e colaborar com outras empresas. Para resolver esse problema, o trabalho de (KANG et al., 2010) apresenta uma arquitetura corporativa baseada em ontologia. Esta ontologia de arquitetura corporativa é composta em três níveis; sendo que ontologias de termos de negócios estão no primeiro nível, ontologias de componentes de arquitetura de empresa estão no segundo nível, e ontologias de relações entre componentes de arquitetura de empresa estão no terceiro nível. Este trabalho objetiva que tanto seres humanos quanto sistemas possam entender exatamente qual é a semântica pretendida pela organização; o que é essencial para a integração inter e intra-empresas.

Além disso, as linguagens de modelagem de arquitetura corporativa atuais possuem dois problemas. Primeiro, as arquiteturas não têm mecanismos para integrar várias linguagens de descrição de arquitetura. Este problema dificulta a especificação de visualizações usando diferentes linguagens. Em segundo lugar, os modelos de arquitetura empresarial carecem de suporte à análise quantitativa. Neste sentido, o trabalho de (BAKHSHANDEH et al., 2013) descreve uma abordagem baseada em ontologia para ter uma ontologia modular para o domínio de arquitetura corporativa, especificar e integrar múltiplas linguagens de modelagem de arquitetura e analisar os modelos integrados resultantes. Os modelos resultantes são quantificáveis no sentido em que fornecem os meios para avaliar a consistência dos modelos de arquitetura e analisar sua estrutura. A aplicabilidade da abordagem é mostrada através de um estudo de caso e a correção da ontologia é mostrada por um meio de motores de inferência.

Na mesma linha de integração de conhecimento empresarial, o trabalho de (HARRISON; CHAN, 2005) a apresenta o desenvolvimento de um sistema de gestão de ontologias distribuídas cujo objetivo é fornecer uma estrutura para lidar com o

compartilhamento, armazenamento, versão e segurança de ontologias em um repositório. Na proposta apresentada, as ontologias são representadas por uma hierarquia de classes genéricas orientadas a objetos, que podem ser traduzidas para XML. Para compartilhar as ontologias, o sistema usa uma arquitetura cliente-servidor distribuída usando TCP e um banco de dados convencional é usado para armazená-las. Um mapeamento do modelo relacional para a representação orientada a objetos permite criar aplicações que transfiram informações. O autor conclui o trabalho mostrando que o sistema fornece algumas melhorias sobre os sistemas de gerenciamento de ontologias existentes e discute os caminhos para uma maior extensão do sistema.

Por fim, o trabalho de (WANG et al., 2012) apresenta os resultados de um trabalho sobre modelagem semântica para a Internet das coisas que mostra que ela tornou-se fundamental para resolver o problema da interoperabilidade dada a natureza distribuída e heterogênea das "coisas". A pesquisa focalizou na modelagem dos dispositivos e dos recursos e deu menos ênfase para o acesso e na utilização da informação gerada pelas coisas. A ideia de que as coisas são capazes de expor interfaces de serviço padrão coincide com a computação orientada a serviços e, mais importante, representa um meio escalonável para serviços empresariais e aplicativos que precisam de conhecimento de contexto e inteligência para acessar e consumir as informações do mundo físico. Para isso, os autores apresentam o projeto de uma ontologia de descrição abrangente para a representação do conhecimento no domínio da Internet das Coisas e discutem como ela pode ser usada para suportar tarefas como descoberta de serviços.

4 Metodologia e Desenvolvimento

Este capítulo apresenta a metodologia de desenvolvimento da ontologia de ameaça interna que foi criada para validar a hipótese deste trabalho de pesquisa. Ele abrange tanto os procedimentos de seleção do domínio de negócio e da base de dados de incidentes internos, mapeamento e desenvolvimento da ontologia, exemplos de instanciação e os procedimentos de validação da sua consistência interna utilizando os motores de inferência Pellet e Racer.

Esta abordagem foi escolhida porque vai ao encontro de boas práticas de criação de ontologias complementando-as de acordo com a necessidade da pesquisa (CAPPELLI; MOORE; TRZECIAK, 2012; MIZOGUCHI, 2004; HARRISON; CHAN, 2005; KALFOGLOU; SCHORLEMMER, 2003). Por fim, a guisa de conclusão do capítulo são discutidos os resultados sob a perspectiva da aplicabilidade, utilização e relevância do uso de ontologias em ambientes distribuídos.

Como já ressaltado, o uso e a importância das ontologias em Ciência da Computação está se tornando mais difundido, porém a construção de ontologias é em grande parte uma tarefa de tentativa e erro. Na construção da ontologia resultante desta pesquisa, foi utilizada a metodologia SABIO para guiar os passos de construção da Ontologia.

4.1 Seleção do Domínio de Negócio da Ontologia

O estudo da ameaça interna apresenta alguns dos desafios mais complexos na segurança da informação (CAPPELLI; MOORE; TRZECIAK, 2012). O Instituto de Engenharia de *Software* da Universidade Carnegie Mellon define um intruso malicioso como um empregado atual ou antigo, contratante ou outro parceiro de negócio que tem ou teve acesso autorizado a uma rede, sistema ou dado da organização e intencionalmente excedeu este acesso em um gerenciamento que negativamente afetou a confidencialidade, integridade ou disponibilidade de informações da organização (KALFOGLOU; SCHORLEMMER, 2003; LIU; HOGAN; CROWLEY, 2011).

As organizações começaram a reconhecer a importância de detectar e prevenir ameaças internas, mas há uma surpreendente falta de padrões dentro do domínio de ameaças internas para auxiliar no desenvolvimento, descrição, teste e compartilhamento dessas técnicas (WEST-BROWN et al., 2003). Para muitas organizações, o estabelecimento de um programa de ameaças internas e o início de busca por atividades de potenciais intrusos mal-intencionados é uma nova atividade empresarial uma vez que o uso intensivo das redes de comunicação é um caminho de mão única(ALLEN, 2001).

No escopo desta pesquisa, o principal objetivo do desenvolvimento da ontologia de Ameaça Interna é apoiar a criação, o compartilhamento e a análise de indicadores de ameaça interna como forma de verificar a hipótese da pesquisa.

Este domínio de negócio foi escolhido como estudo de caso para desenvolvimento da ontologia porque a segurança da informação é uma preocupação inerente ao mercado de TI, seja qual for sua área de atuação final. A partir daí, pode-se passar para o mapeamento dos seus principais componentes ontológicos (BROWN; DUGUID, 1998; JONG; FERGUSON-HESSLER, 1996).

Como em qualquer outro domínio, a criação de uma ontologia na área de segurança interna deve se atentar para o mapeamento de componentes ontológicos que representem tanto o *conhecimento tácito* quanto o *conhecimento implícito*. (FRAPPAOLO, 2008).

4.2 Mapeamento dos Macro Componentes Ontológicos

Dados de segurança são sensíveis e por isso as equipes de ameaça interna geralmente trabalham apenas com os casos referentes à sua própria organização. O registro destes incidentes frequentemente incluem detalhes documentados sobre comportamentos de funcionários, propriedade intelectual, atividades dos funcionários nas redes e informações sobre a arquitetura de TI (FITHEN; FRASER, 1994; WEST-BROWN et al., 2003).

Organizações e equipes hesitam em divulgar essas informações devido ao risco de violar a privacidade de funcionários, liberar informações organizacionais privilegiadas ou desnecessariamente perder uma vantagem competitiva (CAPPELLI; MOORE; TRZECIAK, 2012).

Neste contexto, uma ontologia sobre estes incidentes permitiria que equipes compartilhassem indicadores de ameaças internas sem divulgar seus dados confidenciais. O resultado desejado é facilitar o compartilhamento de informações sobre indicadores efetivos de atividades mal-intencionadas entre as organizações, com ênfase na extensibilidade, semi-automação e a capacidade de os membros da comunidade se beneficiar de investigações e análises realizadas por outros (FITHEN; FRASER, 1994).

Todos os modelos de dados de entidade e relacionamento, incluindo modelos de dados semânticos, têm suas limitações (TAFAZZOLI; SADJADI, 2008). Os modelos são extremamente formais e podem encontrar problemas ao representar a variedade de ações envolvidas em um caso real de ameaça interna. Além disso, os dados sobre casos de ameaça interna são muitas vezes recolhidos a partir de julgamentos de ações legais, cujos resultados envolvem documentação altamente variável (TAFAZZOLI; SADJADI, 2008).

Como resultado, os especialistas em segurança tendem a confiar na linguagem natural para documentar seus casos e descobertas (JONG; FERGUSON-HESSLER, 1996).

Embora a linguagem natural seja mais expressiva do que um modelo abstrato, esta pesquisa pressupõe que a área de segurança da informação se beneficiaria com a criação de uma ontologia sobre ameaças internas devido aos seguintes fatores (BROWN; DUGUID, 1998):

- Perspectiva de rápido crescimento dos dados coletados e compartilhados pelas organizações, posto que algumas delas já afirmaram informalmente que superar esse desafio é uma de suas principais prioridades; e,
- A comunidade de pesquisa de ameaças internas pode se beneficiar do modelo formal adicional desenvolvido neste trabalho, pois ele é executável por máquina e compreensível por humanos.

