UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

InfoSecRM: UMA ONTOLOGIA PARA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÂO

ÉDER SOUZA GUALBERTO

ORIENTADOR: RAFAEL TIMÓTEO DE SOUSA JUNIOR

DISSERTAÇÃO DE MESTRADO EM
ENGENHARIA ELÉTRICA

PUBLICAÇÃO: MEE.DM - 459 D/11

BRASÍLIA/DF: DEZEMBRO - 2011.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

InfoSecRM: UMA ONTOLOGIA PARA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÂO

ÉDER SOUZA GUALBERTO

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM ENGENHARIA ELÉTRICA.

APROVADA POR:

Prof. RAFAEL TIMÓTEO DE SOUSA JUNIOR, PhD. (ENE-UnB)
(Orientador)

Prof. , PhD. (ENE-UnB)
(Examinador Interno)

Prof. , DR. (CID-UnB)
(Examinador Externo)

BRASÍLIA/DF, 12 DE DEZEMBRO DE 2011.

FICHA CATALOGRÁFICA

GUALBERTO, ÉDER SOUZA
InfoSecRM: Uma ontologia para gestão de riscos de segurança da informação.
[Distrito Federal] 2011.
xvii, 154p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2011).
Dissertação de Mestrado - Universidade de Brasília.
Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.

1. Segurança da Informação	2. Ontologia
3. Gestão de Riscos de Segurança da Informação	4. Conceitualização
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

GUALBERTO, E. S. (2011). InfoSecRM: Uma ontologia para Gestão de Riscos de Segurança da Informação. Dissertação de Mestrado em Engenharia Elétrica, Publicação MEE.DM - 459 D/11, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 154p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Éder Souza Gualberto.

TÍTULO DA DISSERTAÇÃO DE MESTRADO: InfoSecRM: Uma ontologia para Gestão de Riscos de Segurança da Informação.

GRAU / ANO: Mestre / 2011

Éder Souza Gualberto
Qnm 40 conjunto F2 casa 46, M-Norte
72.146-136 Taguatinga - DF - Brasil.

DEDICATÓRIA

Ao meu Deus, por todo majestoso
amor que me faz seguir todos os dias.
A Ele toda honra, glória e louvor.

Aos meus pais, por me guiar sempre
e fazer de mim o homem que sou.

Ao meu irmão Ádison, pelo
amor fraterno e amizade.

À Fernanda, por todo amor,
apoio e carinho presentes em cada
minuto das minhas vitórias e derrotas. Te amo.

Aos amigos e colegas, em especial ao Jurami,
Emílio, Fernando, Bruno, Thiander, Rodrigo,
André Gustavo, Diego, Cesar, Gabriel, Fuji e Luiz,
que, na minha vida como um todo, seja no trabalho,
nas atividades acadêmicas ou nos momentos de lazer
e descontração, fazem dela algo especial.

AGRADECIMENTOS

Agradeço ao professor Rafael por suas importantes orientações, auxílios, atenção e paciência ao longo deste trabalho.

Agradeço ao professor Cláudio e ao professor Jorge pelos auxílios, ensinamentos e conselhos sempre presentes em boa parte da minha vida acadêmica.

RESUMO

InfoSecRM: UMA ONTOLOGIA PARA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÂO

Autor: Éder Souza Gualberto

Orientador: RAFAEL TIMÓTEO DE SOUSA JUNIOR

Programa de Pós-graduação em Engenharia Elétrica

Brasília, dezembro de 2011

Gerenciar os riscos de segurança da informação a que uma organização está sujeita auxilia na implementação, monitoração e melhoria contínua de seus controles e ações de segurança da informação. Este tipo de processo de gestão de riscos utiliza informações de fontes variadas como dados sobre ativos e suas vulnerabilidades, logs de sistemas, decisões gerenciais etc. Assim, recursos que possam auxiliar na manipulação de informações deste complexo arcabouço são necessidades reais e relevantes a serem consideradas. Nesta dissertação, é apresentada uma ontologia como proposta de representação para formalizar, compartilhar, manipular e processar conceitos e informações relacionadas ao domínio de gestão de riscos de segurança da informação. São apresentadas as atividades realizadas para seu desenvolvimento, cujo processo guiou-se por três abordagens: metodologia Methontology, Método 101 e a metodologia proposta por Fox e Gruninger. Também são descritas as abordagens utilizadas para sua verificação (baseada em pré-requisitos que a ontologia deve alcançar e também comparando-a com outras ontologias do domínio relacionado) e validação (utilização da ontologia em um ambiente corporativo por especialistas do domínio e comparação com documentos de referência), que denotam a correta representação do domínio e a sua utilidade neste tipo de processo.

ABSTRACT

MULTISTAGE FILTRATION APPLIED TO THE TREATMENT OF ALGAL LADEN WATERS: EVALUATION OF OPERATIONAL CONDITIONS

Author: Éder Souza Gualberto

Supervisor: RAFAEL TIMÓTEO DE SOUSA JUNIOR

Programa de Pós-graduação em Engenharia Elétrica

Brasília, December of 2011

Managing information security risks of organizations assists in the implementation, monitoring and continuous improvement of their controls and information security actions. This type of risk management process uses information from various sources such as data about assets and their vulnerabilities, system logs, manager decisions. Thus, resources that can help in handling of this complex framework of information are real and relevant needs to be considered. In this thesis, an ontology is presented as a proposal to formalize representation, share, manipulate and process concepts and information related to the field of information security risk management. The activities for development are present, a process that was guided by three approaches: Methontology methodology, Method 101 and the methodology proposed by Fox and Grüninger. It also describes the approaches used for verification (based on ontology prerequisites that must be achieved and also comparing it with other related domain ontologies) and validation (using the ontology in a corporate environment by domain experts and comparison with documents reference), which denote the correct representation of the domain and its usefulness in this type of process.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

ABNT: Associação Brasileira de Normas Técnicas.

ABox: Assertional Box

COBIT: Control Objectives for Information and Related Technology

DAML: DARPA Agent Markup Language.

GRSI: Gestão de Riscos de Segurança da Informação.

GSI: Gestão de Segurança da Informação.

IEEE: Institute of Electrical and Electronics Engineers.

ISO: International Organization for Standardization.

NBR: Norma Brasileira.

OIL: Ontology Inference layer.

OWL: Web Ontology Language.

PDCA: Plan-Do-Check-Act.

POSIC: Política de Segurança da Informação e Comunicações

RDF: Resource Description Framework.

SGSI: Sistema de Gestão de Segurança da Informação.

SPARQL: SPARQL Query Language for RDF.

TBox: Terminological Box

TI: Tecnologia da Informação

URI: Uniform Resource Identifier.

XML: Extensible Markup Language

W3C: World Wide Web Consortium.

Web: World Wide Web.

1 INTRODUÇÃO

Promover e gerir a segurança da informação tem sido um grande desafio para as organizações, visto a alta criticidade deste tipo de ativo e dos ativos de suporte relacionados, e as constantes ameaças que os cercam. Neste sentido, considerando que esta prática vai além de questões inerentemente relacionadas à tecnologia da informação (TI), ações gerenciais que baseiam-se em processos, tecnologias e pessoas são importantíssimas para a efetividade da segurança da informação.

Assim, a questão da gestão da segurança da informação (GSI) em ambientes corporativos, públicos e privados, tem sido bastante discutida, prova disso foram as publicações das normas da família ISO 27000 que são, conforme afirmado em ISO (2009), o estado da arte internacional nesta área. Estas normas definem um modelo para sistemas de gerenciamento de segurança da informação (SGSI) com vistas a proteger os ativos de informação e permitir à organização continuar realizando sua missão.

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

Ocorre no entanto que a implementação e manutenção de um processo de GRSI opera sobre uma grande quantidade de conceitos. Conceitos estes que manifestam muitos relacionamentos entre si, tornando seu entendimento e aprendizado, por parte dos colaboradores e intervenientes (*stakeholders*), fator crítico à aquisição e ao compartilhamento de conhecimento relativo à segurança da informação da organização. Além disso a GRSI atua sobre uma grande quantidade de informações e a utilização de mecanismos que permitam a sua manipulação de forma eficiente e eficaz são extremamente relevantes, conforme indica AS/NZS (2004).

Neste cenário, a utilização de ontologias permite, ao mesmo tempo, a representação

das relações semânticas entre os conceitos envolvidos em um processo de GRSI e de GSI, e a criação e estruturação de uma base de conhecimento a respeito da segurança da informação na organização, além de possibilitar a comunicação e interoperabilidade entre agentes de software e agentes humanos sobre uma mesma representação de dados. As ontologias, consoante ao definido em Gruber (1995), especificam, formalmente e de maneira explícita, um domínio de conhecimento, ou seja, modelam uma abstração de um domínio por meio de conceitos, suas respectivas propriedades e restrições associadas.

1.1 Contexto e Motivação

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

Uma ontologia, indica Guarino (1998), refere-se a uma teoria lógica (representada, por exemplo, por um artefato computacional), definida com base em um vocabulário formal e aderente a um compromisso (objetivo), utilizada para descrever uma conceitualização particular do mundo (tal como um domínio por exemplo).

Em Donner (2003) e em Andersson e Hallberg (2003), são elencados aspectos das ontologias que as caracterizam como uma abordagem facilitadora na concepção de abstrações para os domínios de segurança da informação e de sua gestão: a versatilidade possibilitada à descrição dos conceitos, a dinamicidade estrutural permitida pela forma com que os conceitos são dispostos (relações entre conceitos e de herança para representar especializações por exemplo) e a possibilidade de instanciação da estrutura modelada (que permite a sua utilização como base de conhecimento).

A utilização e os benefícios que abordagens ontológicas podem trazer para o campo da segurança da informação, principalmente com relação ao formalismo na conceitualização, compartilhamento e aquisição de conhecimento, são discutidos em Raskin et al. (2001). Em Martimiano (2006) e em Andersson e Hallberg (2003), são apresentadas abordagens ontológicas desenvolvidas para auxiliar a tomada de decisão, em nível gerencial, com relação a incidentes de segurança. Propor uma ontologia que representasse

o domínio de segurança da informação e possibilitasse o desenvolvimento de ontologias de níveis mais específicos foi o trabalho realizado por Azevedo et al. (2008). Além destes, em Chiang, Kouh e Chang (2009), é apresentada uma proposta que combina ontologias relacionadas à segurança da informação com uma ontologia de gestão de riscos genérica, com vistas a facilitar a implantação dos controles e melhores práticas propostos em ABNT (2006).

Diante o exposto, foi desenvolvida uma ontologia para gestão de riscos de segurança da informação denominada InfoSecRM. Esta ontologia, desenvolvida tendo como base o processo proposto na norma ISO 27005 (ABNT, 2008), caracteriza-se como uma ontologia de domínio, visto que dispõe dos conceitos básicos relacionados ao domínio de GRSI e de GSI. Por meio da utilização dessa, pode-se documentar e operar o processo de GRSI e subsidiar decisões gerenciais relacionadas à GSI.

1.2 Objetivos

Propor uma ontologia para a GRSI nos moldes do processo proposto na norma ISO 27005 de modo a favorecer a conceitualização do conhecimento de riscos de segurança da informação, e também o compartilhamento, a aquisição e o reuso das informações relacionadas em um SGSI é o objetivo central deste trabalho.

Assim, como objetivos específicos elencam-se os seguintes:

Estudar os principais elementos relacionados à segurança da informação (com ênfase na gestão de riscos de segurança da informação);

Estudar os principais elementos relacionados às ontologias (benefícios, tipos, linguagens, lógica de representação, metodologias de desenvolvimento e de avaliação).

Formalizar de maneira padronizada uma estrutura que represente informações relacionadas à segurança da informação tais como ativos, vulnerabilidades, ameaças, controles, riscos etc, bem como as próprias atividades de uma GRSI, com vistas a auxiliar a implementação deste processo em ambientes corporativos.

Analisar a utilização de ontologias como elemento facilitador na padronização, compartilhamento, reuso e aquisição/geração de conhecimento e informações sobre segurança da informação.

1.3 Organização do Trabalho

Esta dissertação está organizada em seis capítulos, descritos a seguir:

O capítulo 1 apresenta o contexto e a motivação deste trabalho, explicitando as características das informações relacionadas a segurança da informação e os benefícios que a utilização de formalismos para representação do conhecimento, como ontologias, podem trazer para este domínio. São apresentados os objetivos deste trabalho e é apresentado o conteúdo de cada um dos capítulos que compõem esta dissertação.

No capítulo 2, explicitam-se os princípios e conceitos relacionados à segurança da informação e sua gestão, além das normas da família ISO 27000. Uma ênfase maior é dada à descrição do processo de gestão de riscos de segurança da informação visto este ser o elemento central da ontologia desenvolvida.

Já o capítulo 3 aborda o contexto das ontologias, descreve as características de sua conceitualização e os elementos relacionados a esta. São apresentados algumas metodologias para o processo de engenharia de ontologias, os métodos e formalismos para este tipo de representação, além das ferramentas que podem auxiliar e automatizar as atividades e tarefas inerentes ao desenvolvimento deste constructo.

No capítulo 4 são descritas as atividades do processo de desenvolvimento da ontologia proposta por este trabalho. As principais idéias utilizadas para a concepção da InfoSecRM, os principais conceitos, as classes que os representam e seus respectivos relacionamentos são descritos com detalhes ilustrando o cenário de criação desta conceitualização.

As atividades de avaliação da InfoSecRM são apresentadas no capítulo 5. A avaliação foi dividida em verificação, que verifica a corretude da apresentação, e em validação, que verifica quanto foi representado do domínio e se este está conceitualização está de acordo com a realidade.

No capítulo 6, são discutidas as principais conclusões obtidas neste trabalho e as propostas de trabalhos futuros.

2 Segurança da Informação e Elementos Relacionados

Os sistemas de informação e, sobretudo, as informações relacionadas a estes caracterizam-se como ativos de grande criticidade para as organizações. Prover segurança a estes ativos e gerir as ações que garantam a manutenção efetiva desta segurança é essencial para o negócio destas. A segurança da informação diz respeito a proteção da informação contra ameaças que possam valer-se das vulnerabilidades deste ativo, preservando-a assim em suas propriedades quais sejam disponibilidade, integridade, confidencialidade e autenticidade, dentre outras.

É importante observar, no entanto, que a segurança da informação não se concentra exclusivamente sobre questões relacionadas à tecnologia da informação (TI), visto que a segurança que é proporcionada por meios tecnológicos não supre toda a demanda por segurança que este ativo apresenta, conforme afirma a norma ABNT NBR ISO/IEC 27002 - Código de Prática para a Gestão da Segurança da informação (ABNT, 2005). Esta, juntamente com a norma ABNT NBR ISO/IEC 27001 - Sistemas de Gestão de Segurança da informação (ABNT, 2006), que refere-se aos requisitos de sistemas de gestão de segurança da informação que devem ser implementados por uma organização; e com a norma ABNT NBR ISO/IEC 27005 - Gestão de Riscos de Segurança da informação (ABNT, 2008), que, como o próprio nome indica, é relativa ao processo de gestão de riscos de segurança da informação e das suas atividades; além do restante das normas da família ISO 27000; formam um grupo completo de controles contendo as melhores práticas para segurança da informação.

Estas normas versam acerca da importância da segurança da informação, seja ela inerente a organizações públicas ou privadas, concentrando indicações de requisitos e melhores práticas para sistemas de gestão de segurança da informação. Nelas está explícito que a gestão da segurança da informação não deve ser tratada apenas pela área de TI, mas por todas as áreas da organização, sobretudo pela alta administração. Esta abordagem, indica ABNT (2006), é condizente com os propósitos de governança corporativa, além de viabilizar a promoção da conscientização em segurança da informação, fazendo com que a cultura de segurança da informação seja parte das atividades de seus colaboradores.

Neste capítulo, são discutidos os principais tópicos relacionados à segurança da informação e a sua gestão, além de apresentar previamente os elementos e aspectos relacionados que têm grande influência sobre esta questão.

2.1 O Ambiente Corporativo e a Informação

2.1.1 Governança Corporativa

Conforme indicado em IBGC (2010), Lameira (2001) e em CVM (2002), governança corporativa diz respeito a um processo que otimiza os negócios e lucros da organização, além de garantir a preservação dos direitos de todos aqueles que nela tem interesse (stakeholders).

A governança corporativa tem como princípios, de acordo com o Código de Melhores Práticas de Governança Corporativa, IBGC (2010): a transparência, a equidade, a prestação de contas e a responsabilidade corporativa. Estes princípios devem existir conjuntamente e mutuamente se relacionar.