O domínio da segurança de TI contém também outros conceitos de interesse na descrição do domínio de ameaças internas, como, confidencialidade, integridade e disponibilidade.

Desde 2001, o CERT (*Computer Emergency Response Team*) tem registrado e analisado mais de 800 casos reais de incidentes de segurança em que os profissionais de TI utilizaram a própria infraestrutura tecnológica da organização para interromper seus serviços críticos, cometer fraudes contra alvos internos, roubar propriedade intelectual ou conduzir espionagem de segurança (CAPPELLI; MOORE; TRZECIAK, 2012). As informações são codificadas em campos estruturados e de texto livre na base de dados. Esses dados fornecem a base para toda a pesquisa sobre ameaças internas deste trabalho (HARVEY, 1991).

O CERT disponibiliza dois conjuntos de dados que contêm informações estruturadas sobre incidentes de ameaça interna. A base de dados MERIT contém informações sobre casos de ameaça interna maliciosa envolvendo fraude, sabotagem ou roubo de propriedade intelectual. A base de dados SpyDR contém casos de espionagem nacional. Este trabalho considerou apenas a base de dados MERIT para a criação da ontologia[1].

Este conjunto de dados, cuja macro estrutura é ilustrada na figura 4, baseia-se no recolhimento de informações sobre três entidades: as organizações envolvidas; o executor da atividade maliciosa; e, os detalhes do incidente. Cada caso do repositório de incidentes internos contém uma descrição em linguagem natural dos observáveis técnicos e comportamentais do incidente. Essas descrições foram usadas como a fonte de dados primária para o desenvolvimento da ontologia.

A ontologia foi construída com os resumos das histórias de incidentes da base de dados MERIT e sua consistência foi verificada para determinar quão eficiente a ontologia pode expressar incidentes de ameaça interna (CAPPELLI; MOORE; TRZECIAK, 2012). A ontologia visa responder as seguintes questões de competência:

[1] O *dataset* pode ser obtido no endereço ftp://ftp.sei.cmu.edu/pub/cert-data/

Figura 4 – Modelo do CERT para incidentes internos

Q1: O que é uma ameaça interna? Q2: Quais entidades podem estas envolvidas em um incidente de ameaça interna? Q3: Qual a interação entre estas entidades? Q4: Quais ativos podem ser afetados ou manuseados durante um incidente? Q5: Quais ações podem ser realizadas durante um incidente? Q6: Quais informações pode ser impactadas durante um incidente?

À medida que dados são coletados de várias fontes, pode-se repetir o processo de extração e adicioná-las na ontologia com o objetivo final de melhorar a habilidade da ontologia em expressar indicadores de ameaça interna.

Uma vez que o domínio de negócio foi selecionado e o mapeamento dos macro componentes ontológicos foi realizado, o próximo passo é o desenvolvimento da ontologia, que é detalhado na próxima seção.

4.3 Desenvolvimento da Ontologia

A figura 5 apresenta a modelagem da ontologia de acordo com os conceitos da UFO.

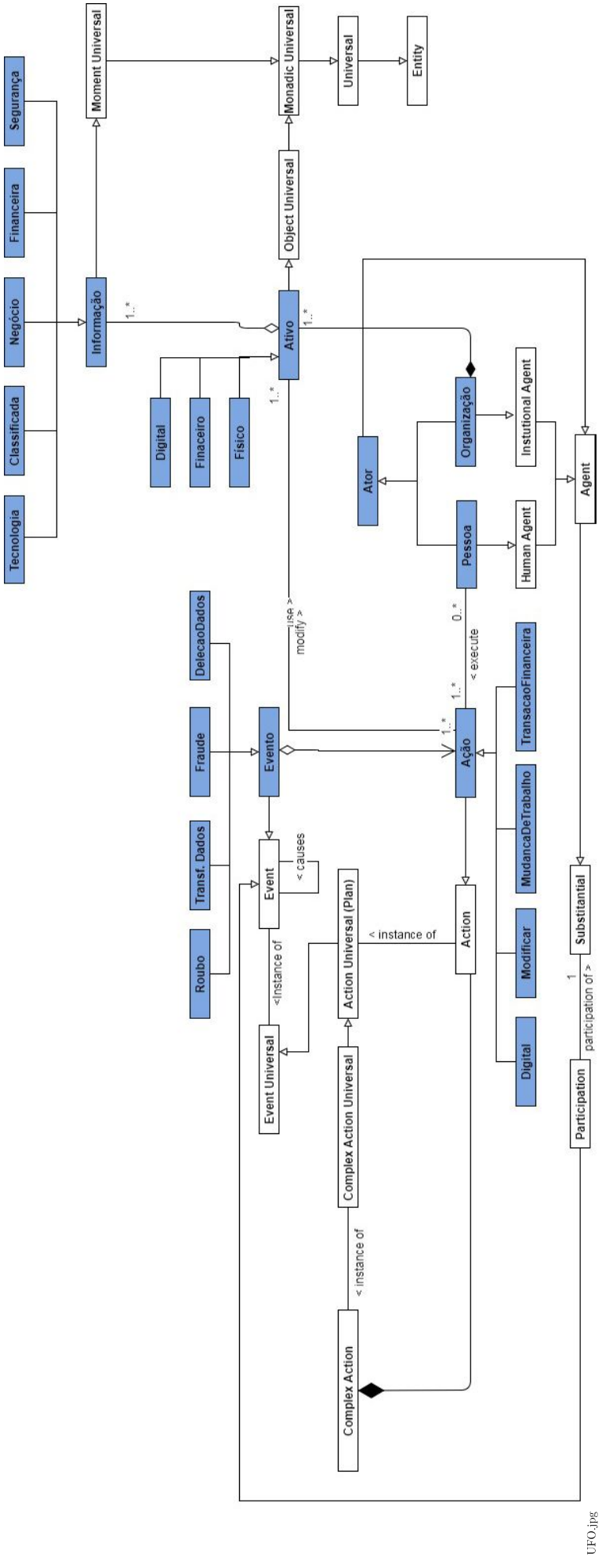
As Ações (*Action*) são executadas por um Ator (*Human Agent*) e podem ser da natureza de: ações digitais; ações de modificação; ações de mudança de trabalho; e, ações de transações financeiras. As ações somente são realizadas se envolver pelo menos uma pessoa e uma organização.

(A1) $\forall x(\exists y(\exists z(\text{ação}(x) \rightarrow (pessoa(y) \wedge organização(z)))))$

Duas ou mais ações combinadas culminam em um Evento do tipo *Event* que é uma instância de um *Event Universal*. Os Eventos mapeados na ontologia são da origem de roubo, transferência de dados, fraude e deleção de dados.

(A2) $\forall x(\exists y((evento(x) \rightarrow \text{ação}(y))))$

Os Ativos são objetos universais (*Object Universal*) que podem ser usados ou modificados durante uma ação. Os ativos mapeados na ontologia são: ativos financeiros; ativos físicos; e, ativos digitais. Eles fazem parte das Organizações (*Instutional Agent*)


Moment Universal
Monadic Universal
Universal
Entity
Segurança
Financeira
Negócio
Classificada
Tecnologia
Informação
Object Universal
Ativo
Digital
Finaceiro
Físico
Ator
Organização
Instutional Agent
Agent
Pessoa
Human Agent
DelecaoDados
Fraude
Transf. Dados
Roubo
Evento
Ação
TransacaoFinanceira
MudancaDeTrabalho
Modificar
Digital
Event
Action
Substitantial
Participation
Event Universal
Action Universal (Plan)
Complex Action Universal
Complex Action
use >
modify >
0..*
1..*
< execute
< causes
<Instance of
< instance of
participation of >
UFO.jpg

que estão envolvidas durante uma ação de incidente.

(A3) $\forall x(\exists y((ação(x) \rightarrow modifica(y))))$

(A4) $\forall x(\exists y((organização(x) \rightarrow ativo(y))))$

Tanto as Pessoas quanto as Organizações são *Agents* que tem uma participação (*participation*) em um evento (*Event*) de incidente de ameaça.

A relação de causalidade (*causes*) entre eventos está formalizada pelos axiomas (A5), (A6), (A7) e (A8). É uma relação irreflexiva (um evento x não pode causar ele mesmo), assimétrica (se um evento x causa outro evento y, então y não pode causar x) e transitiva (se um evento x causa um evento y que causa outro evento z, então x causa z) (COSTA, 2008).

(A5) $\forall e1, e2((event(e1) \wedge event(e2) \wedge causes(e1, e2)) \rightarrow$
$\exists s(situation(s) \wedge posState(s, e1) \wedge preState(s, e2)))$

(A6) $\forall x(event(x) \rightarrow \neg causes(x, x))$

(A7) $\forall x, y(event(x) \wedge event(y) \wedge causes(x, y) \rightarrow causes(y, x))$

(A8) $\forall x, y, z(event(x) \wedge event(y) \wedge event(z) \wedge causes(x, y) \wedge causes(y, z) \rightarrow causes(x, z))$

A ontologia de ameaça Interna foi modelada utilizando-se a ferramenta Protégé, que é um sistema de gerenciamento do conhecimento e oferece uma interface gráfica para definição de ontologias.

4.3.1 Classes da Ontologia

O modelo lógico de alto nível da ontologia está representado na Figura 6 e é composto por cinco classes: Ator; Acao; Ativo; Evento; e, Informação.

Figura 6 – Modelo de Entidade Lógica de Alto Nível

4.3.1.1 Classe Ator

A classe **Ator** contém subclasses que representam **Organizações** e **Pessoas** conforme apresentado na Figura 7.

Figura 7 – Hierarquia da Classe **Ator**

4.3.1.2 Classe Acao

A classe **Acao** e suas subclasses definem as ações que o ator pode executar no domínio de ameaça interna. A subclasse **AcaoModificar** contém subclasses que são qualitativamente modificadores para serem usadas em combinação com outra subclasse de **Ação**. Por exemplo, para modelar uma ação de pesquisa suspeita, um indivíduo pode ser associado às classes **AcaoPesquisar** e **AcaoSuspeita**. A hierarquia da classe **Acao** pode ser vista na Figura 8.

Figura 8 – Hierarquia da Classe **Acao**

A Figura 9 mostra as subclasses das classes **AcaoDigital**, **AcaoModificar**, **AcaoMudancaDeTrabalho** e **AcaoTransacaoFinanceira**.

4.3.1.3 Classe Evento

Eventos são mecanismos por meio dos quais várias ações podem ser agrupadas e relacionadas por uma análise qualitativa ou contextual. Uma ação é classificada como o que é observado e evento como o que é inferido. A criação de um indivíduo da classe **Evento** geralmente requer alguma inferência, o contrário de um indivíduo da classe Ação, que pode ser criado através da observação direta.

Por exemplo, a ontologia contém a subclasse chamada **EventoTransfDados** que é uma cópia, transferência ou recuperação de dado não autorizada de um computador ou servidor. Extravio de dado por si só não é tecnicamente observável, mas as ações específicas de cópia, transferência ou recuperação de dado associado com o extravio são

Figura 9 – Hierarquia das Classes AcaoDigital, AcaoModificar, AcaoMudancaDeTrabalho e AcaoTransacaoFinanceira

observáveis. Então, a ação específica pode ser dita correspondente ao evento de extravio.

A hierarquia de classe **Evento** é representada na Figura 10.

Figura 10 – Hierarquia da Classe **Evento**

4.3.1.4 Classe Ativo

A classe **Ativo** provê subclasses que definem os objetos da ação. Esta classe contém subclasses que representam os alvos das ações ou instrumentos usados como objetos das ações no nosso domínio. A Figura 11 é uma representação da hierarquia da classe **Ativo**.

Figura 11 – Hierarquia da Classe **Ativo**

4.3.1.5 Classe Informação

A classe Informação contém subclasses que provêm suporte para modelagem de informações de alguns ativos ou informações afetadas pelas ações (exemplos incluem informações de identificação pessoal, segredos comerciais e informações classificadas). A figura 12 apresenta a hierarquia da classe **Informacao**.

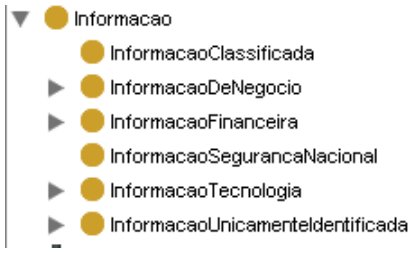


Figura 12 – Hierarquia da Classe **Informacao**

4.3.2 Propriedades de Objetos da Ontologia

A hierarquia de propriedade de objetos (apresentada na figura 13) provê a habilidade para especificar vários tipos de relacionamentos familiar, de trabalho e de evento entre

dois atores. A propriedade de objeto também fornece relacionamentos para associar vários atores e ativos às ações via propriedades como, por exemplo, **temAtor**, **temAtivo**, **temObjeto** e **temInstrumento**.

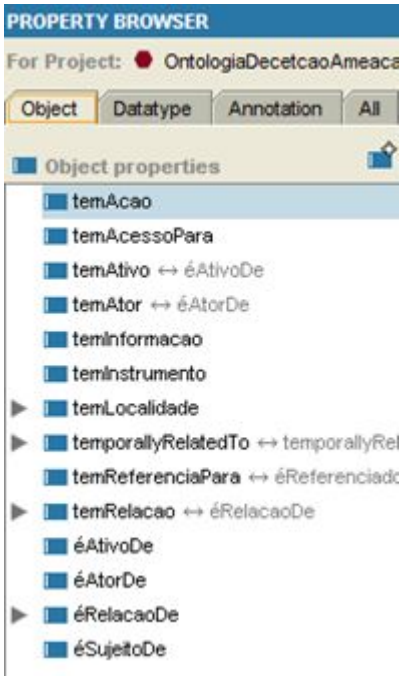


Figura 13 – Hierarquia das Propriedades de Objetos

4.4 Tradução de incidentes na Ontologia de Ameaça Interna

Esta seção apresenta os detalhes do processo de análise de instanciação de casos de ameaças internas segundo a ontologia, o qual se inicial com um exemplo de amostra em linguagem natural:

"O invasor modificou dados críticos da organização vítima"

As atividades chaves de análise durante a validação são:

1. Determinar se as ações do incidente detalhado estão representadas na ontologia;
2. Identificar itens ausentes; e,
3. Revisar a representação na ontologia comparando com o domínio do mundo real.

Deve-se repetir as atividades de análise para cada ação até que todas as ações sejam representadas com sucesso na ontologia. Do exemplo mencionado, a frase "o invasor modificou dados críticos" requer que a ontologia esteja apta a expressar:

- Uma ação onde o resultado é a modificação do dado;
- Importantes propriedades dos dados, como eles sendo críticos para o negócio; e,
- Importantes relacionamentos entre a ação e objetos de dados, como a pessoa que executou a ação e o dono do dado.

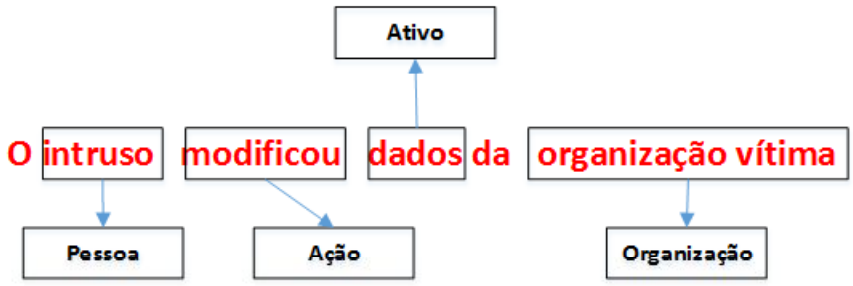


Figura 14 – Análise do Exemplo

Deve-se avaliar a sentença rotulada para identificar algum aspecto ausente que a ontologia deveria ser capaz de representar, bem como transformações importantes que serão requeridas para traduzir a sentença na ontologia enquanto preservando o significa original. Algumas vezes isto requer o uso de termos substitutos. Por exemplo, o termo "furtou" pode tornar-se **AcaoRoubar** com múltiplas propriedades. Geralmente ações ou eventos são os pontos de início para expressar uma dada sentença.

Após a tradução e validação dos dados brutos para ontologia, é realizada a diagramação do modelo para visualização.

Os passos abaixo resumem o processo de representar um texto na ontologia:

1. Rotular texto natural: Adicione tipos semânticos para cada parte da sentença;
2. Analisar o texto rotulado. Verifique se os rótulos necessários estão listados para cada tipo e se cada conceito está representado;
3. Traduzir o texto rotulado: Represente as atividades ou eventos de casos importantes usando a linguagem definida na ontologia. Por exemplo, a descrição de um dado que é modificado torna-se uma instância da classe **AcaoModificar**, da propriedade de objeto **temObjeto** e uma instância da classe Dado; e,
4. Modelar o texto traduzido: Modelar os aspectos importantes das atividades ou eventos do caso e seus importantes atributos ou relacionamentos.

As próximas subseções e as respectivas Figuras 15, 16 e 17 apresentam três exemplos de tradução de casos reais de incidentes para a Ontologia de Ameaça Interna desenvolvida neste trabalho.

4.4.1 Exemplo 1: Roubo de Credenciais

"O invasor roubou as credenciais de senha de colegas de trabalho para se autenticar no sistema e cometer fraude".