Para que uma governança corporativa aconteça de maneira efetiva, além de considerar os princípios elencados acima, a administração deve ter à sua disposição vários ativos (tudo aquilo que tem valor para a organização) tais como maquinário, capital, recursos humanos etc. Para fazer com que esses ativos se relacionem, a organização se vale de informação e a mesma deve estar disponível sempre que requerida, de maneira segura e confiável. Ou seja, deve-se zelar pela manutenção da disponibilidade, integridade e confidencialidade da informação, a fim de mobilizar adequadamente os demais ativos da organização.

2.1.2 Informação, sistemas de Informação e Tecnologia da Informação

A informação, como explicitado em Shannon (1948), é aquilo que reduz a incerteza. Consoante a esta definição, segundo Florid (2005),como estrutura, a informação pode ser conceituada como um conjunto de dados ou registros representados em uma determinada forma/ordem que lhes permitem ser entendidos; e como processo, pode ser entendida como o resultado da interação entre agentes capazes de interpretar e decidir. Não obstante, a informação caracteriza-se como um ativo com grande importância

para as organizações, visto que a mesma ajuda, e por vezes determina, a tomada de decisões, a coordenação e o controle que se tem da organização e de seus negócios.

Para coletar, recuperar, processar, armazenar e distribuir essas informações, utiliza-se um conjunto de componentes inter-relacionados ao qual denominamos sistema de informação, como observado em Rezende (2005) e Shitsuka (2005). Conforme indica Laudon e Laudon (2004), sistema de informação é uma solução organizacional e administrativa, que utiliza ferramentas automatizadas e manuais, a fim de administrar situações advindas das atividades da organização. Pode-se notar que os sistemas de informação, na verdade, são partes integrantes das organizações e para uma utilização efetiva dos mesmos faz-se necessário um entendimento aprofundado da organização e de sua administração.

Por sua vez a tecnologia da informação corresponde à combinação entre o conjunto de recursos de processamento (hardware, software, redes, etc.), as pessoas, as comunicações e os frameworks; objetivando a criação, a manutenção, a utilização e a recuperação da informação, conforme indicado em Laudon e Laudon (2004). Pode-se afirmar que as tecnologias da informação são ferramentas dos sistemas de informação. São elas que em parte possibilitam a sua existência. Logo a TI funciona em prol dos sistemas de informação, ajudando-os a fazer com que a organização desempenhe suas funções e administre seus negócios.

Como já dito anteriormente, a informação é um ativo crítico para as organizações, pois os seus negócios dependem dela. Portanto aqueles que, de melhor maneira, a organizam e a preservam, melhores resultados e rendimentos obtêm em suas funções e negócios.

Embora a segurança da informação, como já afirmado, não seja uma questão que se restrinja somente à área de TI, muito de suas atenções e medidas são direcionadas para tal, haja visto que a TI proporciona tanto tratamentos para riscos de segurança da informação como também vulnerabilidades que podem vir a ser exploradas. Assim é fundamental que existam controles específicos voltados para a área de TI.

Para tratar e especificar técnicas de gestão de segurança das Tecnologias da Informação foi criada a norma ISO/IEC 13335, ISO (2004). Esta norma define os termos e discute acerca dos modelos de gerenciamento de segurança das tecnologias da informação. Uma nova versão desta norma está sendo elaborada com vistas a atualizá-la e estabelecer também técnicas para gerenciamento de riscos de segurança das tecnologias da

informação.

2.1.3 Governança de TI

Atualmente é uma tarefa complicada dissociar uma empresa de seus sistemas de informação, e consequentemente da tecnologia da informação que a suporta e da qual ela depende. Fundar e manter a estrutura de tecnologia da informação de uma organização envolve grande aplicação de capital. Esse investimento muitas das vezes, quando não planejado, pode não produzir o retorno esperado. Logo é preciso definir uma estrutura por meio da qual seja possível o gerenciamento e o controle da área de TI, objetivando garantir o retorno dos investimentos feitos nesta área e agregar melhorias aos processos de negócios da organização.

O conceito de governança de TI vem ao encontro disso. De acordo com Weill e Ross (2005) e ITGI (2008), governança de TI é o termo utilizado para designar as estruturas e processos que buscam maximizar o valor dos objetivos e estratégias da organização por meio do alinhamento da tecnologia de informação aos interesses da organização. Como afirmado em (FERNANDES; ABREU, 2006):

"A Governança de TI busca o compartilhamento de decisões de TI com os demais dirigentes da organização, assim como estabelece as regras, a organização e os processos que nortearão o uso da tecnologia da informação pelos usuários, departamentos, divisões, negócios da organização, fornecedores e clientes, determinando como a TI deve prover os serviços para a empresa."

A TI geralmente não é vista de modo transparente pelos outros seguimentos da organização, pois sua linguagem e seu funcionamento não são compreendidos. Só mudanças diretamente efetivadas na base da governança desta área podem fazer com que a TI seja entendida de maneira holística e aproveitada de forma abrangente.

A adoção de estratégias organizacionais estáticas, que se resumem a definir uma estrutura e distribuir funções, possibilitam às organizações uma eficiência limitada. Os ambientes onde se dão as ações e processos de negócios utilizam-se cada vez mais da TI, assumindo um dinamismo que exige das organizações uma gestão flexível e mais ágil, que foca seus esforços e atenções nas tomadas de decisão. Para tal prática é necessário

que a TI esteja alinhada às estratégias e objetivos da organização, como afirmado em ITGI (2008).

Assim, como defende Fernandes e Abreu (2006), o modelo de governança de TI deve contemplar tanto um alinhamento estratégico estático [1]; quanto um alinhamento estratégico dinâmico [2], com isso, além de derivar sua estratégia da estratégia de negócios, a TI pode potencializar novas oportunidades para a organização, como por exemplo por meio de novos serviços de TI conforme indica a biblioteca ITIL em sua terceira versão, OGC (2007).

Ainda com relação à governança de TI, um modelo importantíssimo é o COBIT (Control Objectives for Information and Related Technology), que é um modelo que auxilia a organização a identificar e elencar os objetivos estratégicos de negócio e relacioná-los com os processos, projetos e metas da área de TI (ITGI, 2008). Ou seja, auxilia na promoção da governança de TI, na medida que permite, por meio do atendimento aos objetivos de controle por ele propostos, sistematizar e priorizar as decisões de TI segundo às necessidades do negócio da organização (ou seja, segundo o seu *corebusiness*). Os Objetivos de controle são distribuídos em 4 domínios: Planejar e Organizar (PO), Adquirir e Implementar (AI), Entregar e Suportar (DS) e Monitorar e Avaliar (ME).

2.2 Princípios e Conceitos básicos de Segurança da Informação

Faz-se necessário aqui alguns conceitos e definições para que o leitor situe-se no contexto da segurança da informação e principalmente no contexto de riscos de segurança da informação, visto este ser o elemento central da ontologia proposta.

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

A definição de impacto auxilia a diferenciar evento de segurança da informação de

[1] derivação da estratégia de TI a partir do plano estratégico ou de negócios da organização

[2] alteração da estratégia de TI em função da mudança aleatória da estratégia de negócios da organização

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

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

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

O conjunto de riscos de segurança ao qual uma organização está sujeita denomina-se **perfil do risco de segurança**.

2.3 Propriedades e Aspectos da Informação

Independente da sua forma: textual, digital, oral etc; a informação, enquanto ativo, cada vez mais, tem ficado sujeita a ameaças tais como: fraudes eletrônicas, espionagem, sabotagem etc, que podem explorar suas vulnerabilidades. Caso esta exploração aconteça, potenciais conseqüências podem ocorrer e impactar nos objetivos da organização negativamente.

Considerando a criticidade em torno da informação, as organizações implementam

conjuntos variados de controles para protegê-la, incluindo: políticas, processos, procedimentos etc; com o intuito de alcançar os objetivos de negócio e de segurança dessa informação. Obtêm-se aí, o que denominamos segurança da informação, que é a proteção da informação contra vários tipos de ameaças, objetivando a continuidade dos negócios, minimizando os riscos, maximizando os lucros e as suas oportunidades, conforme indicado em ABNT (2005).

A segurança da informação tem o intuito de preservar as características da informação no que concerne a sua disponibilidade, confidencialidade e integridade, além de aspectos como autenticidade e legalidade, que são descritos a seguir:

Disponibilidade: propriedade que a informação apresenta, de estar disponível e utilizável numa eventual requisição de uma entidade autorizada (ABNT, 2006).

Integridade: propriedade que a informação apresenta, de estar completa e fiel ao estado original (ABNT, 2006).

Confidencialidade: propriedade que a informação apresenta, de estar disponível apenas para àqueles que estão autorizados a obtê-la (ABNT, 2006).

Autenticidade: aspecto comprovante de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade (GSI, 2008).

Legalidade: aspecto comprovante do valor legal (onde todos os ativos relacionados estão de acordo com os requisitos de conformidade) que uma informação pode ter em um processo de comunicação (SêMOLA, 2003).

Em Sêmola (2003), expressa-se que a informação deve ser protegida ao longo de todo o seu ciclo de vida, pois é quando este ativo ou os ativos que a utilizam e a suportam (ativos de TI, ativos físicos e ativos humanos) ficam expostos a riscos. O ciclo de vida da informação é dividido em 4 momentos: manuseio (criação, coleta e manipulação da informação), armazenamento, transporte e descarte.

A preservação das propriedades e dos aspectos da informação anteriormente mencionados depende do estabelecimento de uma ação gerencial explícita, que é chamada de gestão da segurança da informação (GSI).

2.4 Gestão da Segurança da Informação

Como observado, a segurança da informação diz respeito à proteção da informação em suas propriedades (confidencialidade, integridade e disponibilidade) e em seus aspectos (autenticidade, legalidade etc), evitando que as vulnerabilidades dos ativos relacionados sejam exploradas por ameaças e possam trazer consequências para os negócios de uma organização. Porém para a efetividade das ações de segurança da informação é necessário mais que medidas estritamente técnicas, pois esta questão em âmbitos organizacionais, conforme explicado em Gualberto (2010), envolve também características humanas, organizacionais e estratégicas. É sobre estas características relativas à segurança da informação que a gestão de segurança da informação (GSI) se concentra, pois ao controlar e gerenciar tais pontos potencializa-se a promoção da cultura de segurança da informação, tornando-a uma prática sistêmica.

A GSI tem como objetivo principal fazer com que as ações e decisões relativas à segurança da informação estejam alinhadas aos objetivos e estratégias do negócio da organização.

Considerando a importância de se gerenciar a segurança da informação e as melhores práticas adotadas até então, a International Organization for Standardization (ISO) publicou a família de normas 27000 que tem como objetivo cobrir as necessidades das organizações no que tange à segurança da informação. A tabela 2.1 apresenta a descrição do propósito de cada uma delas.

Tabela 2.1: Normas da família ISO 27000

Norma	**Descrição**
27000	Apresenta uma visão global tanto do sistema de gestão de segurança da informação (SGSI) proposto por esta família de normas quanto da família de normas em si (descrevendo o escopo de cada uma delas).
27001	Concentra os requisitos necessários para implementar e manter um SGSI, sendo aplicável a qualquer organização, independente da especificidade do seu negócio.
27002	Propõe um código de prática para a gestão de segurança da informação, onde são descritos objetivos de controle e melhores práticas relativos à segurança da informação.

27003	Concentra orientações práticas para implementar e manter um SGSI segundo o especificado pela norma 27001.
27004	Elenca métricas e medições para avaliação de um SGSI segundo o especificado pela norma 27001.
27005	Específica um processo de gestão de riscos de segurança da informação.
27006	oferece orientações para certificação de um SGSI.
27007	Apresenta orientações para condução de auditorias internas e externas de um SGSI.
27011	Norma que especifica orientações e melhores práticas em gestão de segurança da informação para organizações do setor de telecomunicações.
27799	Norma que especifica orientações e melhores práticas em gestão de segurança da informação para organizações do setor de saúde.

As três principais normas desta família, ISO 27002, ISO 27001 e ISO 27005, são apresentas nas seções subsequentes.

2.5 ABNT NBR ISO/IEC 27002 - Código de prática para a gestão da segurança da informação

A norma ABNT NBR ISO/IEC 27002 foi a numeração atualizada atribuída à norma ABNT NBR ISO/IEC 17799 para incluí-la na família de normas 27000 que trata da gestão de segurança da informação. Esta foi criada em 2000 com base no padrão britânico BS 7799-1:1999 e revisada em 2005, quando foi incluído um capítulo relacionado à gestão de incidentes de segurança da informação. A ISO 27002 descreve um código de prática para a gestão da segurança da informação baseado nas melhores práticas de segurança da informação. São especificados 39 objetivos de controle e 133 controles, distribuídos em 11 capítulos que denotam as 11 cláusulas de controle.

Os objetos de cada uma destas cláusulas são discutidos a seguir:

2.5.1 Política de Segurança da Informação

Conforme afirmado em Faustini (2010) e em Peltier (2004), a política de segurança da informação de uma organização é o seu "pilar de eficácia"da segurança da informação, caracterizando-se como o arranjo de princípios/procedimentos que servem de base para a gestão de segurança da informação na mesma e que devem ser observados por todos seus colaboradores e intervenientes.

2.5.2 Organização da Segurança da Informação

Diz respeito ao estabelecimento de uma estrutura que suporte a gestão da segurança da informação dentro da organização. Por meio da mesma é que serão planejadas e implementadas as medidas e ações referentes à segurança da informação. Esta estrutura deve ser definida formalmente com vistas a garantir que as ações de segurança da informação sejam instituídas e vistas como atividades de responsabilidade de todos os colaboradores.

2.5.3 Gestão de Ativos

Trata da proteção dos ativos da organização (tais como ativos de informação, ativos de software, ativos físicos, serviços, pessoas e ativos intangíveis). Aborda itens como inventário de ativos, responsabilidade por ativos e utilização de ativos, além de controles e diretrizes específicos para o ativos de informação.

2.5.4 Segurança em Recursos Humanos

Elenca diretrizes que visam garantir a segurança da informação antes, durante e após a contratação de recurso humanos. A observação desta cláusula garante que os recursos humanos envolvidos com a organização (sejam eles funcionários, fornecedores ou terceiros) estejam cientes de suas responsabilidades e papéis no que tange à segurança da informação.

2.5.5 Segurança Física e do Ambiente

Estabelece controles relativos a perímetros de segurança; entrada física e segurança em ambientes físicos (como escritórios, salas e instalações), e instalação, utilização e manutenção de equipamentos dentro e fora da organização.

2.5.6 Gestão das Operações e Comunicações

Este capítulo é um pouco maior que os outros devido ao grande domínio que mapeia. Esta cláusula dispõe diretrizes desde procedimentos e responsabilidades operacionais a itens como cópias de segurança, gerenciamento da segurança em redes e manuseio de mídias. Seu objetivo central, conforme indicado em (ABNT, 2005) é:"Garantir a operação segura e correta dos recursos de processamento da informação".

2.5.7 Controle de Acesso

Aborda a dinâmica de distribuição e manutenção de acessos aos sitemas de informação da organização, com o objetivo de controlar o acesso à informação e ativos relacionados.

2.5.8 Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

A abrangência deste capítulo também é vasta, tem como foco fazer com que os sistemas de informação tenham como parte integrante a segurança da informação (desde a especificação de requisitos), com vistas a garantir a segurança da informação processada pelos mesmos.

2.5.9 Gestão de Incidentes de Segurança da Informação

Como explicitado em (ABNT, 2005), este capítulo/cláusula tem como objetivo: "Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil."

2.5.10 Gestão de Continuidade do Negócio

De acordo com Sêmola (2003), a gestão de continuidade do negócio tem como objetivo permitir a continuidade de processos, serviços e informações essenciais à sobrevivência da organização, no menor intervalo de tempo possível, com vistas a evitar/minimizar os impactos de incidentes.

2.5.11 Conformidade

Elenca os objetivos de controle e controles necessários para que a organização possa respeitar os requisitos de conformidade relacionados à segurança da informação a que está sujeita, ou seja, tem como objetivo garantir que o conjunto de normas, leis, regulamentações, políticas etc (impostas interna ou externamente) sejam cumpridos.

2.6 ABNT NBR ISO/IEC 27001 - Sistemas de gestão de segurança da informação

Conforme descrito acima, a segurança da informação é promovida por meio de um conjunto de controles (tais como procedimentos, estruturas organizacionais, políticas etc) com objetivos específicos. Um Sistema de Gestão de Segurança da Informação (SGSI) visa (com base na análise, avaliação e tratamento de riscos) justamente permitir que a organização que o implementa alcance seus objetivos relativos à segurança da informação. A própria norma ABNT NBR ISO/IEC 27001, ABNT (2006), que específica requisitos para um SGSI, versa que um Sistema de Gestão de Segurança da Informação baseia-se numa análise de riscos para estabelecer, programar, operar, monitorizar, rever, manter e melhorar a Segurança da Informação.