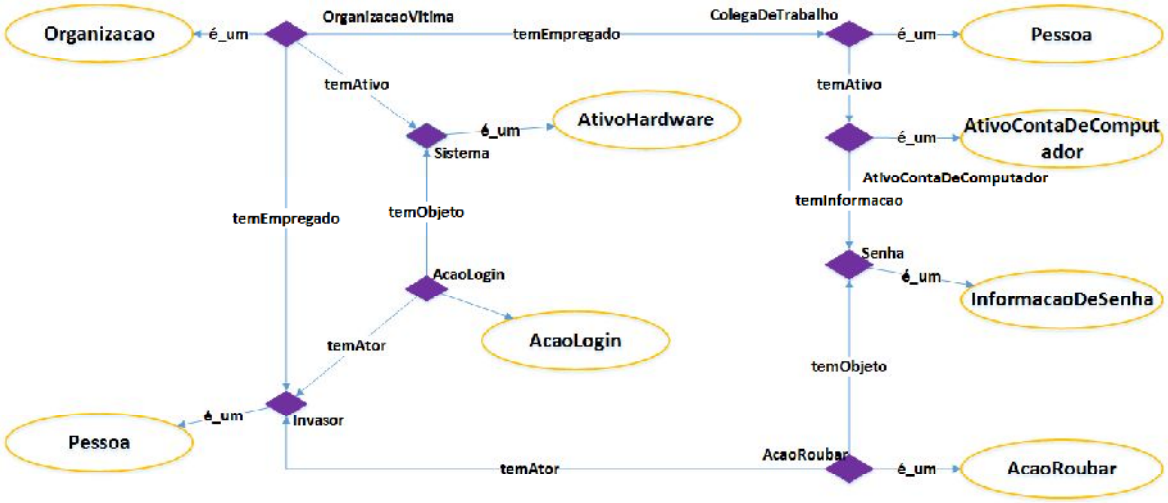


Figura 15 – Diagrama Exemplo 1: Roubo de Credenciais

4.4.2 Exemplo 2: Transferência de Planos Proprietários

"O invasor transferiu planos proprietários de engenharia dos sistemas de computação da organização vítima para sua nova organização de trabalho".

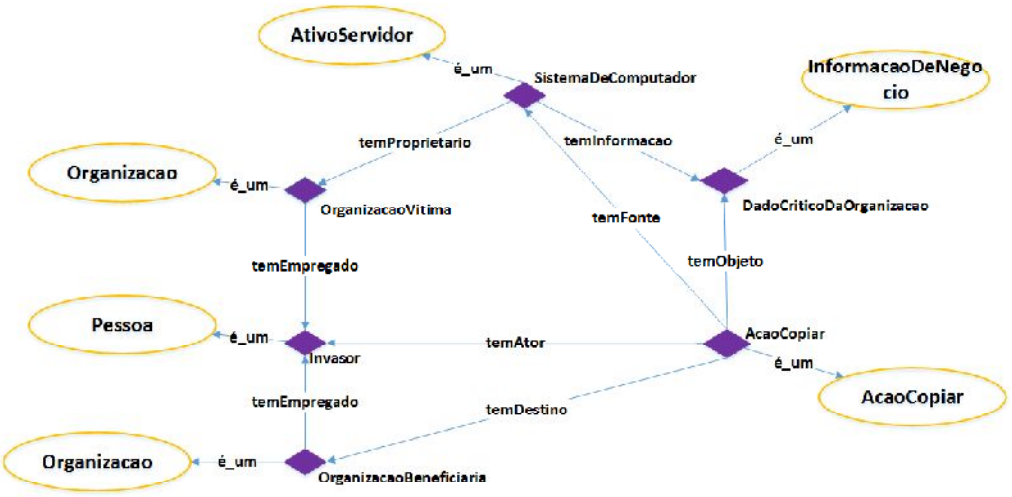


Figura 16 – Diagrama Exemplo 2: Transferência de Planos Proprietários

4.4.3 Exemplo 3: Acesso Remoto a Servidor Web

"O invasor acessou um servidor web remotamente com uma conta de administrador e deletou aproximadamente 1.000 arquivos".

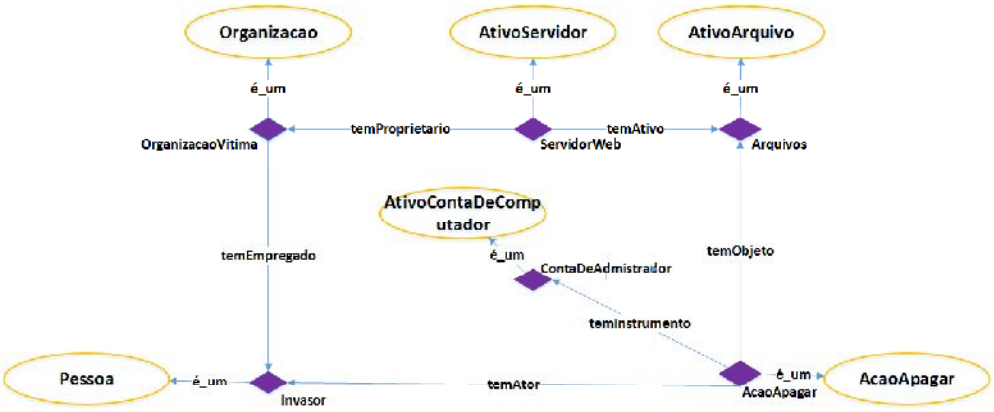


Figura 17 – Diagrama Exemplo 3: Acesso Remoto a Servidor Web

4.5 Validação da Consistência da Ontologia

A Ontologia de Ameaça Interna foi executada em dois motores de inferência (Pellet e Racer) para validação da consistência. O Pellet foi escolhido por ser nativo do Protégé e por ter sido utilizado em vários projetos de pesquisa da indústria com sucesso (SIRIN et al., 2007; KHAN; KUMAR, 2014).

A escolha do RACER se deu por ele ser um motor de inferência que se integra bem ao Protégé e por ser complementar ao Pellet no processo de validação da consistência da ontologia. (HAARSLEV; MÖLLER, 2001; HAARSLEV; MÜLLER, 2001; ILIE; MOLNAR, 2013; CHEN; HAARSLEV; WANG, 2005). Entende-se que com a validação por esses dois motores de inferência é possível afirmar que a ontologia está consistente e apta a ser utilizada pelas aplicações que demandam serviço de ameaça interna.

Para validar a ontologia construída, foi verificada sua consistência, cujo objetivo é assegurar que a ontologia desenvolvida não contém fatos contraditórios. Por exemplo, um indivíduo não pode ser instância das classes **Organizacao** e **Pessoa** ao mesmo tempo, uma vez que na ontologia foi declarado que estas classes são disjuntas[2].

Além disso, os motores de inferência Pellet e Racer calculam a hierarquia de classe inferida, ou seja, computa as relações das subclasses entre todas as classes principais para criar a hierarquia de classe completa. A hierarquia de classe pode ser usada para

[2] Classes disjuntas definem que um indivíduo não pode ser instância de mais de uma das classes configuradas como disjuntas

responder perguntas, tais como a obtenção de todas ou apenas as subclasses diretas de uma classe.

4.5.1 Validação com o Pellet

Pellet é um motor de inferência completo e capaz do OWL-DL com um bom desempenho e com um número de características únicas. Ele é construído em Java e é código aberto. Ele é utilizado em uma série de projetos de pesquisas para ambientes industriais.

Pellet é a primeira implementação do procedimento de decisão completo para OWL-DL e tem suporte extensivo para raciocínio com indivíduos, tipo de dados definidos e debug de ontologias. Ele implementa várias extensões para OWL-DL e provou ser uma ferramenta confiável para trabalhar com este tipo de ontologia. O Pellet é nativo do Protégé, então para fazer a validação da ontologia com este motor, basta selecioná-lo na barra de ferramentas conforme Figura 18.

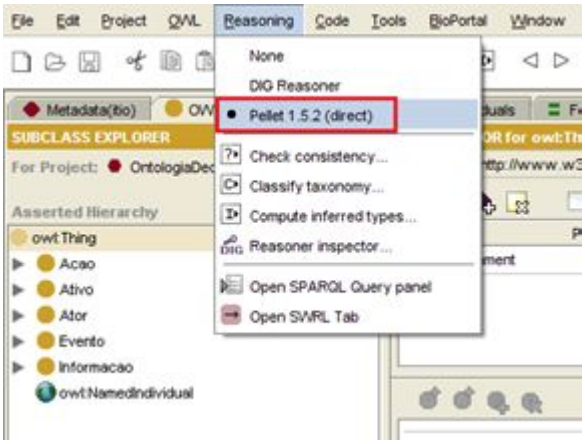


Figura 18 – Chamada do Pellet no menu do Protégé

Uma vez selecionado o Pellet como o motor de inferência que fará as validações na ontologia, escolhe-se a opção de *"Classify taxonomy"* para que Pellet possa fazer as checagens de consistência.

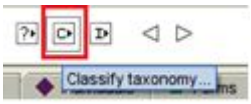


Figura 19 – Botão de Chamada para Classify Taxonomy no Protégé

Assim, o Pellet lê toda a estrutura de classes da Ontologia de Ameaça Interna afim de validar sua consistência. Conforme ilustrado na Figura 20, o Pellet foi executado na Ontologia de Ameaça Interna e não encontrou nenhum problema com a estrutura e ligações das classes.

4.5.2 Validação com o Racer

Racer é um motor de inferência para OWL DL. Ele suporta a API OWL e a interface DIG e segue múltiplas estratégias de otimização para melhor realizar as inferências;

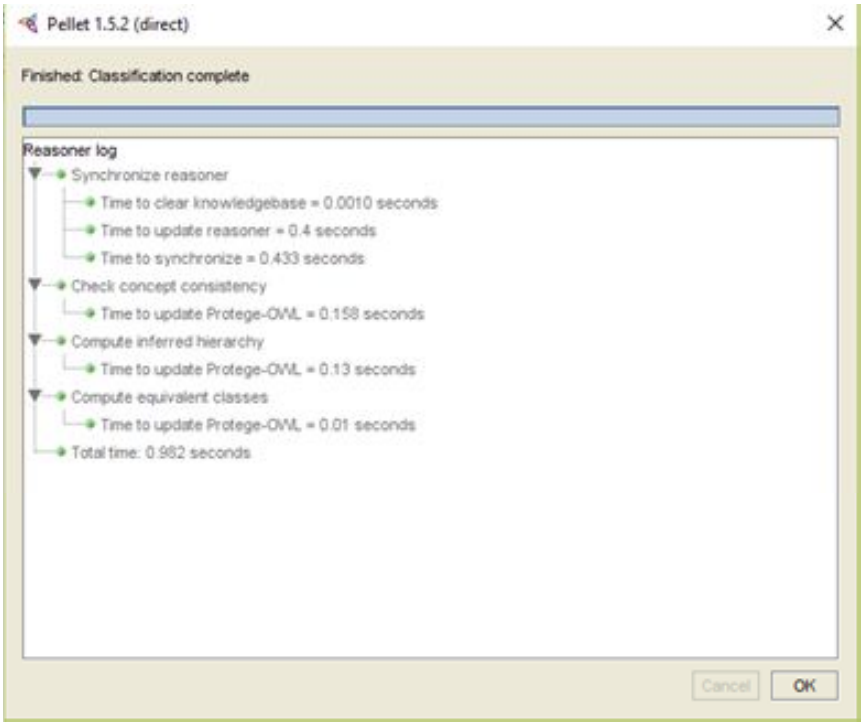


Figura 20 – Tela de Saída de Validação de Consistência do Pellet

podendo ser implementado em projetos baseados em RDF e OWL. O Racer se baseia na representação do conhecimento que implementa um cálculo *Tableau* otimizado usado para uma Lógica Descritiva expressiva. A Figura 21 apresenta a tela de instanciação do Racer.

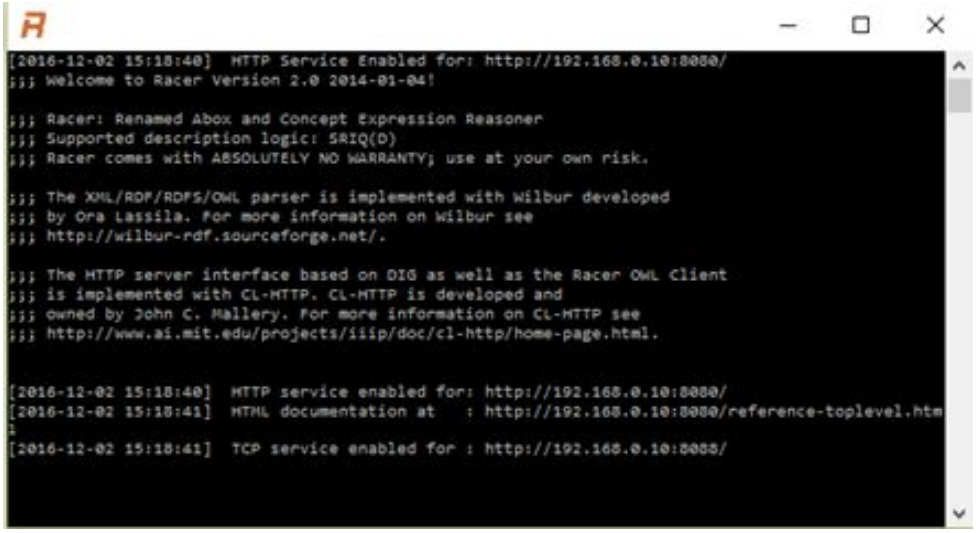


Figura 21 – Tela de Instanciação do Servidor do Racer

Feito isso, é necessário informar ao Protégé que será utilizado um motor de inferência externo. Esta escolha é feita conforme apresentado na Figura 22.

Assim, a comunicação entre o Protégé e o Racer já é estabelecida automaticamente para

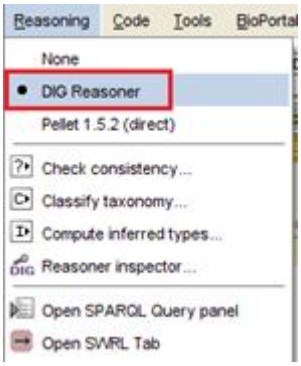


Figura 22 – Seleção do DIG Reasoner

fazer as validações, ficando o Racer pronto para analisar a consistência na estrutura de classes da ontologia.

A Figura 23 ilustra a tela de saída do motor de inferência, que mostra que o Racer validou a Ontologia de Ameaça Interna e não encontrou problemas em suas validações, ou seja, assim como o Pellet, o Racer provou que a ontologia está apta a ser utilizada pelas aplicações que requeiram os serviços providos por ela.

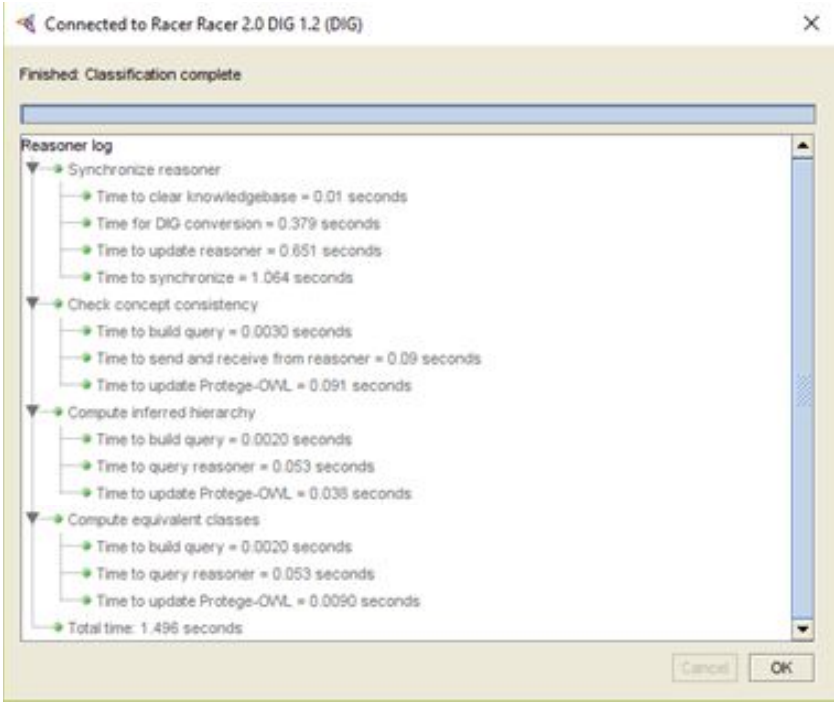


Figura 23 – Tela de Saída do Racer

A partir de um conjunto de incidentes reais de ameaça interna originados da base de dados MERIT foi possível criar uma ontologia que represente estas atividades mal-intencionadas; que pode ser utilizada em aplicações reais. Nesse caso, o ideal é que o conhecimento expresso nela seja sempre atualizado a cada novo incidente. Assim, estes casos reais poderão ser compartilhados entre todas as organizações que utilizam esta

ontologia sem que nenhum dado confidencial seja divulgado.

A ontologia foi submetida aos motores de inferência Pellet e Racer que analisaram sua consistência interna, consistência dos conceitos, hierarquia das classes e existência de classes equivalentes. Isso mostrou que ela não apresenta problemas de consistência e, portanto, está pronta para ser utilizada e compartilhada entre sistemas de informação de organizações que entendam que a segurança da informação é um tema a ser tratado.

Após a realização de alguns ciclos de teste, os resultados mostraram que o tempo de execução do Pellet foi, em média, 52% mais rápido que o Racer, apesar de ambos terem indicado a consistência da ontologia.

4.6 Pontos de Atenção

Esta seção apresenta categorias de pontos de atenção que foram detectados ao longo do desenvolvimento deste trabalho de pesquisa e podem servir de guia para futuros pesquisadores.