"O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas."

Um SGSI, conforme especificado na norma, dentre outros requisitos, prevê uma estrutura organizacional definida, metodologia de medição e avaliação, e sistematização de processos. Por meio de tais, potencializa-se a identificação e correção de pontos

fracos na GSI, promoção da cultura de segurança da informação, alcance dos objetivos propostos aos controles implementados etc.

Os processos do SGSI, que são estruturados com base no modelo *Plan-Do-Check-Act* (PDCA) e sua sistematização podem ser visualizados na figura 2.1.

Figura 2.1: Modelo PDCA aplicado aos processos de um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com (ABNT, 2006).

Na figura 2.1, que ilustra um SGSI, como em qualquer sistema de informação, temos as entradas, que são as expectativas das partes interessadas e os requisitos de segurança da informação; o processamento que é o ciclo de processos do SGSI estruturados com base no modelo PDCA e a saída, que é a própria segurança da informação gerenciada. Além disso, pode-se observar o relacionamento das partes interessadas com este sistema de informação.

Os processos do SGSI proposto são:

2.6.1 Estabelecimento do SGSI *(Plan)*

Aqui são planejados e elaborados os princípios e as estruturas em que se baseará o SGSI, tais como política, objetivos de controle, controles, processos e procedimentos. Também é definido o escopo de aplicação do SGSI, além de analisar e avaliar os riscos de segurança da informação;

2.6.2 Implementação e Operação do SGSI *(Do)*

Os princípios e estruturas são então implementados, e os tratamentos para os riscos analisados e avaliados são formulados e também colocados em prática;

2.6.3 Monitoramento e Análise crítica do SGSI *(Check)*

Segundo ABNT (2005), os processos implementados são monitorados, analisados criticamente e passam por auditorias, considerando as metas traçadas pela política e objetivos controle. São analisados também os resultados dos tratamentos de riscos implementados, levando em consideração os níveis de riscos (residuais e aceitáveis);

2.6.4 Manutenção e Melhoria do SGSI *(Act)*

Os pontos de melhoria diagnosticados no processo de "monitoramento e análise do SGSI"são analisados frente aos objetivos traçados, e então ações que atuarão sobre estes são implementadas.

Além da descrição destes processos, a ISO 27001 traz ainda, em seu anexo A, uma relação dos objetivos de controles e controles derivados daqueles especificados em ABNT (2005).

2.7 ABNT NBR ISO/IEC 27005:2008 - Gestão de riscos de segurança da informação

A gestão de riscos de segurança da informação, assim como qualquer processo de gestão de riscos, é uma gestão interativa cuja implementação tem o intuito de melhorar continuamente o desempenho e a tomada de decisões de uma organização maximizando as possibilidades de ganho, ao mesmo tempo em que minimiza as possibilidades de perda, conforme indicado em ABNT (2008).

A gerência de riscos será tanto mais eficaz, quanto mais presente e incorporada estiver na cultura organizacional da empresa. Ou seja, quanto mais importância for dada à

gestão de riscos nas atividades da organização e na forma em que estas atividades são executadas, mais qualidade e resultados serão resultantes da mesma.

A gerência de riscos pode ser aplicada nas mais variadas esferas de uma organização, seja nela como um todo, ou apenas em um projeto específico. Em qualquer situação esse ambiente onde a mesma será desenvolvida deve ser bem definido, de modo a permitir as decisões específicas e corretas que impliquem em ações eficientes nestes processos. Ou seja, o escopo de aplicação da gestão de riscos deve ser transparente e delineado. A definição de onde ou em que será implantada a gerência de riscos de segurança da informação é um dos itens mais importantes no que tange ao princípio de estabelecer uma base para um processo de gestão contínuo, define Alberts e Audrey (2002).

A gestão de riscos caracteriza-se como parte imprescindível em uma boa governança corporativa, pois organizações que conseguem com êxito cuidar dos riscos aos quais estão propensas, tendem a atingir seus objetivos e a fazê-lo com um menor custo global, afirma AS/NZS (2004).

Segundo IBGC (2007), a gestão de riscos promove maior transparência, ao informar, aos investidores e ao público em geral, os riscos aos quais a organização está sujeita, as políticas adotadas para sua mitigação, bem como a eficácia das mesmas, além de melhorar os padrões de governança, mediante a explicitação do perfil de riscos verificado, em consonância com o posicionamento dos acionistas e a cultura da organização. Adicionalmente, a gestão de riscos introduz uma uniformidade conceitual em todos os níveis da organização, seu conselho de administração e acionistas.

Não se pode confundir incertezas com riscos, pois esses termos não são sinônimos. O ponto chave para definir o que é risco e o que é apenas incerteza é a relação que esses eventos têm com os objetivos da organização. Se um evento é incerto, mas as suas consequências são indiferentes à organização ele não se caracteriza como um risco, mas apenas como uma incerteza, pois como afirmado em Hillson (2007), um risco não pode existir num vácuo. É preciso enumerar os objetivos ou informações que seriam afetados (sofreriam impacto) se esse evento ocorresse.

2.7.1 Princípios da gerência de riscos de segurança da informação

Quando da implementação de uma gerência de riscos de segurança da informação, deve-se garantir o respeito a alguns princípios, princípios esses que moldam a natureza da gerência de riscos, indica Alberts e Audrey (2002), e que podem ser agrupados em três áreas: avaliação de riscos de segurança da informação, gerência de riscos, e organização e cultura.

2.7.1.1 Princípios de avaliação de riscos de segurança da informação

São os princípios que constituem o alicerce para um processo de avaliação de riscos de segurança da informação eficaz.

Auto-direcionamento - a avaliação de riscos deve ser moldada de forma a contemplar o contexto da organização, assim modelos e metologias utilizados devem ser adaptados a essas necessidades.

Medidas adaptáveis - um processo de avaliação deve ser flexível de modo a permitir medidas adaptáveis pois o contexto da segurança da informação e da tecnologia de informação são muito dinãmicos, e os controles relacionados devem considerar esta perspectiva.

Processos definidos - a institucionalização de práticas relacionadas à avaliação de riscos devem estar associadas a processos e procedimentos definidos, padronizados e documentados, e que contemplem a distribuição de responsabilidades e os insumos necessários a sua execução.

Base para um processo contínuo - estratégias, planos e documentos que reflitam esses, como uma política de segurança da informação por exemplo, permitem a caracterização e institucionalização dos processoos relacionados à segurança da informação da organização como prática inerente a todas suas atividades.

2.7.1.2 Princípios de gerência de riscos

São os princípios básicos para uma prática efetiva da gerência de riscos. Os princípios aqui encontrados são extensíveis a todas as categorias de riscos, não só aos de segurança

da informação.

Perspectiva de visão futura - refere-se à necessidade de se planejar não só o presente, o cotidiano, mas o amanhã da organização, ou seja, deve-se tentar preestabelecer ações para eventuais acontecimentos futuros (identificar os riscos associados aos cenários de incidentes de segurança da informação considerados).

Foco nos pontos críticos - as questões mais críticas de segurança de informação, e que priotariamente devem ser tratadas, são aquelas relacionadas à missão da organização e ao seu respectivo negócio.

Gestão integrada - refere-se à necessidade de que as políticas e estratégias de segurança sejam coerentes com as demais políticas e estratégias organizacionais.

2.7.1.3 Princípios organizacionais e culturais

Os princípios organizacionais e culturais auxiliam na promoção da cultura organizacional favorável a uma gestão de riscos efetiva. Conforme indicado em (ALBERTS; AUDREY, 2002), a não-observação a esses princípios pode fazer que questões importantes para a organização passem despercebidas pela gestão de riscos, além de acarretar em um falta de compromisso e empenho para com esse gerenciamento, por parte das pessoas que constituem a organização.

Comunicação aberta - o êxito da gestão de riscos de segurança da informação está diretamente ligado a uma comunicação aberta dentro da organização, pois não se pode tratar um risco de segurança da informação se o mesmo não for comunicado e entendido pelos tomadores de decisões. Somente por meio de atividades de avaliação que são desenvolvidas por meio de colaboração e intercâmbio de informações relativas a riscos de segurança entre todos os níveis de uma organização é que se pode gerenciar riscos de segurança da informação de forma eficiente.

Perspectiva global - com base na missão da organização e nos seus objetivos de negócio, deve-se consolidar o perfil de riscos de segurança da informação da organização.

Trabalho de equipe - refere-se à necessidade de que os indivíduos membros da organização se unam, formando equipes interdisciplinares, com representantes da área de TI e da área de negócios, de forma a ampliar o entendimento das questões relacionadas à segurança da informação da organização.

Esses princípios baseiam as atividades de gestão de riscos de segurança da informação. Pode-se observar na figura 2.2 um quadro resumo desses princípios.

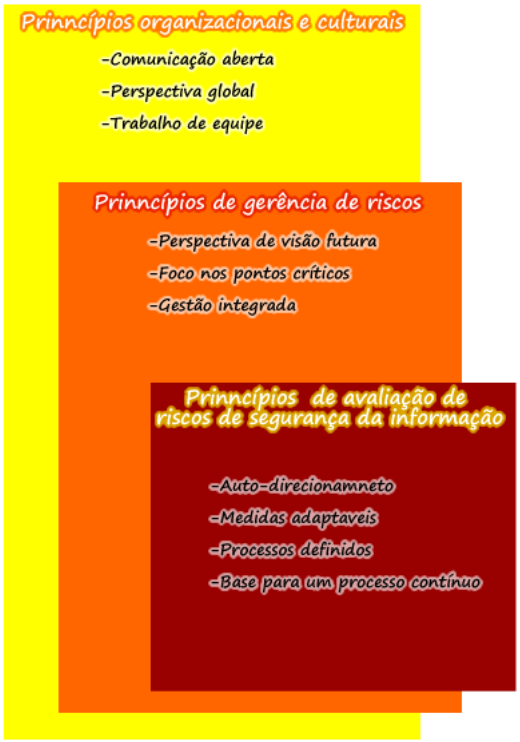

Figura 2.2: Princípios de gerenciamento de riscos de segurança da informação de acordo com (ALBERTS; AUDREY, 2002).

2.7.2 Atividades da Gestão de Riscos de Segurança da Informação

As atividades que compõem a gestão de riscos de segurança da informação são descritas a seguir segundo o definido em ABNT (2008) que, como já mencionado, é uma integrante da família de normas 27000 e é totalmente aderente ao que é proposto em ABNT (2005) e em ABNT (2006). Cada uma destas atividades deve ter suas entradas, ações e resultados registrados, pois esses registros são um dos requisitos para uma boa governança corporativa.

As atividades de um processo de gestão de riscos de segurança da informação, mostradas na figura 2.3, são descritos a seguir.

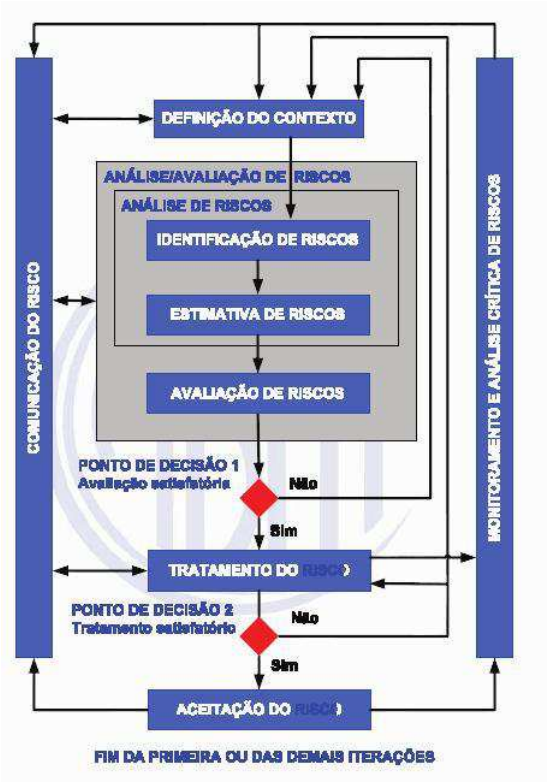

Figura 2.3: Fluxo do processo de Gestão de Riscos de Segurança da informação (GRSI), considerando o disposto em (ABNT, 2008).

2.7.2.1 Definição de contexto

Quando da decisão da implementação de uma gerência de riscos, faz-se extremamente necessário o estabelecimento de um contexto bem definido, que serão os parâmetros básicos para que possa ser diagnosticado com excelência o escopo dos riscos que serão considerados. Expõe AS/NZS (2004), que esse contexto além de detalhar o ambiente da organização, se estende a definir o propósito da aplicação da gerência de riscos de segurança da informação; seus objetivos; suas estratégias; seus critérios para avaliação de riscos, de impacto e de aceitação de riscos; e a sua organização e distribuição de responsabilidades.

2.7.2.2 Apreciação de riscos

Nessa etapa, que se divide em análise de riscos e avaliação de riscos, identificam-se: os ativos de segurança de informação, sua valoração, as ameaças potenciais, os controles existentes, as vulnerabilidades que podem ser exploradas, as consequências que podem advir de uma eventual exploração de uma vulnerabilidade por uma ameaça; analisa-se qualitativa e/ou quantitativamente as consequências, a probabilidade dos incidentes, estima-se o nível dos riscos; e avaliam-se os riscos, com base nos critérios estabelecidos na definição do contexto, e os ordena de acordo com as prioridades definidas.

Análise de Riscos

A análise de riscos se subdivide em identificação de riscos e estimativa de riscos, que são descritas a seguir.

- ***Identificação de riscos***

  Identificar os riscos é delinear e caracterizar os potenciais incidentes que podem interferir nos propósitos de uma atividade, sistema, processo, organização, etc, a fim de gerenciá-los. Para isso, como exposto em IRM (2002), é necessário um conhecimento intrínseco da organização, do campo em que ela atua, do ambiente em que ela existe, das relações e serviços jurídicos, políticos, sociais, culturais que ela engloba, e sobretudo ter uma visão ampla de seus objetivos, descrevendo as informações críticas para o seu sucesso.

  Não se pode confundir, aqui, incertezas com riscos, pois esses termos não são sinônimos. O ponto chave para definir o que é risco e o que é apenas incerteza é a relação que esses eventos têm com os objetivos da organização. Se um evento é incerto, mas as suas consequências são indiferentes à organização ele não se caracteriza como um risco, mas apenas como uma incerteza, pois como afirma Hillson (2007), um risco não pode existir num vácuo. É preciso enumerar os objetivos ou informações que seriam afetados se esse evento ocorresse.

  Pode-se dividir a identificação de riscos nas seguintes etapas: identificação dos ativos, identificação das ameaças, identificação dos controles existentes, identificação das vulnerabilidades e identificação das consequências.

- ***Estimativa de riscos***

  Esta atividade objetiva desenvolver a compreensão dos riscos. A observação nessa etapa se baseia nas potenciais consequências de um determinado evento

e nas suas probabilidades de acontecer. Analisando a natureza, as consequências e as probabilidades dos mesmos, subsidia-se as decisões se os riscos identificados e estimados devem ser tratados, com qual prioridade e quais as estratégias de tratamento apropriadas e com melhor custo-benefício para a organização.

A estimativa de riscos, segundo ABNT (2008) e AS/NZS (2004), pode ser qualitativa (geralmente a primeira a ser feita, dando uma visão geral dos níveis dos riscos e identificando os riscos de maior prioridade), quantitativa (em geral utilizada depois de uma estimativa qualitativa, atuando sobre os riscos mais prioritários, ou que podem trazer maior impacto por meio de suas consequências) ou ainda semi-quantitativa.

Avaliação de riscos

De acordo com IRM (2002), o processo de avaliação de riscos consiste na comparação dos riscos estimados com os critérios que foram estabelecidos no processo de definição do contexto. Além de considerar a definição do contexto, deve-se levar em conta outros documentos e requisitos tais como: cláusulas contratuais, requisitos legais e requisitos regulatórios.

Conforme explicitado em ABNT (2008), o principal objetivo desse processo é a tomada de decisões a respeito dos riscos que necessitam de tratamentos e daqueles que necessitam de tratamentos prioritários, baseando-se nos objetivos e no grau de segurança que pode ser gerado para a organização, respeitando o contexto definido.

2.7.2.3 Tratamento de riscos

Na atividade de tratamento de riscos, define AS/NZS (2004), identificam-se opções para proteger a organização dos riscos identificados, analisados e avaliados.

Avaliam-se esses tratamentos decidindo-se quais opções serão adotadas e em qual ordem serão executadas, fazendo-se a preparação para que seja possível executá-las e finalmente, implementando as ações planejadas.

Fazer com que uma organização não fique exposta a nenhum risco é impossível. Diante dessa certeza, faz-se extremamente necessário a definição de prioridades e de direções

dos esforços e controles a fim de minimizar o impacto negativo sobre os objetivos de negócio da organização e sua missão.

Consoante ao definido em ABNT (2008), o processo de tratamento de riscos pode ser de quatro tipos, não excludentes entre si: redução do risco (seleção de controles apropriados para mitigar os riscos de segurança da informação), retenção do risco (que refere-se à opção de não implementar controles para tratamento de um risco, diante do fato de o nível desse risco atender aos critérios para a aceitação de riscos), evitar o risco (eliminação das atividades/eventos que causam o risco ou alteração nas condições de operação de tais) e transferência do risco (compartilhar determinados riscos com entidades externas, para que o mesmo seja tratado de forma mais eficaz).

2.7.2.4 Aceitação do risco de segurança da informação

De acordo com ABNT (2008), é nessa atividade que se delimita quais riscos serão ou não aceitos formalmente, de acordo com os critérios para aceitação de riscos, descrevendo como esses serão considerados, os possíveis riscos residuais resultantes e as condições associadas a essas decisões.

2.7.2.5 Monitoramento e Revisão

A atividade de monitoramento e revisão ao longo do gerenciamento de riscos e ao seu final assegura que novos riscos que surjam durante a execução da gestão de riscos não sejam desconsiderados e que mudanças nos riscos serão rapidamente reconhecidas pelo fato de os mesmos serem analisados e revisados frequentemente, além de revisar a execução de respostas a riscos enquanto avalia sua eficácia. Em suma, esse processo prima pela continuidade da pertinência da gerência de riscos, conforme entendimento explícito em AS/NZS (2004) e em ABNT (2008).

2.7.2.6 Comunicação e Consulta

Engloba os diálogos com as partes interessadas, internas e externas, sabendo que os mesmos têm visões pertinentes acerca dos riscos da organização e que essas percepções

têm grande influência em quais decisões são tomadas. Então, a partir desta premissa, as comunicações e consultas a esses intervenientes devem ser constantes, envolvendo assuntos tanto dos riscos, quanto da sua gestão ao longo de todo esse macro-processo que é a gestão de riscos.

Além disso, quando existe uma comunicação efetiva, a distribuição de responsabilidades e o entendimento da base em que se tomam as decisões são facilitados.

2.8 Comentários Finais

Este capítulo apresentou os principais conceitos e temas relacionados à segurança da informação e ao seu processo de gestão, com vistas a permitir uma visão clara do domínio a ser representado pela ontologia proposta.

Foi explicitado que a segurança da informação precisa de um processo de gestão que seja de responsabilidade de todos aqueles que interagem com a organização. Assim, o conhecimento de atividades e conceitos segurança da informação é vital para que se compreenda a importância de se implementar e manter este processo. Neste sentido, representações de conhecimento que apresentem estes conceitos, suas propriedas e as relações entre eles, auxiliam na formalização do conhecimento deste domínio, na sua aquisição e no seu compartilhamento.

O capítulo 3 apresenta as ontologias como forma de conceitualização que pode auxiliar nesse tipo de contexto.

3 Ontologias e Elementos Relacionados

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

As visões de mundo descritas em uma ontologia devem representar um consenso entre os usuários e desenvolvedores envolvidos no domínio a ser representado. Além disso, deve-se ter em mente que os conceitos, relacionamentos e atributos representados devem ser relevantes para o próposito da criação da ontologia em si, pois uma ontologia caracteriza-se como um abstração da realidade, e assim, apenas parte dos objetos do domínio é considerada quando da sua construção.

O processo de criação de ontologias também deve envolver atividades de planejamento e avaliação, para que os objetivos deste desenvolvimento sejam traçados e seus resultados verificados. Além do processo e de suas atividades em si, formalismos que possibilitem estabelecer relações de inferência sobre a representação, assim como ferramentas que possibilitem automatizar algumas dessas atividades devem ser considerados.

Este capítulo tem como foco as ontologias, e as seções a seguir as descrevem, discutem os benefícios de sua utilização e os aspectos relacionados ao seu processo de desenvolvimento.

3.1 Ontologia: conceito e benefícios de sua utilização

Embora para os profissionais e pesquisadores de áreas como a ciência da computação e as engenharias, o termo ontologia denote um modelo de dados que expresse conceitos, suas hierarquias e propriedades associadas, a utilização deste termo representa para a filosofia, desde 1613, conforme aponta Catro (2008), o estudo ou conhecimento do ser enquanto ser (ou seja, o estudo do ser por meio de suas manifestações físicas).

Em Machado (2010), expõe-se que a utilização da denominação ontologia como um conjunto de entidades com suas propriedades, restrições, axiomas e vocabulários, tal como definido em Guarino e Welty (2001), trata-se de uma feliz metonímia baseada na idéia geral de "conhecimento do ser".

De forma mais clara, uma ontologia pode, conforme indicado no capítulo 1, Guarino (1998), ser definida como um artefato de engenharia, baseado em vocabulário formal específico, cujo uso permite a descrição de um domínio que se quer representar. Consoante a esta definição, uma formalização do conceito de ontologia pertinente é a proposta por Stumme e Maedche (2003) e complementada por Ehrig et al. (2004), representada pela 10-upla conforme equação 3.1.

$$O := (C, T, \leq_C, \leq_T, R, A, \sigma_A, \sigma_R, \leq_R, \leq_A). \tag{3.1}$$

Na equação 3.1, C refere-se ao conjunto de conceitos, R ao conjunto de relacionamentos e T ao conjunto de tipos de dados, estes três conjuntos são disjuntos. O conceitos estão organizados segundo uma hierarquia $\leq_C$, as relações segundo $\leq_R$ e os atributos segundo $\leq_T$. Os relacionamentos têm assinatura $\sigma_R : R \rightarrow$ C x C. A é o conjunto dos atributos de tipos de dados associados a conceitos, com assinatura $\sigma_A : A \rightarrow$ C x T e organizados segundo a taxonomia $\leq_A$.

Assim, com base na explicação da equação 3.1, explicitam-se alguns entendimentos: o conjunto de conceitos são representações de objetos (entidades) do mundo real, que possuem propriedades com outros objetos (propriedades relacionais ou relacionamentos) e propriedades descritivas (atributos com valores de determinados tipos de dados) que os descrevem (representando estados, eventos ou processos destas entidades). As instâncias de um conceito representam um objeto particular e a sua descrição (atributos e relacionamentos) dentro de um conjunto de objetos do mesmo tipo. O conjunto de instânciações associado a ontologia constitue uma base de conhecimento relativa aquele domínio.

Com base na equação 3.1, a equação 3.2, explicita uma formalização do conceito de base de conhecimento, também proposta em Ehrig et al. (2004):

$$BC := (C_{BC}, T_{BC}, R_{BC}, A_{BC}, I, V, \iota_C, \iota_T, \iota_R, \iota_A). \tag{3.2}$$

Onde C_{BC}, T_{BC}, P_{BC} e A_{BC} são definidos como na equação 3.1, I é um conjunto de instâncias, V é um conjunto de valores de dados, enquanto $\iota_C, \iota_T, \iota_R$ e ι_A, são, respectivamente, instancializações de conceitos, de valores de dados, de relações e de atributos.

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

Diante das características da definição acima exposta, podem-se citar como principais benefícios da utilização de ontologias, tanto no que tange a domínios relacionados à segurança da informação, como apontado em Donner (2003) e Raskin et al. (2001), quanto na sua utilização de uma forma geral, segundo Noy e McGuinners (2001), os seguintes:

> Formalização de um fenômeno, por meio da organização e sistematização de conceitos relacionados ao domínio em questão, seus relacionamentos e atributos, propiciando um compartilhamento do entendimento comum a pessoas e agentes de software;
>
> Uma compreensão mais clara do domínio modelado, devido à definição formal e explícita, além da aquisição de conhecimento (geração automática) possibilitada por meio das regras de inferência e axiomas;
>
> A manutenção do conhecimento no modelo obtido (seja pela reuso ou extensão) também é facilitada pela especificação formal e explícita empregada nas ontologias;

O compartilhamento de conhecimento e informações também é favorecido devido ao domínio modelado o ser com base em uma conceitualização compartilhada e permitir a instanciação dos conceitos e propriedades especificados;

A utilização de ontologias permite separar conhecimento de um domínio do conhecimento operacional, assim uma mesma ontologia pode ser utilizada em variadas aplicações, além de admitir a interoperabilidade entre elas.

3.2 Classificações de Ontologias

As ontologias podem ser classificadas sob diversas perspectivas. Em Heijst, Schreiber e Wielinga (1997), elas são classificadas consoante ao assunto de suas respectivas conceitualizações, sendo divididas nos seguintes tipos: ontologias de representação, ontologias genéricas, ontologias de domínio e ontologias de aplicação. De acordo com Guarino (1998), ainda podem ser incluídas nesta classificação as ontologias de tarefas.

Os tipos citados são descritos a seguir:

Ontologias de representação - destinam-se a explicar as conceitualizações baseadas em formalismos de representação do conhecimento, sem contudo realizar afirmações e inferências sobre o conteúdo modelado.

Ontologias genéricas - descrevem conceitos e vocábulários gerais que são independentes de uma tarefa ou domínio particular, como por exemplo: estado, processo, componente etc.

Ontologias de domínio - as conceitualizações deste tipo de ontologias expressam descrições sobre um domínio em particular (segurança da informação por exemplo), por meio da especialização de ontologias genéricas. As ontologias de domínio, assim como as ontologias genéricas, são descritas usando as primitivas fornecidas pelas ontologias de representação.

Ontologias de tarefa - expressam conceitualizações destinadas a tarefas ou atividades genéricas, por meio da especialização de ontologias genéricas.

Ontologias de aplicação - a conceitualização deste tipo de ontologias se destinam a descrever conceitos baseados em uma tarefa e domínio específicos. Estas

ontologias são especializações de ontologias de domínio e/ou de ontologias de tarefa.

Também em Heijst, Schreiber e Wielinga (1997), as ontologias são classificadas segundo a quantidade e o tipo de estrutura da conceituação modelada. Esta classificação divide as ontologias em ontologias terminológicas, ontologias de informação e ontologias de modelagem do conhecimento, que são descritas a seguir:

Ontologias terminológicas - especificam apenas os termos utilizados para representar o conhecimento de um domínio.

Ontologias de informação - especificam estruturas de registros de informações em bancos de dados.

Ontologias de modelagem do conhecimento - especificam conceitualizações de conhecimento de um domínio.

3.3 Engenharia de ontologias

Em Bruijn (2003), são elencados fatores como: a complexidade de se construir uma ontologia, considerando requisitos e restrições relativas não só ao próprio desenvolvimento da ontologia em si, como também ao domínio e perspectiva desta modelagem, e a complexidade inerente às linguagens de representação de ontologias. Esses explicitam bem a necessidade de que o desenvolvimento de ontologias seja regido por uma metodologia, ou seja, que haja um processo que defina a abordagem a ser adotada ao longo de toda esta elaboração.

Assim uma abordagem sistemática e disciplinada, com base em sólidos princípios de engenharia, semelhante ao estabelecido para a engenharia de software em Pressman (2006), auxilia o desenvolvimento eficiente de ontologias.

Neste sentido, são descritas nas próximas seções as principais metodologias para engenharia de ontologias.

3.3.1 Metodologias de Desenvolvimento

Embora exista uma variedade de metodologias e métodos para o desenvolvimento de ontologias, não existe uma metodologia padrão para este tipo de desenvolvimento. Alguns destes foram concebidos como parte de um projeto, como o método proposto no projeto Cyc[1], que tinha no processo de desenvolvimento de sua ontologia, consoante ao indicado em Lenat e Guha (1990), apenas 3 fases: extração manual do conhecimento, extração de conhecimento apoiada por computadores e extração do conhecimento gerenciada por computadores. Outros foram desenvolvidos a partir da experiência de seus idealizadores em projetos passados, como a *Skeletal Model*[2], que conforme disposto em Bruijn (2003) e em Uschold e King (1995), elenca 4 etapas que devem ser seguidas no processo de engenharia de uma ontologia (identificação de propósito e de escopo, construção da ontologia, avaliação, e documentação), além de apontar princípios (como clareza, coerência e extensibilidade) desejáveis de serem seguidos em todas estas etapas.

Como explicitado em Silva, Souza e Almeida (2008), também podem ser citados como métodos que surgiram a partir de projetos específicos os métodos: Kactus[3] e o Sensus[4]. O primeiro, consoante a Bernaras, Laresgoiti e Corera (1996) tem sua abordagem voltada para o desenvolvimento de aplicações, onde a ontologia que representa o conhecimento necessário daquele domínio deve ser refinada sempre que novas aplicações forem desenvolvidas. Já o segundo, conforme indicado em Swartout et al. (2009), utiliza a ontologia Sensus como ontologia de alto nível para gerar novas ontologias, onde por meio da ferramenta OntoSaurus, são estabelecidas ligações entre os termos específicos na nova ontologia com os termos da Sensus.

Para a elaboração da InfoSecRM foram utilizadas as perspectivas de três abordagens, a metodologia **methontology** como o processo que define o arcabouço das atividades a serem realizadas, **o método 101** para definir o "como fazer"de algumas destas atividades (na conceituação por exemplo, onde os passos são bem detalhados) e a

[1] o projeto Cyc iniciou-se em 1984, sob o comando de Douglas Lenat, tinha como objetivo central, conforme informado em Smith (2001) e em Fensel (2003), codificar todo o conhecimento que compõe o senso comum de forma a realizar inferências sobre os domínios mapeados de maneira automatizada, ou seja, a ontologia criada serviria como uma base de conhecimento, uma enciclopédia do conhecimento humano. O nome cyc vem justamente do termo enciclopedia, em inglês encyclopedia (en-cyc-lopedia).

[2] Método proposto por Uschold e King, após participarem do projeto **Enterprise Ontology**.

[3] Utilizado no projeto de mesmo nome, para desenvolvimento de uma ontologia de redes elétricas.

[4] Este método foi criado para o desenvolvimento da ontologia Sensus utilizada para o processamento de lingauem natural.

metodologia proposta por Fox e Gruninger no projeto TOVE, com a utilização das idéias de cenários de motivação e de questões de competência por ela proposta.

As abordagens utilizadas são descritas mais detalhadamente nas próximas seções:

3.3.1.1 Methontology

Esta metodologia teve como base o processo padronizado de desenvolvimento de software do *Institute of Electrical and Electronics Engineers* (IEEE). Em Corcho et al. (2005), expõe-se que as fases e atividades do processo proposto por esta metodologia são divididas em três categorias: relacionadas à gestão (planejamento, controle e garantia de qualidade), relacionadas à atividade de desenvolvimento/construção da ontologia em si (especificação, conceitualização, formalização, implementação e manutenção) e relacionadas às atividades de suporte (aquisição de conhecimento, integração, avaliação, documentação e gestão de configuração). A disposição destas fases e atividades, e a sua concentração ao longo do ciclo de vida do processo de desenvolvimento são ilustradas na figura 3.1.

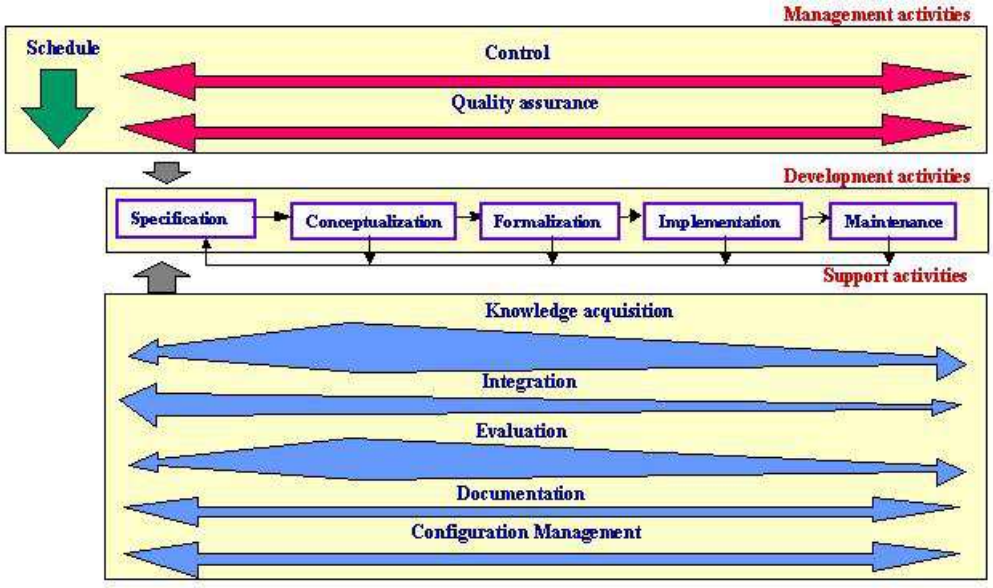

Figura 3.1: Fases e atividades propostas pela Methontology (CORCHO et al., 2005)

As fases e atividades são descritas a seguir:

Planejamento - identificam-se e descrevem-se as tarefas e recursos que serão

utilizados durante o processo de desenvolvimento da ontologia, seu escopo e objetivos.