- **Divisão**:
  - Delimitação das classes e atributos que estão sendo representados; e,
  - Escolha dos elementos que possuem um valor agregado maior; ou seja, distinção entre as classes e atributos mais relevantes.
- **Granularidade**:
  - Definição do grau de detalhamento que o domínio deverá ter; e,
  - Critério de tratamento do limite de ramificações.
- **Escopo**:
  - Tipo de conhecimento a ser representado; e,
  - Fronteiras do conhecimento do domínio.
- **Validação**:
  - Tipo de modelagem que será utilizada;
  - Formas de detectar aspectos importantes que foram esquecidos;
  - Escolha da abordagem de avaliação da qualidade da ontologia; e,
  - Escolha dos motores de inferência para assegurar consistência.

4.7 Aplicabilidade do Uso de Ontologias

O desenvolvimento da ontologia de ameaça interna permitiu encontrar indícios relevantes de que a utilização de uma ontologia pode pode ser proveitosa em diversas áreas da Ciência da Computação e ocorrer por diferentes motivos ou necessidades. Alguns destes indícios e razões são listados a seguir:

1. O desenvolvimento da ontologia de ameaça interna forneceu um vocabulário padronizado, sustentado por uma completa conceitualização dos termos, evitando interpretações equivocadas e contribuindo para uma maior confiabilidade da representação do conhecimento sobre incidentes;

2. O resultado final permite que seu conteúdo suporte a modelagem adequada para compartilhar o conhecimento do domínio de segurança da informação, deixando-o acessível para outras empresas que tenham interesse em desenvolver ou ampliar aplicações dentro do mesmo contexto. Assim, a ontologia de ameaça interna, uma vez compartilhada, permitiria ser expandida para tratar de outras questões de segurança, tais como autorização e autenticação de usuários em uma rede segura; sem a necessidade de refazer uma análise de seu domínio;

3. A descrição do conhecimento é feita de forma exata, ao contrário das linguagens naturais em que as palavras podem ter a semântica diferente conforme o seu contexto; e a interpretação poderia variar de pessoa para pessoa. Entretanto, uma vez que a ontologia permite haver uma conceitualização comum entre elas, então a possibilidade de um mal entendido é reduzida drasticamente; e,

4. A modelagem de requisitos – sejam eles de negócio, funcionais ou não funcionais –, usando ontologias permite que sejam lançadas as bases de *frameworks* de desenvolvimento de aplicações intercambiáveis que podem ser consumidas por arquiteturas de infra-estrutura que utilizem qualquer protocolo.

Além disso, deve-se ressaltar que a utilização de ontologias em outras áreas da Ciência da Computação tais como Recuperação de Informações, Bibliotecas digitais, *Web* semântica, Gestão de conhecimento, Processamento da linguagem natural, Comércio eletrônico, Sistemas multiagentes e documentação de requisitos de aplicações distribuídas.

5 Conclusão

Devido à crescente necessidade de integração de conhecimento entre os ecossistemas virtuais das organizações, os desafios vindouros que as organizações enfrentarão certamente estarão relacionados com o enfrentamento de problemas de segurança externa e interna ao seu ambiente.

Dessa forma, quando são disponibilizados mecanismos adicionais para facilitar e agilizar a integração das informações de forma a maximizar parâmetros de segurança interna, as organizações – sejam elas públicas ou privadas –, passam a contar com uma ferramenta adicional de melhoria de sua capacidade operacional e de resposta às exigências do mercado.

Após escolher o domínio de aplicação que este trabalho explorou, o desenvolvimento da ontologia de ameaça interna forneceu elementos relevantes para que o uso ostensivo de componentes ontológicos seja incentivado em ambientes em que o desenvolvimento de sistemas seja crucial para o negócio.

O desenvolvimento da ontologia de ameaça interna mostrou que o uso de vocabulário padronizado, baseado numa estrutura conceitual que evita interpretações ambíguas contribui para a criação de bases de conhecimento confiáveis e verificáveis formalmente mediante o uso de motores de inferência.

A verificabilidade formal é essencial para que organizações e aplicações distribuídas possam modelar adequadamente o conhecimento a ser compartilhado sem abrir mão de suas especificidades, ao mesmo tempo em que usufruiu de um núcleo comum de interesse e assegura a confidencialidade de suas informações. Essas propriedades inerente às ontologias, permite, por exemplo, que o domínio de incidentes de segurança interna seja expandido para tratar de outras questões de segurança, tais como autorização e autenticação de usuários em uma rede segura; sem a necessidade de refazer a totalidade da análise de domínio.

Como o desenvolvimento de ontologias pode ser feito com base em processos padronizados e como a representatividade não ambígua de conhecimento é uma premissa essencial, isso cria as bases necessárias para que mecanismos de pesquisa robustos sejam implementados para que respostas rápidas e assertivas sejam dadas com base no conhecimento formalmente representado.

Ciente e confiante de que a utilização de ontologias na área de sistemas distribuídos tem um horizonte amplo, as próximas seções deste capítulo apresentam para os próximos pesquisadores, os desafios encontrados, as ameaças à validade da pesquisa e algumas

indicações de trabalhos futuros.

5.1 Desafios

A criação de uma ontologia a partir de um conjunto organizado, ou semi-organizado, de dados, se torna problemática por exigir esforço considerável de entendimento do domínio que está tentando ser formalmente representado, já que o conhecimento adequado demanda profissionais especializados.

Embora existam ferramentas que auxiliem neste processo, ainda é tarefa dos especialistas selecionar os dados e relacionar os termos mais relevantes e suas relações. Por fim, é necessário revisar a ontologia gerada, procurando por erros ou ambiguidades e submetê-la a um processo formal de verificação de consistência.

Por ser uma tarefa trabalhosa, se o pesquisador não se preocupa em adotar uma metodologia adequada, partindo direto para a implementação antes adquirir conhecimento sobre o domínio, isso tem o potencial de gerar os seguintes problemas:

1. O código da implementação acaba descrevendo os modelos conceituais da ontologia;
2. Baixa reusabilidade, pois a estruturação da ontologia e as decisões de projeto ficam implícitas no código;
3. A passagem da aquisição de conhecimento para a implementação ocorre de maneira repentina, gerando dificuldade para o desenvolvimento de ontologias mais complexas; e,
4. A linguagem escolhida pode limitar a capacidade de descrição conceitual do domínio da ontologia.

Dessa maneira, o conhecimento prévio do domínio é essencial para que a ontologia desenvolvida possa ser utilizada em aplicações reais.

5.2 Trabalhos Futuros

O desenvolvimento da ontologia de ameça interna se mostrou promissora e algumas indicações de trabalhos futuros são citadas a seguir:

1. Integração da ontologia desenvolvida em um ambiente de sistemas distribuído de tal forma que estes sistemas possam compartilhar o conhecimento disponibilizado pela ontologia de ameação interna; e,

2. Desenvolvimento de uma interface e de uma linguagem de consulta para busca de conhecimento na ontologia.

5.3 Considerações Finais

O objetivo do trabalho foi atingido porque foi criada uma ontologia de representação e compartilhamento de conhecimento que tem por base um conjunto organizado de informações sobre casos reais de incidentes relacionados à segurança da informação. Ela também pode ser utilizada como fundamento para a criação e manutenção de sistemas de informação que compartilhem dados de ameaças internas à segurança.

Além disso, a ontologia foi modelada a partir de uma base de dados de casos reais de incidentes de segurança interna; ela foi validada por motores de inferência quanto à sua consistência interna e apresentou indicações e exemplos de aplicabilidade da ontologia no domínio de sistemas distribuídos.

Referências

ABBURU, S. A Survey on Ontology Reasoners and Comparison. *International Journal of Computer Applications*, v. 57, n. 17, p. 33–39, 2012. Citado na página 33.

ABDOLI, F.; KAHANI, M. Ontology-based distributed intrusion detection system. *2009 14th International CSI Computer Conference*, p. 65–70, 2009. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5349372>. Citado na página 16.

ALLEN, G. A.; MARCH, S. T. A critical assessment of the Bunge-Wand-Weber ontology for conceptual modeling. In: *16th Workshop on Information Technologies and Systems, WITS 2006*. [s.n.], 2006. p. 25–30. ISBN 1556-5068. ISSN 1556-5068. Disponível em: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84864949167&partnerID=tZOtx3y1>. Citado na página 22.

ALLEN, J. CERT System and Network Security Practices. *Carnegie Mellon University. Software Engineering Institute. CERT Coordination Center*, p. 11, 2001. Disponível em: <http://repository.mdp.ac.id/ebook/library-ref-eng/ref-eng-1/network/network-security/NCISSE_practices.pdf>. Citado 2 vezes nas páginas 14 e 41.

ATKIN, A. "Peirce ' s Theory of Signs". *The Stanford Encyclopedia of Philosophy*, v. 13, n. 4, p. 1–17, 2010. Disponível em: <http://plato.stanford.edu/archives/sum2013/entries/peirce-semiotics/>. Citado na página 21.

BAKHSHANDEH, M. et al. A modular ontology for the enterprise architecture domain. In: *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOC*. [S.l.: s.n.], 2013. p. 5–12. ISBN 978-1-4799-3048-7. ISSN 15417719. Citado na página 39.