Controle - ocorre durante o processo de desenvolvimento da ontologia, verificando escopo, tempo, recursos etc.

Garantia de qualidade - assim como a fase de Controle, ocorre ao longo de todo o processo, verificando se a ontologia atingirá os objetivos especificados e se o fará de forma eficiente.

Especificação - ocorre juntamente com o planejamento, são identificados o propósito da ontologia, seu nível de formalidade e alguns dos termos mais importantes de serem representados podem ser elencados.

Conceitualização - nesta fase, de acordo com o domínio de conhecimento a ser representado, são elencados os conceitos, as propriedades a eles inerentes, seus relacioamentos e restrições.

Formalização - a partir do modelo conceitual concebido pela fase anterior formalizam-se os componentes (classes e propriedades) por meio de uma linguagem formal ou semiformal de representação.

Integração - nesta fase pode-se proceder, caso opte por esta alternativa, á integração da ontologia formalizada com outras já existentes.

Implementação - a partir da representação dada pela linguagem formal ou semi formal na fase de formalização, implementa-se a ontologia utilizando alguma linguagem para representação de ontologias, como a por exemplo.

Manutenção - caso ocorram mudanças no domínio de conhecimento representado, é nesta fase que essas devem ser consideradas.

Aquisição de conhecimento - as atividades desta fase são constantes em todos as etapas do processo de construção, embora tenha maior concentração nas fases de planejamento, especificação e conceituação.

Avaliação - os objetivos das atividades dest fase são: verificar se as atividades de desenvolvimento da ontologia foram realizados segundo definido, e se a ontologia é consistente e representa o domínio de conhecimento especificado.

Documentação - nesta fase, devem ser gerados documentos que descrevam a ontologia e a sua implementação com vistas a auxiliar na sua utilização e também facilitar quando das eventuais manutenções.

Gestão de configuração - devem ser especificadas as condições técnicas necessárias para desenvolvimento e utilização da ontologia.

3.3.1.2 Método 101

Em Noy e McGuinners (2001) é discutido este método, criado por Noy e McGuiness, que baseia-se na idéia de que o desenvolvimento de ontologias deve ser um processo iterativo. Os passos definidos por esta metodologia são citados a seguir:

Determinar o domínio e o escopo da ontologia;

Considerar o reuso de ontologias existentes;

Enumerar termos importantes para a ontologia;

Definir as classes e suas respectivas hierarquias;

Definir as propriedades das classes;

Definir os valores das propriedades;

Criar instâncias.

3.3.1.3 A metodologia proposta no projeto TOVE

O projeto TOVE (TOronto Virtual Enterprise), conforme indica Fensel (2003), tinha como objetivo criar um modelo de dados que fosse capaz de prover, em um ambiente empresarial, uma terminologia compartilhada com significado para cada termo e com uma semântica definida por meio de axiomas capaz de realizar inferências automaticamente para questões de senso comum.

Também por meio de suas experiências neste projeto, Fox e Gruninger, consoante ao indicado em Bruijn (2003) e em Grüninger e Fox (1995), desenvolveram esta metodologia que considera de forma explicita as peculiaridades de um ambiente corporativo na construção de ontologias. As etapas propostas para esta metodologia são:

Captura de cenários de motivação - os cenários capturados devem auxiliar na concepção do domínio e da utilização que a ontologia a ser construída terá.

Formulação de questões de competências informais - devem ser formuladas questões que ajudem a definir as informações que a ontologia expressar quando construída. Neste momento, estas questões de competência são escritas em linguagem natural.

Especificação da terminologia da ontologia com uma linguagem formal - os termos e conceitos considerados como essenciais para o domínio a ser representado devem ser selecionados, estes devem ser capazes de garantir respostas às questões de competência.

Formulação de questões de competência usando a terminologia - as questões de competência definidas anteriormente devem agora ser formuladas utilizando a mesma linguagem formal da etapa anterior e apenas com os conceitos utilizados na ontologia.

Especificação formal de axiomas - nesta etapa a ontologia é formalizada por meio de uma linguagem lógica, OWL por exemplo, são criados axiomas e definições para os seus termos e conceitos.

Verificação de completude - aqui é verificado, de maneira formal (utilizando teoremas), se as questões de competência podem ser respondidas pela ontologia desenvolvida.

3.4 Web semântica

conforme explicitado em Bruijn (2003) e em Berners-Lee, Hendler e Lassila (2001), a idéia da Web Semântica foi concebida a partir da necessidade de relacionar significados semanticamente definidos às informações disponíveis na web, significados estes passíveis de compreensão tanto por agentes humanos quanto agentes de software. Porém para isto, eram necessárias a utilização de abordagens e tecnologias que permitissem a representação deste conteúdo de forma inteligível e processável. Neste sentido foram adotados e desenvolvidos novos formalismos e linguagens para este fim. As subseções que se seguem descrevem a lógica descritiva, formalismo para representação de conhecimento que permite decibilidade e expressividade, a linguagem para representação de

ontologia OWL e a linguagem RDF utilizadas, respectivamente, para formalizar a InfoSecRM, e para representar e armazenar as instâncias de classes e propriedades desta mesma ontologia.

3.4.1 Lógica Descritiva

A Lógica descritiva refere-se a uma classe de formalismos para representação do conhecimento. Esta é uma variante da lógica de primeira ordem que oferece expressividade e decibilidade às conceitualizações nela baseadas, ou seja, permite métodos de raciocínio automatizado sobre a representação do mundo modelada, indica Baader et al. (2003).

Conforme indicado em Baader, Horrocks e Sattler (2003), nos formalismos por ela propostos, a representação do conhecimento se dá por meio de predicados unários, predicados binários, construtores e axiomas. Além disso, ela permite a distinção entre a especificação da ontologia em si e das instâncias de seus conceitos, consoante ao definido pelas equações 3.1 e 3.2. Para isto, utiliza-se dos componentes **TBox**, que representa a terminologia, os axiomas e as características dos conceitos de um domínio, e **ABox**, que por sua vez representa as assertivas sobre as instâncias destes conceitos. A combinação destes dois componentes representa a base de conhecimento (Knowledge base - KB).

A figura 3.2 abaixo, obtida em Baader et al. (2003), expressa uma base de conhecimento (KB) representata por meio de lógica descritiva, com os conceitos de TBox e ABox conforme descrito acima, indicando ainda a possibilidade de racioncínio sobre esta representação, com base nas assertivas e axiomas definidos.

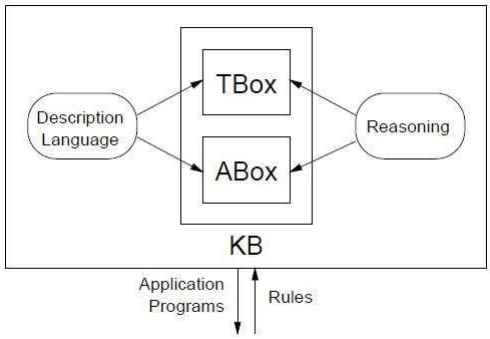

Figura 3.2: Representação do conhecimento por meio de lógica descritiva (BAADER et al., 2003)

3.4.2 Linguagens de representação

3.4.2.1 Resource Description Framework (RDF)

O *Resource Description Framework* (RDF), conforme indica Bruijn (2003), é uma linguagem que permite adicionar e representar metadados (dados sobre dados) para recursos disponíveis na Web, além de promover o intercâmbio destes na internet. Ela foi a primeira linguagem desenvolvida especificamente para a Web Semântica. Baseado na **Extensible Markup Language** (XML), além de proporcionar a representação de dados estruturados que pode ser processada de forma automatizada por agentes computacionais, a RDF permite representar relações entre objetos.

As relações entre objetos, indica Beckett (2004), são representadas por meio de declarações baseadas em triplas compostas pelos elementos sujeito, predicado e objeto. conforme explica Martimiano (2006), sSujeito é um recurso que é identificado por um *Uniform Resource Identifier* (URI), predicado indica um relacionamento entre um recurso e um objeto, ou uma propriedade do sujeito, enquanto o objeto pode ser, conforme o predicado, um outro recurso ou um valor para a propriedade do sujeito.

Com o esquema RDF (*RDF Schema*, além do relacionamento entre recursos, o RDF define os tipos de recursos que podem ser utilizados nestes, ou seja, permite a definição de restrições para estes relacionamentos. Por meio da utilização do esquema RDF e dos recursos oferecidos pela XML, Horrocks, Patel-Schneider e Harmelen (2003), é que foram criadas algumas das principais linguagens para representação de ontologias, como a *Ontology Inference layer* (OIL), a *DARPA Agent Markup Language* (DAML) e a *Web Ontology Language* (OWL), esta última, que foi utilizada na InfoSecRM, é descrita a seguir.

3.4.2.2 Web Ontology Language (OWL)

A *Web Ontology Language* (OWL), segundo Staab e Studer (2004) e McGuinness e Harmelen (2004), teve como base para seu desenvolvimento a linguagem DAML+OIL, (HORROCKS; PATEL-SCHNEIDER; HARMELEN, 2002), e estende o vocabulário RDF, adicionando maior capacidade de representação como restrições de cardinalidade por exemplo. Foi criada com o objetivo de representar conhecimento por meio de

ontologias e assim permitir maior capacidade de processamento do conteúdo da Web por agentes de software.

Conforme indicado em Dean e Schreiber (2004) e em Horridge et al. (2004a), a linguagem OWL possue três sub-linguagens (ou dialetos): OWL-Lite, OWL-DL e OWL-Full, que são descritas a seguir:

OWL-Lite - é a sublinguagem mais simples das três, permite apenas hierarquias de classes e restrições simples. Tem expressividade SHIF(D)[5]. OWL-Lite não permite descrições de classes por enumeração, por exemplo.

OWL-DL - é baseada em lógica descritiva, ou seja, seus constructos podem ser raciocinados automaticamente, tal como as hierarquias de classes representadas e axiomas, além de possibilitar a verificação de inconsistências. Possui maior expressividade que a OWL-Lite, SHOIN(D)[6], além de oferecer computabilidade.

OWL-Full - possui maior expressividade de todas os três dialetos, utilizando toda a expressividade da lógica de primeira ordem, no entanto não garante decibilidade. Permite o uso completo da sintaxe RDF e dos contrutores OWL. Por exemplo, permite que uma classe seja instância e propriedade ao mesmo tempo.

Em termos de expressividade, OWL-Lite está contida em OWL-DL, que por sua vez, está contida em OWL-FULL, conforme indica a figura 3.3.

Para o desenvolvimento da InfoSecRM foi utilizada a linguagem OWL por ter a expressividade necessária para a descrição do domínio representado neste trabalho e garantir decibilidade.

[5]Conforme indica Baader et al. (2003): S corresponde a uma abreviação de ALC_{R^+} - AL refere-se a propriedade conjunção, restrições e alguns quantificadores existenciais limitados; C refere-se a construtores AL, propriedade de disjunção e nenhuma restrição quanto aos quantificadores existenciais; e $_{R^+}$ refere-se a propriedade de transitividade - H corresponde a hierarquia de propriedades, I corresponde a propriedade inversa, F a propriedade funcional e D corresponde a utilização de tipos de dados.

[6]Conforme indica Baader et al. (2003): S corresponde a uma abreviação de ALC_{R^+} - AL refere-se a propriedade conjunção, restrições e alguns quantificadores existenciais limitados; C refere-se a construtores AL, propriedade de disjunção e nenhuma restrição quanto aos quantificadores existenciais; e $_{R^+}$ refere-se a propriedade de transitividade - H corresponde a hierarquia de propriedades, O corresponde a instâncias das classes (indivíduos), I corresponde a propriedade inversa, N corresponde a restrições de cardinalidade adicionais do tipo "$\leq$"e "$\geq$"(e não apenas igual 0 ou 1 como em OWL-Lite) e D corresponde a utilização de tipos de dados.

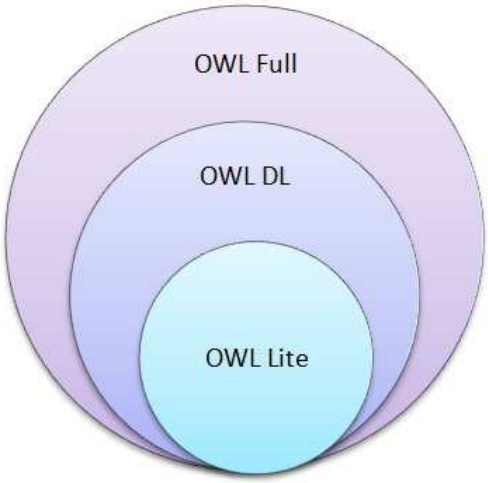

Figura 3.3: Representação da expressividade dos dialetos OWL (HORRIDGE et al., 2004a)

Tabela 3.1: Construtores OWL (STAAB; STUDER, 2004) e (AZEVEDO, 1994)

Construtores OWL		
Construtor	**DL Sintaxe**	**Exemplo**
intersectionOf	$C_1 \cap ... \cap C_n$	$Homem \cap Mulher$
unionOf	$C_1 \cup ... \cup C_n$	$Advogado \cup Lei$
complementOf	$\neg C$	$\neg Woman$
oneOf	$x_1 ... x_n$	{John, Marie}
allValuesFrom	$\forall$ P.C	$\forall$ temFilho.Medico
someValuesFrom	$\exists$ P.C	$\exists$ temFilho.Advogado
maxCardinality	$\leq nP$	$\leq 1 temFilho$
minCardinality	$\geq nP$	$\geq 2 temFilho$

Tabela 3.2: Axiomas OWL (STAAB; STUDER, 2004) e (AZEVEDO, 1994)

A OWL tem como componentes classes, que representam conceitos atômicos, propriedades, que representam relações binárias entre conceitos ou entre um conceito em um tipo de dado, e indivíduos que representam instâncias dos conceitos definidos pelas classes. Para representar conhecimento por meio destes componentes, Staab e Studer (2004) e Azevedo (1994), a OWL-DL utiliza-se dos construtores e axiomas listados nas tabelas 3.1 e 3.4.2.2:

Axiomas OWL		
Axioma	**DL Sintaxe**	**Exemplo**
subClassOf	$C_1 \subseteq C_2$	$Humano \subseteq Animal \cap Bipede$
equivalentClass	$C_1 \equiv C_2$	$Homem \equiv Humano \cap Male$
disjointWith	$C_1 \subseteq \neg C_2$	$Macho \subseteq \neg Femea$
sameIndividualAs	$\{X_1\} \equiv \{X_2\}$	Ronaldinho Fenômeno $\equiv$ R9
differentFrom	$\{X_1\} \subseteq \neg \{X_2\}$	$\{Fernanda\} \subseteq \neg \{Eder\}$
subPropertyOf	$P_1 \subseteq P_2$	temFilho $\subseteq$ temParente
equivalentProperty	$P_1 \equiv P_2$	apresentaSinopse $\equiv$ apresentaResumo
inversepropertyOf	$P_1 \equiv P_2^-$	$temAscendencia \equiv temDescendencia^-$
transitiveProperty	$P_1^+ \subseteq P_2$	$temAscendencia^+ \subseteq temAscendencia$
functionalProperty	$C_1 \subseteq \leq 1 P_1$	Pessoa $\subseteq \leq 1$ temMae
inverseFunctionalProperty	$C_1 \subseteq \leq 1\ P_1^-$	CPF $\subseteq \leq 1\ identificaUmUnicoIndividuo^-$

3.5 Ferramentas para Desenvolvimento e Avaliação de Ontologias

Além de um processo que concentre as atividades relacionadas à engenharia de ontologias e de métodos que possibilitem o seu desenvolvimento e avaliação, fazem-se necessárias ferramentas na construção de uma ontologia, pois elas fornecem, conforme indica Pressman (2006), apoio automatizado ou semi-automatizado para execução das atividades e tarefas propostas.