BARCELLOS, M. P.; De Almeida Falbo, R. Using a foundational ontology for reengineering a Software Enterprise Ontology. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [S.l.: s.n.], 2009. v. 5833 LNCS, p. 179–188. ISBN 364204946X. ISSN 03029743. Citado na página 37.

BEJI, S.; El Kadhi, N. Security ontology proposal for mobile applications. In: *Proceedings - IEEE International Conference on Mobile Data Management*. [S.l.: s.n.], 2009. p. 580–587. ISBN 9780769536507. ISSN 15516245. Citado na página 37.

BERNERS-LEE, T.; FISCHETTI, M. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. 1st. ed. [S.l.]: Harper San Francisco, 1999. ISBN 0062515861. Citado na página 15.

BEYER, C. *Edmund Husserl*. 2013. Disponível em: <http://plato.stanford.edu/archives/win2013/entries/husserl>. Citado na página 23.

BOBILLO, F.; DELGADO, M.; GÓMEZ-ROMERO, J. DeLorean: A reasoner for fuzzy OWL 2. *Expert Systems with Applications*, v. 39, n. 1, p. 258–272, 2012. ISSN 09574174. Citado na página 34.

BROWN, J. S.; DUGUID, P. Organizing Knowledge. *California Management Review*, v. 40, n. 3, p. 90–111, 1998. ISSN 15241734. Citado 2 vezes nas páginas 42 e 43.

BUCCELLA, A.; CECHICH, A.; BRISABOA, N. R. An Ontology Approach to Data Integration. *Journal of Computer Science & Technology*, v. 3, n. 2, p. 62–68, 2003. Citado na página 15.

CAPPELLI, D.; MOORE, A.; TRZECIAK, R. *The CERT Guide to Insider threats*. [S.l.: s.n.], 2012. v. 1. 1829–1841 p. ISBN 9780321812575. Citado 4 vezes nas páginas 14, 41, 42 e 43.

CHANDY, K. M. Distributed Snapshots: Determining Global States of Distributed Systems. *ACM Transactions on Computer Systems*, v. 3, n. 1, p. 63–75, 1985. ISSN 07342071. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.119.7694>. Citado na página 15.

CHEN, C.; HAARSLEV, V.; WANG, J. LAS: Extending racer by a large abox store. In: *CEUR Workshop Proceedings*. [S.l.: s.n.], 2005. v. 147. ISBN 16130073 (ISSN). ISSN 16130073. Citado 2 vezes nas páginas 35 e 53.

CHEN, Y. J.; CHEN, Y. M.; CHU, H. C. Development of a mechanism for ontology-based product lifecycle knowledge integration. *Expert Systems with Applications*, v. 36, n. 2 PART 2, p. 2759–2779, 2009. ISSN 09574174. Citado na página 15.

CHEN, Y. J.; CHEN, Y. M.; SU, Y. S. An ontology-based distributed case-based reasoning for virtual enterprises. In: *Proceedings of the International Conference on Complex, Intelligent and Software Intensive Systems, CISIS 2009*. [S.l.: s.n.], 2009. p. 128–135. ISBN 9780769535753. ISSN 0218-1940. Citado na página 14.

CHOI, N.; SONG, I.-Y.; HAN, H. A Survey on Ontology Mapping Namyoun Choi, Il-Yeol Song, and Hyoil Han College of Information Science and Technology Drexel University, Philadelphia, PA 19014. *SIGMOD Record*, v. 35, n. 3, p. 34–41, 2006. ISSN 01635808. Citado na página 14.

CHRUDZIMSKI, A. Objects, Properties and States of Affairs. An Aristotelian Ontology of Truth Making. *Axiomathes*, 2002. ISSN 11221151. Citado na página 22.

COMPANY, E. B. *Ontology*. [S.l.: s.n.], 2014. Citado na página 21.

CORAZZON, R. Notes on the history of ontology, descriptive and formal ontology. 2013. Disponível em: <http://www.ontology.co/>. Citado na página 23.

CORCHO, O.; FERNANDEZ-LOPEZ, M.; GOMEZ-PEREZ, A. Ontological engineering: Principles, methods, tools and languages. In: *Ontologies for Software Engineering and Software Technology*. Berlin, Alemania: Springer-Verlag, 2006. p. 1–48. Ontology Engineering Group ? OEG. Disponível em: <http://oa.upm.es/5457/>. Citado 2 vezes nas páginas 15 e 23.

COSTA, A. C. M. *Modelagem do Processo de Gerenciamento de Nível de Serviço ITIL em uma Plataforma de Serviços Sensíveis a Contexto*. Tese (Doutorado) — Universidade Federal do Espírito Santo, Centro Tecnológico, Departamento de Informática, Vitoria, 2008. Citado 6 vezes nas páginas 26, 27, 29, 33, 38 e 46.

D'AQUIN, M.; NOY, N. F. *Where to publish and find ontologies? A survey of ontology libraries*. 2012. 96–111 p. Citado na página 21.

De Nicola, A.; MISSIKOFF, M.; NAVIGLI, R. A software engineering approach to ontology building. *Information Systems*, v. 34, n. 2, p. 258–275, 2009. ISSN 03064379. Citado na página 15.

DING, Y.; FENSEL, D. Ontology Library Systems : The key to successful Ontology Re-use. *Proceedings of SWWS*, p. 93–112, 2001. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.2159&rep=rep1&type=pdf>. Citado na página 16.

EKELHART, A. et al. Security Ontology : Simulating Threats to Corporate Assets. *Proceedings of the 2nd Intl. Conf. on Information Systems Security (ICISS)*, p. 249–259, 2006. Citado na página 38.

FALBO, r. d. A. Sabio: Systematic approach for building ontologies. *Ontology and Conceptual Modeling Research Group (NEMO)*, 1997. Citado 3 vezes nas páginas 17, 25 e 26.

FARINELLI, F.; ALMEIDA, M. Interoperabilidade semntica em sistemas de informao de sade por meio de ontologias formais e informais: um estudo da norma openehr. *Conferncia Internacional Acesso Aberto, Preservao Digital, Interoperabilidade, Visibilidade e Dados Cientficos*, Universidade Federal de Minas Gerais, 2013. Citado na página 16.

FARQUHAR, A.; FIKES, R.; RICE, J. The Ontolingua Server: a tool for collaborative ontology construction. *International Journal of Human-Computer Studies*, v. 46, n. 6, p. 707–727, 1997. ISSN 1071-5819. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1071581996901214>. Citado na página 15.

FIKES, R.; FARQUHAR, a. Distributed repositories of highly expressive reusable ontologies. *IEEE Intelligent Systems and their Applications*, v. 14, p. 1–14, 1999. ISSN 1094-7167. Citado na página 15.

FITHEN, K.; FRASER, B. CERT incident response and the Internet. *Association for Computing Machinery. Communications of the ACM*, v. 37, n. 8, p. 108, 1994. ISSN 00010782. Citado na página 42.

FLAHIVE, A. et al. A distributed ontology framework in the semantic grid environment. In: *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*. [S.l.: s.n.], 2005. v. 2, p. 193–196. ISBN 0769522491. ISSN 1550445X. Citado na página 16.

FRAPPAOLO, C. Implicit knowledge. *Knowledge Management Research Practice*, v. 6, n. 2008, p. 23–25, 2008. ISSN 1477-8238. Citado na página 42.

FU, G.; COHN, A. *Formal Ontology in Information Systems*. [S.l.: s.n.], 2008. 297–310 p. ISSN 09226389. ISBN 9781586039233. Citado na página 15.

GOMEZ-PREREZ, A. Ontology Evaluation. *Handbook on Ontologies*, p. 293–313, 2004. ISSN 10744770. Disponível em: <http://dx.doi.org/10.1007/978-3-540-92673-3_13>. Citado na página 21.

GREGOR, D. et al. A methodology for structured ontology construction applied to intelligent transportation systems. *Computer Standards and Interfaces*, v. 47, p. 108–119, 2016. ISSN 09205489. Citado na página 16.

GRUBER, T. R. A translation approach to portable ontology specifications. *Knowledge Acquisition*, v. 5, n. 2, p. 199–220, 1993. ISSN 1042-8143. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1042814383710083>. Citado na página 23.

GRUNINGER, M.; LEE, J. Ontology Applications and Design. *Communications of the ACM*, v. 45, n. 2, p. 39–41, 2002. ISSN 0001-0782. Citado na página 22.

GUIZZARDI, G. *Foundations for Structural Conceptual*. Centre for Telematics and Information Technology, University of Twente, 2005. v. 015. 441 p. (Telematica Instituut Fundamental Research Series, CTIT Ph.D.-thesis series No. 05-74). ISBN 9075176813. Disponível em: <http://doc.utwente.nl/50826>. Citado 2 vezes nas páginas 17 e 27.