No contexto das ferramentas utiizadas na engenharia de ontologias, destacam-se aquelas utilizadas:

> Na modelagem, especificação, formalização e manutenção de ontologias. Exemplos: OntoEdit [7], WebOnto, WebOde e Protégé.
>
> Na avaliação, verificação e manipulação (por meio regras e axiomas, para aquisição de conhecimento) de ontologias, as chamadas máquinas de inferência (reasoners). Exemplos: Fact, Racer e Pellet.

Além das ferramentas, ainda devem ser consideradas as linguagens de consulta para ontologias. Essas auxiliam na sua avaliação e também na sua utilização, além de

[7] http://www.ontoknowleddge.org/tools/ontoedit.shtml

permitir explicitar conhecimento tácito por meio das consultas/buscas em um domínio de conhecimento representado. Como exemplo de linguagens de consulta para ontologia podem-se citar a SeRQL, a RDQL e a SPARQL.

A seguir são descritos mais detalhadamente o *framework* Protégé, a máquina de inferência Pellet e a linguagem de consulta para ontologias SPARQL. Esses foram utilizados no desenvolvimento e avaliação da InfoSecRM. O Protégé foi escolhido devido a oferecer diversos *plugins* que auxiliam no processo de desenvolvimento e manutenção de ontologias, por ter interface intuitiva, possuir ampla documentação e permitir integração com máquinas de inferência e linguagems de consulta a ontologias. Pellet foi a motor de inferência adotado devido a implementar todo o dialeto OWL-DL (ou seja, expressividade SHOIN(D)). E escolheu-se a SPARQL como linguagem de consulta a ontologia desenvolvida devido ao fato de ser uma recomendação W3C, possuir a capacidade de fazer inferências e pode ser integrada ao Protégé.

3.5.1 Protégé

O Protégé[8] não é somente um editor de ontologias, mas um *framework* para construção de aplicações baseadas em domínios de conhecimento. Ele é baseado em java, um software livre e de código aberto. Este ambiete permite o desenvolvimento de ontologias na linguagem OWL por exemplo e a sua exportação para outros formatos.

Por meio de plugins, como indicado em Horridge et al. (2004b), pode-se adicionar funcionalidades que tornam este *framework* ainda mais robusto, como a incorporação de ferramentas de visualização (como o Jambalaya e o OWLViz), de avaliação (utilização de máquinas de inferência como a Pellet) e de consulta (como a utilização da SPARQL) às ontologias criadas.

A versão do Protégé utilizada na construção da InfoSecRM foi a 3.4.7, cuja interface é ilustrada na figura 3.4.

Na figura 3.4, na parte superior, são exibidas as abas de visualização dos principais componentes propostos em uma ontologia OWL (classes, propriedades e instâncias), a aba Form que auxilia quando das instanciações dos conceitos no próprio framework Protégé (apresentando formulários para cada conceito a ser instanciado, onde podem

[8]http://protege.stanford.edu/

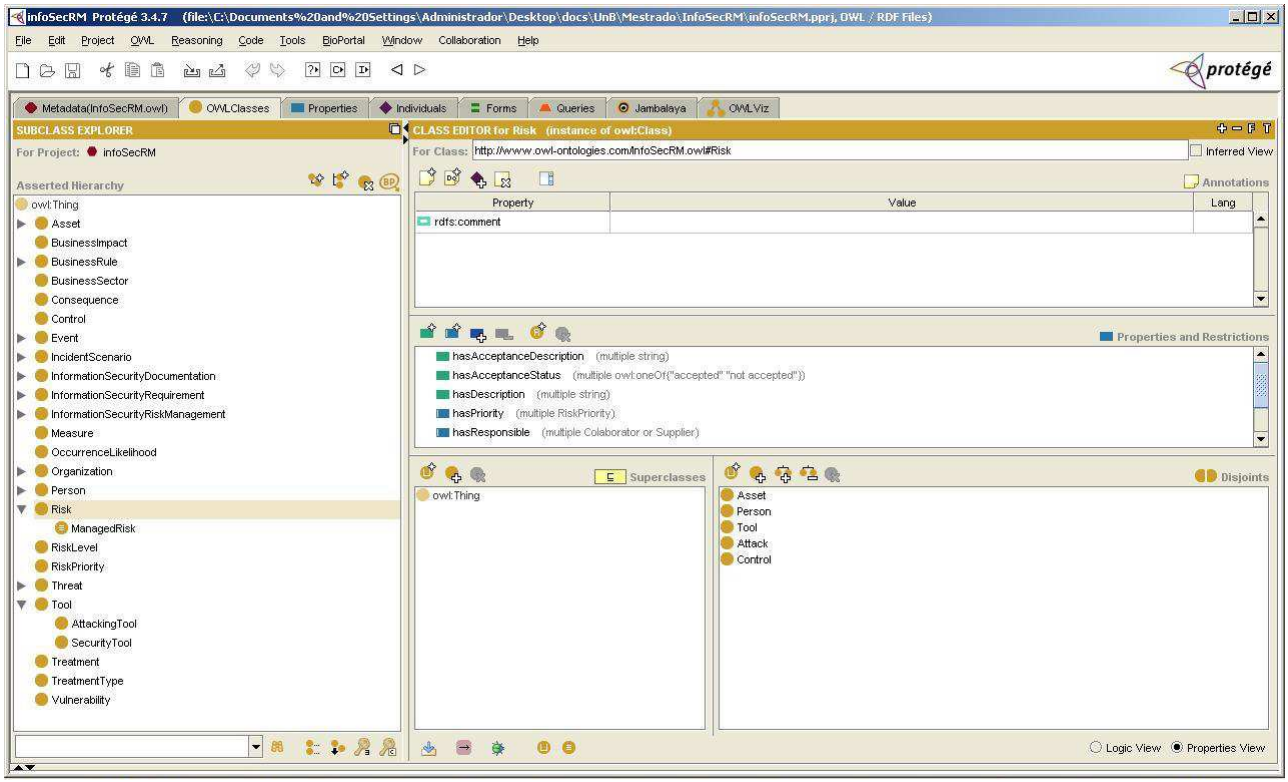

Figura 3.4: Tela da Interface do Protégé 3.4.7

ser preenchidos todos os dados relativos à instância, seus relacionamentos e propriedades) e as demais abas relativas a plugins que foram incorporados (como o Jambalaya e o OWLViz que permitem a visualização das classes e seus relacionamentos como grafos). À esquerda, são exibidas algumas das classes criadas para a ontologia proposta por este trabalho e ao centro algumas das propriedades e relacionamentos da classe Risk.

3.5.2 Pellet

Conforme indica Dentler et al. (2011), máquinas de inferência (motores de inferência, ou ainda mecanismos de inferência) têm por função raciocinar sobre axiomas e assertivas explicitas, ou seja, processar e apresentar informações que podem estar implícitas em uma ontologia (gerando assim novos conhecimentos sobre este domínio).

A Pellet é uma máquina de inferência, desenvolvida em Java e de código aberto, que permite avaliar ontologias OWL-DL na plenitude da expressividade SHOIN(D). Expõe Sirin et al. (2007a), que Pellet realiza checagem de consistência, verificação de hierarquias e de potenciais instanciações por exemplo.

A figura 3.5 ilustra uma verificação de consistência utilizando o mecanismo de inferência Pellet versão 1.5.2 (versão utilizada no desenvolvimento da InfoSecRM) dentro do *framework* Protégé.

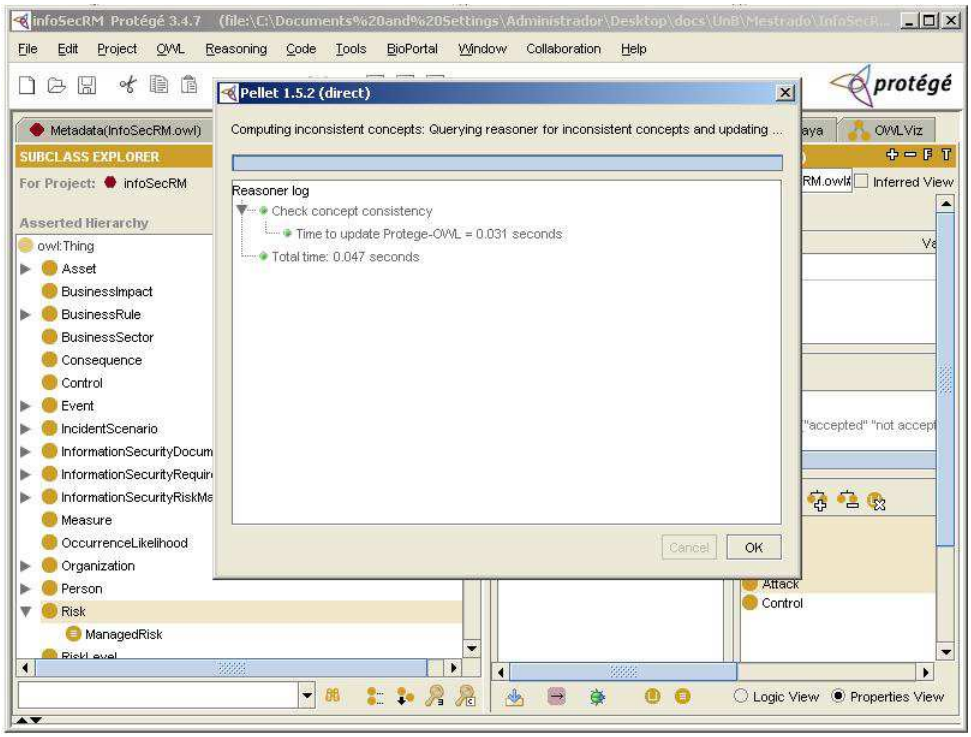

Figura 3.5: Verificação de consistência utilizando a máquina de inferência Pellet

3.5.3 SPARQL

Conforme já citado, a SPARQL **Query Language** é uma linguagem de consulta a dados armazenados no formato RDF (um grafo RDF é uma tripla -Sujeito, predicado, objeto). Esta linguagem, como exposto em Sirin e Parsia (2007) e Prud'hommeaux e Seaborne (2008), tem sintaxe muito similar à *Structured Query language* (SQL) e seus comandos seguem o modelo SELECT A FROM B WHERE C.

O código **??** exemplo abaixo refere-se a uma busca por riscos considerados de nível alto, onde, à frente de SELECT, é indicado o tipo de dado que espera-se que a consulta retorne e à frente de WHERE, o padrão de tripla a ser utilizado como filtro na consulta à base de dados RDF da ontologia.

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

```
\label{cod1}
\caption{Código SPARQL exemplo}
```

3.6 Comentários Finais

Este capítulo apresentou as ontologias como forma de representação de conhecimento. Foram apresentados as metodologias possíveis de serem adotadas como processo de desenvolvimento de ontologias, os formalismos e linguagens que podem ser adotados como métodos nestes processos de construção e as tecnologias que podem ser utilizadas como ferramentas para auxiliar e/ou automatizar as atividades e tarefas da engenharia de ontologias.

O capítulo 4 apresenta como se deu o desenvolvimento da ontologia InfoSecRM (planejamento, especificação, conceitualização, formalização etc).

4 O processo de desenvolvimento da InfoSecRM

A arquitetura das informações que compõem o domínio de conhecimento em segurança da informação tem como base variadas fontes, expõe Schumacher (2003), e representações que possam defini-la de maneira formal e auxiliem no compartilhamento e no processamento deste conhecimento caracterizam-se como constructos relevantes neste contexto.

As ontologias apresentam-se então como uma alternativa aderente a esta necessidade. Por meio das conceitualizações formais por elas propostas, podem-se estabelecer representações semânticas possíveis de serem processadas pelos agentes relacionados a este contexto. Isto facilita não só o compartilhamento e a aquisição de conhecimento sobre este domínio, mas também a institucionalização dos processos gerenciais envolvidos.

Neste contexto, este capítulo descreve o processo de desenvolvimento da InfoSecRM que é uma ontologia que descreve o conhecimento relacionado ao processo de gestão de riscos de segurança da informação (nos moldes do proposto na norma ISO 27005 ABNT (2008)). São apresentadas as atividades/fases deste processo com base nas metodologias adotadas, juntamente com os principais conceitos da ontologia.

4.1 O processo

Conforme descrito no capítulo 3, para a elaboração da InfoSecRM foram utilizadas as perspectivas de três abordagens, a **metodologia methontology** como o processo que define o arcabouço das atividades a serem realizadas, **o método 101** para definir o "como fazer"de algumas destas atividades (na conceituação por exemplo, onde os passos são bem detalhados) e a **metodologia proposta por Fox e Gruninger no projeto TOVE**, com a utilização das idéias de cenários de motivação e de questões de competência por ela proposta.

As atividades realizadas no processo de desenvolvimento da InfoSecRM são descritas nas seções subsequentes:

4.1.1 Planejamento e Especificação

Foram definidas as atividades e recursos a ser utilizados no processo de desenvolvimento da InfoSecRM, seu escopo e seus objetivos. Para isso inicialmente foram elencados os seguintes cenários de motivação:

> O conhecimento em segurança da informação deriva de diversas fontes e uma conceitualização que represente os conceitos inerentes a este domínio de forma padronizada pode facilitar o compartilhamento deste conhecimento em ambientes corporativos.
>
> A gestão de riscos de segurança da informação (GRSI) é um dos principais elementos em um processo de gestão de segurança da informação (GSI), assim uma ontologia que permita operar sobre os conceitos e atividades deste tipo de processo auxiliam na identificação das necessidades e prioridades de segurança da informação de uma organização.
>
> A utilização de processos padronizados para a gestão de riscos, como o proposto pela norma ABNT NBR ISO/IEC 27005, auxiliam no mapeamento dos conceitos e atividades relevantes a serem descritas pela conceitualização proposta pela ontologia.

A partir destes foram definidos:

> ***Domínio:*** especificamente a Gestão de Riscos de Segurança da Informação, porém como este este processo está inserido em um domínio maior, de forma pontual descreve-se também a Gestão de Segurança da Informação.
>
> ***Objetivo:*** estabelecer uma estrutura de representação para informações e atividades relacionadas à GRSI.
>
> ***Usuários:*** reponsáveis pela segurança da informação e tecnologia da informação em organizações, e estudiosos e especialistas neste domínio.
>
> ***Tarefas e Atividades:*** as tarefas e atividades para o desenvolvimento são algumas daquelas indicadas pelas fases de cada uma das três metodologias utilizadas. Estas são descritas neste capítulo.

Recursos: para a construção e avaliação da InfoSecRM foram utilizados os seguintes recursos: *framework* Protégé versão 3.4.7, a máquina de inferência Pellet 1.5.2, as linguagens OWL-DL, RDF e SPARQL e as normas da família ISO 27000.

4.1.2 Aquisição do Conhecimento

Para a aquisição do conhecimento relacionado ao domínio escolhido foram pesquisados vários livros, normas, padrões e glossários de termos. As principais fontes foram as normas da família ISO 27000. Além das fontes citadas, o conhecimento representado pela ontologia foi amplamente discutido no curso de especialização em Gestão de Segurança da Informação e Comunicações que faz parte do Programa de Formação de Especialistas para a Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações. Esse é promovido pelo Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil, mais especificamente pelo Departamento de Segurança da Informação e Comunicações vinculado a este gabinete.

As atividades desta fase também contemplam a elaboração das chamadas questões de competência, que são os questionamentos para os quais a ontologia proposta deverá oferecer respostas. Estas questões auxiliam a definir os conceitos que serão representados.

As questões de competência definidas são listadas a seguir:

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

Quais os cenários de incidentes de segurança da informação caso se concretizem podem ter como consequência impactos na reputação da organização?

Qual o perfil de riscos de segurança da informação de uma organização?

Qual a probabilidade de ocorrência de um cenário de incidente de segurança da informação?

Qual o nível de impacto de um cenário de incidente de segurança da informação?

Quais as consequências de um cenário de incidente de segurança da informação específico?

Quais as vulnerabilidades associadas a um ativo?

Quais ameaças podem explorar uma vulnerabilidade?

Quais os controles existentes/previstos para tratar um risco?

Quais os principais documentos em que se baseia a gestão de riscos de segurança da informação em uma organização?

Qual o tipo de tratamento dado a um risco em específico?

Quais riscos foram avaliados como de prioridade alta?

Qual o contexto estabelecido para a GRSI em uma organização?

Pra responder algumas das questões acima, era necessária a instanciação dos conceitos e relacionamentos representados pela ontologia. Foram utilizados então, para verificar as consultas na linguagem SPARQL, as informações obtidas/geradas quando de um processo, ainda de nível inicial, de GRSI em uma gerencial operacional do departamento de TI de uma organização, conforme descrito no capítulo 5 que descreve a avaliação da ontologia desenvolvida.

4.1.3 Conceituação

Nesta fase, de acordo com o domínio de conhecimento a ser representado, são elencados os conceitos, as propriedades a eles inerentes, axiomas e restrições.

A InfoSecRM teve como idéia base o conceito de risco associado a um cenário de incidente de segurança da informação. Assim, um **risco** está associado a um **cenário de incidente de segurança da informação**, que conforme explicado no capítulo 2, é uma descrição fictícia de um potencial conjunto de incidentes que uma organização pode estar sujeita. A este cenário são associados os **ativos**, as **vulnerabilidades** inerentes a esses, as **ameaças** que podem explorar essas últimas, os **controles**, assim como as **consequências**, **probabilidade de ocorrência** e medida de **impacto**. Com base nestes é estimado o **nível de risco**. A representação do núcleo da InfoSecRM descrito pode ser observada na figura 4.1.

Além da idéia central, outra elemento importante na concepção da InfoSecREM, foi o processo de gestão de riscos de segurança da informação definido na norma ISO 27005.

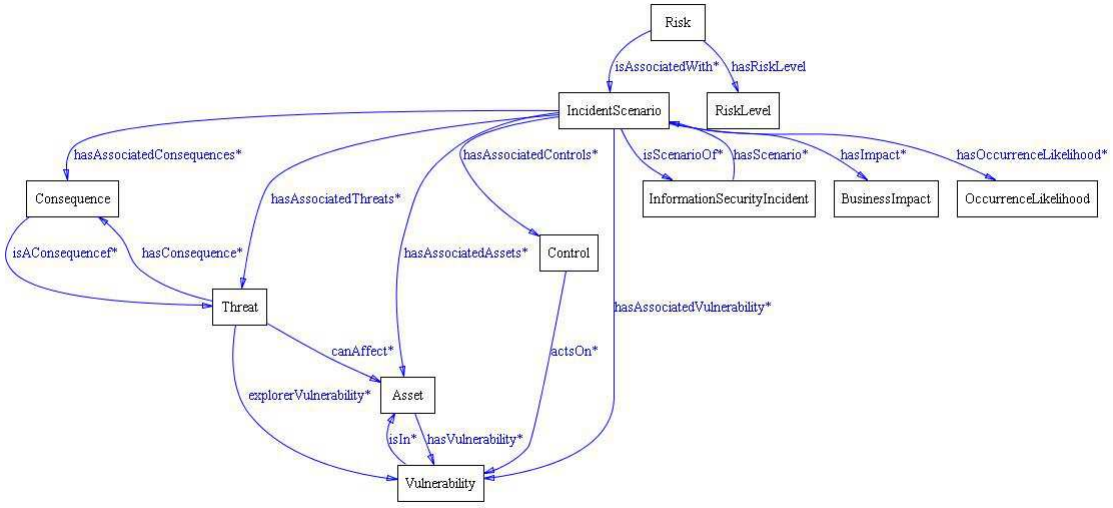

Figura 4.1: Representação do núcleo de conceitos e relacionamentos que formam a base da InfoSecRM

Consoante ao descrito do capítulo 2, este processo conta com as atividades de: definição de contexto, análise de riscos, avaliação de riscos, tratamento de riscos e aceitação de riscos (além da análise e monitoramento do processo, e da comunicação e consulta ao longo de todas as atividades). O contexto deste processo, estabelecido também com base nos conceitos de cenário de incidentes de segurança da informação e de risco, é ilustrado na figura 4.2.

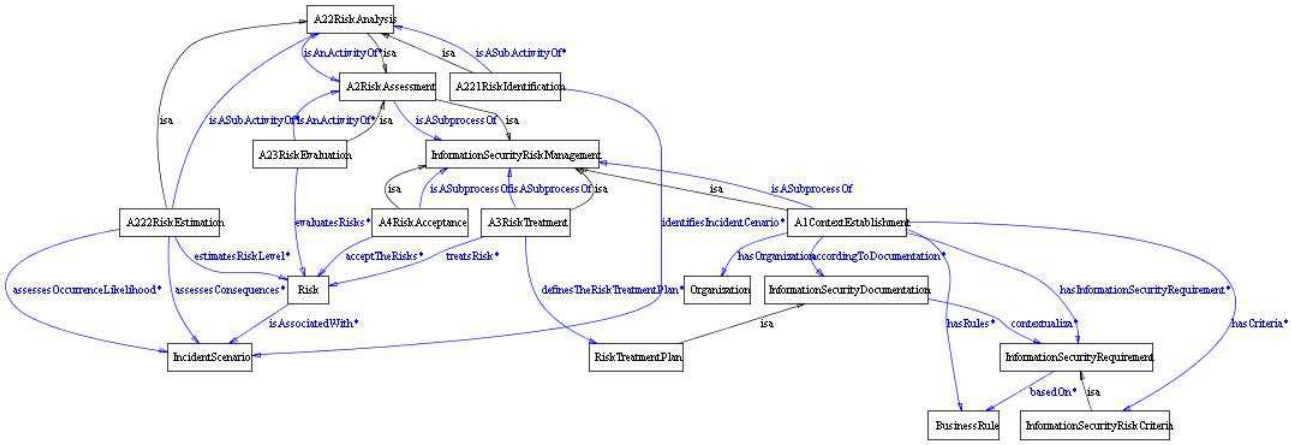

Figura 4.2: Representação do processo de GRSI proposto na norma ISO 27005 (ABNT, 2008)

Com base nas duas idéias citadas, desenvolveu-se a InfoSecRM. Para isso foi utilizada a abordagem *middle-out* proposta em Uschold e Grüninger (1996). Nessa perspectiva, são definidos os principais conceitos do domínio a ser representado e após a idéia central ser estabelecida, esta é desenvolvida até o nível de detalhe requerido para a representação. Esta abordagem, em comparação às abordagens *bottom-up* e *top-down*, proporciona à ontologia desenvolvida imperfeições reduzidas por detalhar os

conceitos (seja por generalização ou especialização) apenas até o nível requerido pela representação que a conceitualização da ontologia se propõe, o que proporciona um esforço global menor e menos retrabalho.

Dessa forma, foram elencados os termos mais importantes a serem representados pela ontologia, definidas classes e suas hierarquias, e as propriedades de cada classe e suas restrições.

Os termos elencados foram obtidos com base nas idéias citadas acima e com fóco nas questões de competência definidas na fase de aquisição do conhecimento. Estes termos são os seguintes: risco, cenário de incidente de segurança da informação, incidente de segurança da informação, ativo, vulnerabilidade, ameaça, controle, consequência, impacto, probabilidade de ocorrência, política de segurança da informação, requisitos de segurança da informação, organização, confidencialidade, integridade, disponibilidade, regras de negócio, gerenciamento de riscos de segurança da informação, análise de riscos, avaliação de riscos, tratamento de riscos, aceitação de riscos, nível de risco.

A InfoSecRM possui 88 classes, 68 relacionamentos e 9 atributos. A representação completa de toda a InfoSecRM pode ser visualizada no Anexo A desta dissertação. A seguir as principais classes desta ontologia, as hierarquias a que estão sujeitas (quando for o caso), seus propriedades e suas respectivas restrições são descritas.

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

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

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

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

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

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

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

hasDescription - apresenta uma string de descrição do risco.

Figura 4.3: Hierarquia da classe **Risk**

A classe **Risk** (classe nomeada) possui a hierarquia representada na figura 4.3. As suas subclasses (classes definidas) identificam quais atividades já foram realizadas sobre um determinado risco. Por exemplo: a classe **TreatedRisk** possui as condições necessárias e suficientes, indicadas na equação 4.2:

$$\begin{aligned}\text{TreatedRisk} \equiv \text{Risk} \cap \forall\ \text{isAssociatedWith.IncidentScenario} \cap \exists\ \text{hasLevel.RiskLevel} \cap \\ \exists\ \text{hasPriority.RiskPriority} \cap \exists\ \text{hasTreatment.Treatment}\end{aligned} \tag{4.1}$$

Denota-se, das condições expressas acima, que os riscos inferidos como indivíduos da classe **TreatedRisk** já passaram pela atividade de tratamento de risco.

Classe IncidentScenario - Representam os cenários de incidentes de segurança da informação associados a cada elemento da classe **Risk**. Possui as seguintes propriedades:

isScenarioOf - associa uma cenário de incidente de segurança da informação a incidentes.

isAScenarioAssociatedWith - identifica o risco ao qual um cenário está associado.

hasAssociatedAsset, hasAssociatedThreat, hasAssociatedVulnerability, hasAssociatedControl, hasAssociatedConsequence - indicam respectivamente os ativos, as ameaças, as vulnerabilidades, os controles e as consequencias associados a um cenário.

hasImpact - indica o impacto que um cenário de incidente de segurança da informação, caso o(s) incidente(s) associado(s) se concretize(m), pode trazer aos objetivos da organização.

hasOccurenceLikelihood - indica a probabilidade de o cenário se concretizar.

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

hasDescription - apresenta uma descrição do cenário de incidente de segurança da informação.

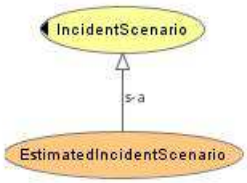

Figura 4.4: Hierarquia da classe IncidentScenario

A classe **IncidentScenario** possui a hierarquia representada na figura 4.4. A subclasse **EstimatedIncidentScenario** identifica um cenário que teve sua probabilidade de ocorrência e impacto estimados, conforme definido pelas condições necessárias e suficientes explicitadas na equação 4.3.

$$EstimatedIncidentScenario \equiv IncidentScenario \cap \exists hasImpacto.BusinessImpact \cap \exists hasOccurrenceLikelihood.OccurrenceLikelihood \quad (4.2)$$

Classe InformationSecurityIncident - Representam os incidentes de segurança da informação. Possui as seguintes propriedades:

hasScenario - relacionamento inverso ao relacionamento *isScenarioOf*, indica o cenário associado a um incidente.

precedesInformationSecurityIncident - indicam os incidentes de segurança da informação que são precedidos por um incidente de segurança da informação em específico.

precedesInformationSecurityEvent - indicam os eventos de segurança da informação que são precedidos por um incidente de segurança da informação em específico.

isPrecededBy - indica os eventos que precederam um incidente de segurança da informação.

isCausedBy - indica as ameaças que causaram um incidente de segurança da informação.

hasDescription - apresenta uma descrição do incidente de segurança da informação.

hasDate - indica a data em que o incidente ocorreu.

A classe **InformationSecurityIncident** está inserida na hierarquia representada na figura 4.5. Esta hierarquia justifica-se pelo explicado no capítulo 2, onde expôs-se que um **evento de segurança da informação** caracteriza-se por uma "ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação", ao passo que **incidente de segurança da informação** diz respeito apenas aquele(s) evento(s) que tenham grande probabilidade de impactar o negócio e a segurança da informação de uma organização.

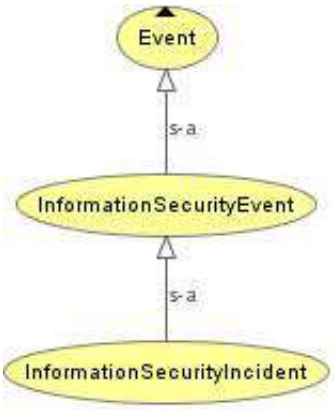

Figura 4.5: Hierarquia da classe InformationSecurityIncident

Classe Asset - Representa os ativos de uma organização. Possui as seguintes propriedades:

hasResposible - identifica os colaboradores ou fornecedores responsáveis pelo ativo.

hasVulnerability - representa as vulnerabilidades presentes em um ativo.

hasDescription - descreve o ativo.

hasValue - indica o valor que aquele ativo tem para a organização.

A classe **Asset** possui a hierarquia representada na figura 4.6, que no primeiro nível está subdividida em serviços (classe **Service**), informações (classe **Information**), ativos intangíveis (classe **IntangibleAsset**), ativos físicos (classe **PhysicalAsset**), processos (classe **Process**), colaboradores (classe **Colaborator**) e softwares (classe **software**). As subclasses da classe **Asset** foram definidas segundo o sugerido no Anexo B da norma ISO 27005 ABNT (2008).

Figura 4.6: Hierarquia da classe Asset

Classe Vulnerability - Representa as vulnerabilidades inerentes aos ativos de uma organização. Possui as seguintes propriedades:

ixExploredBy - identifica as ameaças que podem explorar uma vulnerabilidade.

isIn - relacionamento com a classe **Asset**, que indica que uma determinada vulnerabilidade é inerente a um determinado ativo (é a propriedade inversa à propriedade *hasVulnerability).*

hasDescription - descreve a vulnerabilidade.

A classe **Vulnerabilityy** possui uma subclasse denominada **ConsideredVulnerability**, que é uma classe definida. Esta classe denota aquelas vulnerabilidades que têm pelo menos uma potencial ameaça que possa explorá-la.

Classe Threat - Representa as ameaças que podem explorar vulnerabilidades inerentes a ativos de uma organização. Possui as seguintes propriedades:

canAffect - indica os ativos que podem ser afetados por uma determinada ameaça.

causesEvent - indica os eventos que podem ser causados por uma ameaça.

exploresVulnerability - indica a(s) vulnerabilidade(s) explorada(s) por um ativo .

hasConsequence - indica as consequencias que podem ocorrer se a amaeça explorar uma vulnerabilidade.

hasDescription - apresenta uma descrição da ameaça.

hasOrigin - indica qual a origem da ameaça, se acidental, intensional ou ambiental.

A classe **Threat** possui a hierarquia representada na figura 4.7, que indica que uma ameaça pode ser provocada por um atacante (que pode ser um Hacker, um Cracker, um criminoso digital ou um terrorista, como indicado no Anexo C da norma ISO 27005 ABNT (2008), um ataque ou por causas naturais.

Classe Control - Representa os controles elencados para sanar vulnerabilidades inerentes a ativos de uma organização. Possui as seguintes propriedades:

actsOn - indica as vulnerabilidades sobre as quais o controle atua.

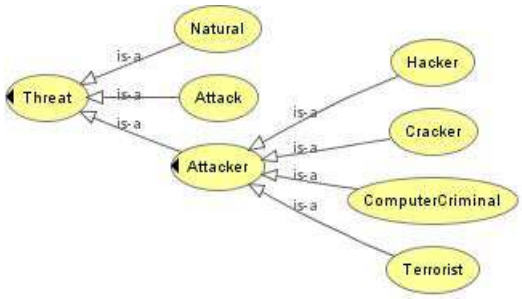

Figura 4.7: Hierarquia da classe Threat

usesTool - identifica as ferramentas utilizadas na aplicação de um determinado controle.

hasDescription - descreve o controle.

hasImplementationStatus - indica se o controle está implementado, parcialmente implementado ou ainda não foi implementado.

Classe Consequence - Representa as consequências que podem ocorrer caso ameaça(s) explore(m) vulnerabilidade(s). Possui as seguintes propriedades:

isConsequenceOf - indica a qual ameaça uma consequencia está associada..

impactsOn - indica se a consequencia ira impactar na disponibilidade, integridade, confidencialidade, autenticidade, privacidade, objetivos de negócio, retorno sobre o investimento (ROI), continuidade do negócio e/ou oportunidade de negócio.

hasDescription - descreve a consequência.

Classe InformationSecurityRiskManagement - Representa o processo de gestão de riscos de segurança da informação. Possui as seguintes propriedades:

hasMonitoringAndAnaysisBy - identifica colaboradores responsáveis/envolvidos nas atividades de monitoração e analise do processo de gestão de riscos de segurança da informação.

hasDescription - descreve o processo de gestão de riscos de segurança da informação em uma organização.

A classe **InformationSecurityRiskManagement** possui a hierarquia representada na figura 4.8. As subclasses **A1ContextEstablishment**, **A2RiskAssessment**, **A3RiskTreatment** e **A4RiskAcceptance** indicam as atividades de um processo de GRSI segundo a norma ISO 27005 ABNT (2008) e a ordem em que elas ocorrem. Nestas classes (e subclasses, no caso da classe **A2RiskAssessment**) estão representadas por meio de suas respectivas propriedades, as tarefas de cada atividade, conforme pode ser verificado na figura 4.2

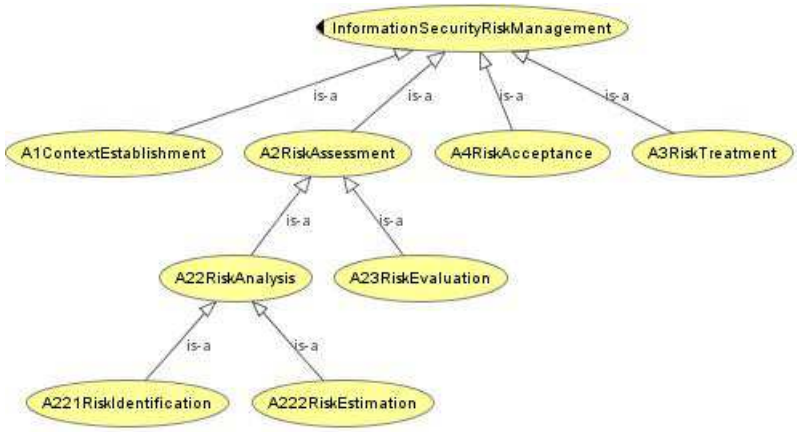

Figura 4.8: Hierarquia da classe InformationSecurityRiskManagement

4.1.4 Formalização

Utilizou-se lógica descritiva para formalizar a InfoSecRM (OWL-DL) e a expressividade obtida foi SHOIN(D). O código foi gerado automaticamente por meio da modelagem feita no *framework* Protégé (todo o código OWL da InfoSecRM pode ser visualizado no Anexo B).