GUIZZARDI, G. Ontological foundations for structural conceptual models. In: *CTIT PH.D. - Centre for Telematics and Information Technology*. Enschede: [s.n.], 2005. Disponível em: <http://doc.utwente.nl/50826/>. Citado na página 21.

GUIZZARDI, R. F. G.; GUIZZARDI, R. A importância de ontologias de fundamentação para a engenharia de ontologias de domínio: o caso do domínio de processos de software. *IEEE Latin America Transactions*, v. 6, n. 3, 2008. Citado 5 vezes nas páginas 17, 27, 28, 29 e 33.

HAARSLEV, V.; MÖLLER, R. Description of the RACER System and its Applications. In: *International Workshop on Description Logics*. [S.l.: s.n.], 2001. v. 1, p. 132–142. Citado 3 vezes nas páginas 34, 35 e 53.

HAARSLEV, V.; MÜLLER, R. RACER System Description. *1st International Joint Conference on Automated Reasoning*, v. 2083, p. 701–705, 2001. ISSN 03029743. Citado 3 vezes nas páginas 34, 35 e 53.

HACKING, I. *Historical Ontology*. [S.l.: s.n.], 2007. v. 116. 136–138 p. ISSN 0031-8108. ISBN 067400616X. Citado na página 21.

HARRISON, R.; CHAN, C. W. Distributed ontology management system. In: *Canadian Conference on Electrical and Computer Engineering*. [S.l.: s.n.], 2005. v. 2005, p. 661–664. ISBN 0-7803-8885-2. ISSN 08407789. Citado 2 vezes nas páginas 39 e 41.

HARVEY, C. C. CERT - Computer Emergency Response Team. *Computer Networks ISDN Systems*, v. 23, n. 1-3, p. 167, 1991. ISSN 01697552. Citado na página 43.

HERZOG, A.; SHAHMEHRI, N.; DUMA, C. An Ontology of Information Security. *International Journal of Information Security and Privacy*, v. 1, n. 4, p. 1–23, 2007. ISSN 1930-1650. Citado 2 vezes nas páginas 36 e 37.

ILIE, L.; MOLNAR, M. RACER: Rapid and accurate correction of errors in reads. *Bioinformatics*, v. 29, n. 19, p. 2490–2493, 2013. ISSN 14602059. Citado 2 vezes nas páginas 35 e 53.

JONG, T. de; FERGUSON-HESSLER, M. G. *Types and qualities of knowledge*. 1996. 105–113 p. Citado na página 42.

KALFOGLOU, Y.; SCHORLEMMER, M. Ontology mapping: the state of the art. *The knowledge engineering ...*, v. 18, n. 1, p. 1–31, 2003. ISSN 02698889. Citado na página 41.

KANG, D. et al. An ontology-based Enterprise Architecture. *Expert Systems with Applications*, v. 37, n. 2, p. 1456–1464, 2010. ISSN 09574174. Citado na página 39.

KHAN, J. A.; KUMAR, S. OWL, RDF, RDFS inference derivation using Jena semantic framework pellet reasoner. In: *2014 International Conference on Advances in Engineering and Technology Research, ICAETR 2014*. [S.l.: s.n.], 2014. ISBN 9781479963935. ISSN 2347-9337. Citado 2 vezes nas páginas 34 e 53.

KIM, K.-Y.; MANLEY, D. G.; YANG, H. Ontology-based assembly design and information sharing for collaborative product development. *Computer-Aided Design*, v. 38, n. 12, p. 1233–1250, 2006. ISSN 00104485. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S0010448506001680>. Citado na página 23.

LAWSON, T. A Conception of Ontology. *The Cambridge Social Ontology*, p. 1–24, 2004. Citado na página 21.

LIU, K.; HOGAN, W. R.; CROWLEY, R. S. *Natural Language Processing methods and systems for biomedical ontology learning*. 2011. 163–179 p. Citado na página 41.

MAEDCHE, A.; STAAB, S. Ontology Learning for. *IEEE Intelligent Systems*, p. 72–79, 2001. ISSN 15411672. Citado na página 21.

MIZOGUCHI, R. Tutorial on ontological engineering Part 2: Ontology development, tools and languages. *New Generation Computing*, v. 22, n. 1, p. 61–96, 2004. ISSN 0288-3635. Citado na página 41.

NECHES, R. et al. Enabling technology for knowledge sharing. *AI Mag.*, American Association for Artificial Intelligence, Menlo Park, CA, USA, v. 12, n. 3, p. 36–56, set. 1991. ISSN 0738-4602. Disponível em: <http://dl.acm.org/citation.cfm?id=123768.123775>. Citado 2 vezes nas páginas 15 e 24.

PARSIA, B.; SIRIN, E. Pellet : An OWL DL Reasoner. *Artificial Intelligence*, p. 1–2, 2000. Citado na página 35.

PEREIRA, J. H. D. S.; KOFUJI, S. T.; ROSA, P. F. Distributed systems ontology. In: *3rd International Conference on New Technologies, Mobility and Security, NTMS 2009*. [S.l.: s.n.], 2009. ISBN 9781424462735. Citado na página 14.

PEREIRA, J. H. S. et al. Layers Optimization Proposal in a Post-IP Network. *International Journal On Advances in Networks and Services*, 2011. Citado na página 14.

SAúDE, M. da. Regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do sistema Único de saúde, nos níveis municipal, distrital, estadual e federal, e para os sistemas privados e do setor de saúde suplementar. *Ministério da Saúde*, n. Portaria 2073, 2011. Disponível em: <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html>. Citado na página 16.

SCHOLAR, M. D. et al. A Survey on Ontology Mapping. *SIGMOD Record*, v. 35, n. 3, p. 34–41, 2006. ISSN 01635808. Disponível em: <http://mds.marshall.edu/wdcs_faculty>. Citado na página 15.

SILVA, D. R. P. da; STEIN, L. M. Segurança da informação: uma reflexão sobre o componente humano. *Ciências Cognição 2007;*, v. 10, 2007. Citado 4 vezes nas páginas 14, 18, 19 e 20.

SIRIN, E. et al. Pellet: A practical OWL-DL reasoner. *Web Semantics*, v. 5, n. 2, p. 51–53, 2007. ISSN 15708268. Citado 2 vezes nas páginas 34 e 53.

SMITH, B. Ontology. *Blackwell Guide to the Philosophy of Computing and Information*, n. 1964, p. 155–166, 2003. ISSN 1943-4723. Citado 2 vezes nas páginas 21 e 22.

SMITH, B. *An Introduction to Ontology: From Aristotle to the Universal Core*. 2009. Citado na página 21.

STAAB, S. et al. Knowledge processes and ontologies. *IEEE Intelligent Systems and Their Applications*, v. 16, n. 1, p. 26–34, 2001. ISSN 10947167. Citado 2 vezes nas páginas 23 e 24.

SUN, Y.-C. *The development of an artificially intuitive reasoner.* 2011. 7513 p. Citado na página 16.

TAFAZZOLI, T.; SADJADI, S. H. Malware Fuzzy Ontology for Semantic Web. *IJCSNS International Journal of Computer Science and Network Security*, v. 8, n. 7, p. 153–161, 2008. Citado 2 vezes nas páginas 16 e 42.

TOIT, a. B. du. Logic and Ontology. *Philosophical Papers*, v. 3, n. 1, p. 17–45, 1974. ISSN 0556-8641. Citado 2 vezes nas páginas 21 e 22.

USCHOLD, M. et al. Ontology reuse and application. *Formal Ontology in Information Systems*, v. 179, n. January 2000, p. 192, 1998. Disponível em: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Ontology+Reuse+and+Application#0>. Citado na página 21.

VOROBIEV, A.; HAN, J. Security attack ontology for Web services. In: *2006 2nd International Conference on Semantics Knowledge and Grid, SKG*. [S.l.: s.n.], 2006. ISBN 0769532055. Citado na página 36.

WANG, W. et al. A comprehensive ontology for knowledge representation in the internet of things. In: *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*. [S.l.: s.n.], 2012. p. 1793–1798. ISBN 9780769547459. ISSN 2324-898X. Citado na página 40.

WEST-BROWN, M. J. et al. Handbook for Computer Security Incident Response Teams (CSIRTs). *SEI Digital Library*, n. April, p. 223, 2003. Disponível em: <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305>. Citado 3 vezes nas páginas 14, 41 e 42.

XU, B.; WU, J.; CAI, H. Business process driven ontology discovery method from distributed data environment. In: *Proceedings - 2011 8th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2011*. [S.l.: s.n.], 2011. v. 2, p. 1246–1251. ISBN 9781612841816. Citado na página 15.

ZABLITH, F. Dynamic ontology evolution. *Work*, 2008. Disponível em: <http://oro.open.ac.uk/23527/>. Citado na página 34.

ZÚÑIGA, G. Ontology: its transformation from philosophy to information systems. *Formal Ontology in Information Systems. IOS Press*, p. 187–197, 2001. ISSN 00223263. Disponível em: <http://dl.acm.org/citation.cfm?id=505187>. Citado na página 33.