4.1.5 Integração

No desenvolvimento da InfoSecRM foi utilizada a classe **Tool** tal qual definida na CoreSec, proposta em Azevedo (1994), porém sem as subclasses que indicam os tipos de ferramentas de segurança. Além disso, para seguir os propósitos de representação da ontologia construída neste trabalho, esta classe foi também definida como uma subclasse da classe **Software**, que é um tipo de ativo.

Também da CoreSec, foi utilizada a idéia de um incidente de segurança da informação

preceder ou ser precedido por outro incidente. Porém na InfoSecRM, esta idéia foi ampliada para representar a concepção de que um incidente de segurança da informação pode ser precedido de um outro incidente ou de um evento de segurança da informação, que pode, por sua vez ser precedido de um outro evento de segurança da informação ou de outro tipo de evento (as propriedades *precedesInformationSecurityIncident* e *precedesInformationSecurityEvent* indicam esta noção).

4.1.6 Implementação

Para a implementação da InfoSecRM foram utilizadas as linguagem OWL-DL e SPARQL, o *framework* Protégé 3.4.7 e a máquina de inferência Pellet 1.5.2.

4.1.7 Manutenção

Durante a construção da InfoSecRM, os conceitos por ela representados foram bastante pesquisados o que influenciou diretamente em alterações nas representações desta ontologia (atividades da fase de aquisição do conhecimento que ocorre ao longo de todo processo de desenvolvimento). Além disso, mudanças no domínio de GRSI podem resultar em necessidade de alteração da ontologia para descrever a conceitualização proposta corretamente.

4.1.8 Avaliação

A avaliação da InfoSecRM é apresentada no capítulo 5.

4.1.9 Documentação

Durante o processo de desenvolvimento da InfoSecRm, foram elaborados a documentação listada abaixo:

Documento de planejamento e especificação.

Documentação de aquisição do conhecimento.

Hierarquia de classes e relacionamentos, ambos ilustrados no Anexo A.

Código OWL da ontologia (constante no Anexo B).

4.2 Comentários Finais

Este capítulo apresentou o processo de desenvolvimento definido para a construção da InfoSecRM. Foram descritos os principais conceitos e idéias que deram origem a esta ontologia. Foram apresentadas as questões de competência que auxiliaram na definição destes conceitos e também algumas das classes que os representam.

Juntamente com a exposição das classes, foram descritas as propriedades de cada uma delas. Estas propriedades explicitam as relações semânticas entre os conceitos relacionados ao domínio de gestão de riscos de segurança da informação representados pela ontologia. Ainda foram discutidas as fases de formalização, integração, implementação, manutenção e documentação.

A avaliação da InfoSecRM é discutida no capítulo 5.

5 A Avaliação da InfoSecRM

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

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

Considerando o exposto por Vrandeĉić (2009), onde é afirmado que a validação requer uma colaboração entre os profissionais responsáveis pelo desenvolvimento da ontologia e os profissionais do domínio mapeado, para as atividades de validação, adotou-se a abordagem proposta em Obrst et al. (2007), que avalia a capacidade da ontologia criada de responder a algumas das questões de competência (definidas na fase de aquisição de conhecimento descrita no capitulo 4). Nesse sentido, a ontologia foi utilizada nas atividades de um processo, ainda de nível inicial, de GRSI em uma gerencia operacional do departamento de TI de uma organização governamental, com vistas a instanciar suas classes e relacionamentos, e assim, permitir as pesquisas pelas questões de competência. Para efeitos de sigilo e segurança das informações desta organização, sua identidade foi suprimido desta dissertação.

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

A verificação e a validação da InfoSecRM são descritas nas seções seguintes.

5.1 Verificação

Conforme indicado na seção anterior, a verificação foi realizada em duas etapas, sob duas perspectivas diferentes: avaliação da InfoSecRM quanto a critérios pré-definidos (denominada neste trabalho como verificação qualitativa) e comparação da InfoSecRM com outras ontologias relacionadas ao domínio de segurança da informação (denominada verificação quantitativa). Essas são descritas nas subseções que se seguem.

5.1.1 Verificação Qualitativa

Os critérios utilizados nesta atividade foram:

acurácia, adaptabilidade, transparência, granularidade e adequação organizacional, elencados em Vrandeĉić (2009), e;

os propostos em Lozano-Tello e Gomez-Perez (2004), que são: classificação, consistência, expressividade, precisão, satisfação, usabilidade e utilidade.

Estes critérios são descritos a seguir:

Acurácia - critério relacionado a verificar se a ontologia captura e representa de forma correta o domínio modelado.

Adaptabilidade - refere-se a verificar se uma ontologia permite expansão ou especialização de sua estrutura, sem que seja necessário remoção de seus axiomas, e ainda se pequenas modificações podem alterar signitivamente a conceitualização da ontologia.

Transparência, usabilidade e utilidade - indicam se a ontologia comunica as relações semânticas propostas para o domínio e se esta comunicação se dá de forma compreensiva e efetiva, facilitando a sua utilização nos propósitos para os quais ela foi desenvolvida.

Granularidade e Precisão - referem-se, respectivamente, a verificar a amplitude do conceitualização proposta e o seu nível de detalhe, e a checar se a ontologia apresenta apenas conceitos e/ou propriedades necessárias à representação proposta.

Adequabilidade Organizacional - como as ontologias são artefatos que auxiliam o compartilhamento de conhecimento, pois as conceitualizações por elas concebidas tendem a ser um consenso de compreensão nos domínios por elas representados, este requisito tem por objetivo checar a facilidade de inserção da ontologia em ambientes organizacionais e cooperativos.

classificação - este critério tem como objetivo verificar as classes e suas respectivas hierarquias em uma ontologia.

Consistência - verifica se os axiomas, conceitos e propriedades da ontologia não contêm contradições em suas representações.

Expressividade - verifica a expressividade utilizada frente a expressividade possibilitada pela linguagem de representação utilizada.

Satisfação - checa a necessidade e possibilidade de um conceito ser instanciado.

Para a verificação dos critérios classificação, consistência e expressividade foi utilizada a máquina de inferência Pellet versão 1.5.2, que foi executada por meio do Protégé. Foram obtidos os seguintes resultados:

Foi verificado que InfoSecRM é consistente, conforme indica a figura 5.1.

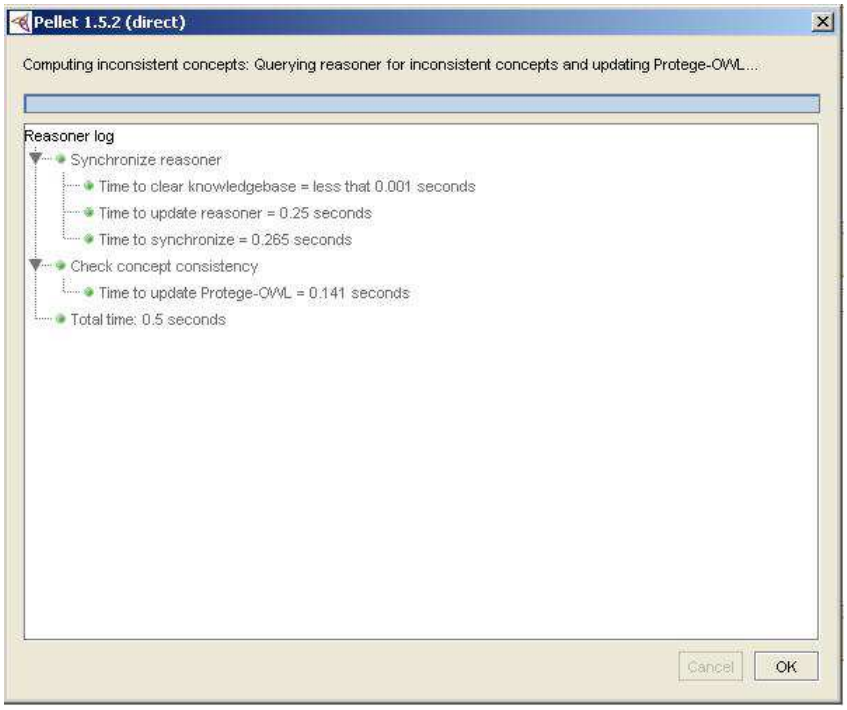

Figura 5.1: Resultado da verificação de consistência da InfoSecRM pela máquina de inferência Pellet

A classificação da taxonomia também foi alvo de verificação, onde foi checada a consistência dos conceitos, inferida a hierarquia da ontologia e a equivalência entre classes, conforme ilustra a figura 5.2.

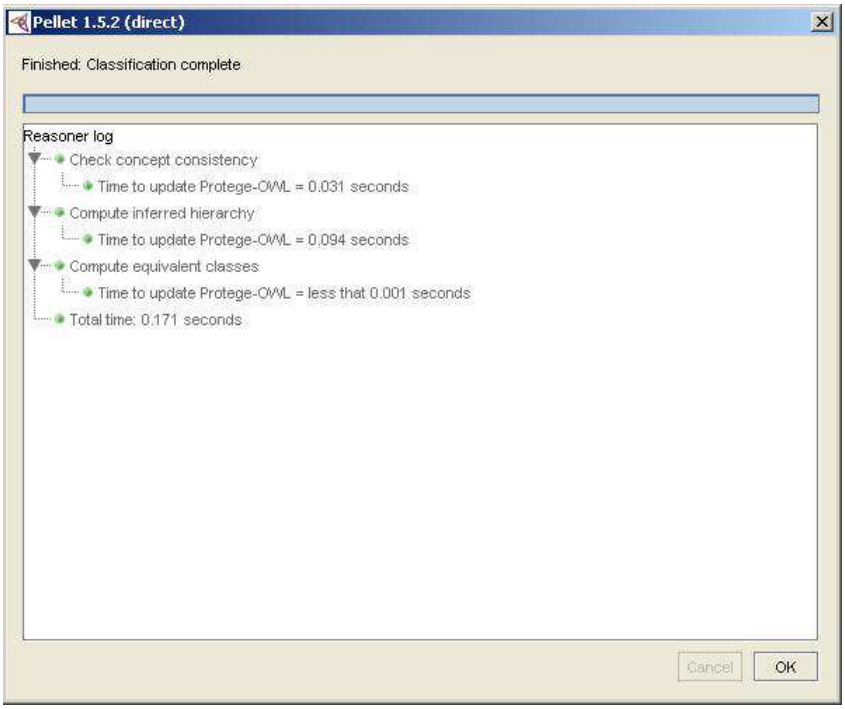

Figura 5.2: Resultado da classificação da taxonomia da InfoSecRM pela máquina de inferência Pellet

O motor de inferência ainda possibilitou verificar que a InfoSecRm possui interseção e disjunção entre classes, quantificação universal e existencial, negação, regras transitivas, inversas e funcionais, hierarquia de classes e de propriedades, definição de classes por enumeração, restrições de cardinalidade e utilização de tipos de dados. Em outras palavras, identificou-se que ontologia verificada possui expressividade SHOIN(D) que é a maior expressividade que a OWL-DL pode proporcionar. A figura 5.3 ilustra estas verificações.

Quanto aos outros critérios, verificaram-se as seguintes características:

O domínio de gestão de riscos de segurança da informação (GRSI) é representado de forma correta, e compreende as idéias centrais indicadas e discutidas no capítulo 4. O processo de gestão de riscos modelado compreende as atividades descritas em ABNT (2008) e também observa-se que a foi explicitada as relações entre os riscos e conceitos como incidente de segurança da informação e seus cenários, ativos, ameaças e vulnerabilidades. Assim, observa-se que a ontologia foi desenvolvida com acurácia frente ao domínio representado.

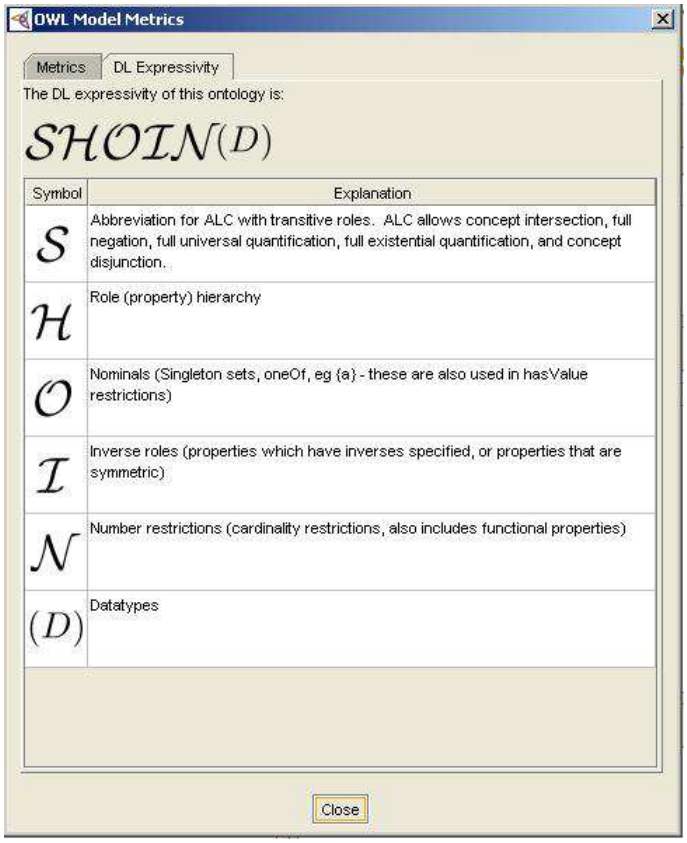

Figura 5.3: Expressividade da InfoSecRM verificada pela máquina de inferência Pellet

No processo de desenvolvimento da InfoSecRM prezou-se por garantir representações consensuais do domínio de gestão de riscos de segurança da informação. Além disso, adotou-se a perspectiva de criar uma subclasse de um conceito relevante da representação sempre que fosse necessário indicar condições necessárias e suficientes para subconjuntos deste conceito. Por exemplo, a classe **Risk** que representa o conceito risco, tem como uma de suas subclasses a classe **EstimatedRisk**, que conceitua os riscos que passaram pela fase de análise de riscos (ou seja, riscos que tem um nível de risco associado). Diante o exposto, somado ao fato de a InfoSecRM ser uma ontologia de domínio, observa-se que a conceitualização por ela proposta permite expansões e especializações em sua estrutura (capacidade de adaptabilidade). Como exemplos de conceitos que podem ser expandidos ou especializados podem-se citar: a classe **Tool** e a classe **Vulnerability**, dentro das quais podem ser criadas subclasses para indicar tipos, ou ainda a classe **OcurrenceLikelihood** para indicar outro tipo de métrica para a probabilidade de ocorrência dos cenários de incidentes.

Por meio da utilização de toda a expressividade possibilitada pela linguagem OWL-DL pode-se representar uma conceitualização compreensível que comunica bem os aspectos do domínio mapeado (transparência). Esta estrutura apresenta-se de forma intuitiva

por meio dos conceitos e propriedades, além de apresentar descrições destes componentes por meio de propriedades de anotações, o que facilita a utilização desta ontologia (utilidade e usabilidade).

A InfoSecRM descreve o domínio de gestão de riscos de segurança da informação em toda sua amplitude, sem com tudo entrar em um nível de detalhe exagerado (nível de granularidade). Todos os conceitos representados são de fato utilizados em um processo de gestão de riscos e são relevantes para a conceitualização modelada (concisão).

Conforme indicado a ontologia desenvolvida representa os conceitos relacionados ao domínio de GRSI com base em definições que são consensuais nesta área. Isso facilita o compartilhamento de conhecimento, visto permitir operar sobre um vocabulário comum. Assim, considerando estes aspectos, a sua utilização tende a ser facilitada em um ambiente organizacional e colaborativo.

Algumas dimensões deste critério têm também grande relação com o objeto da validação, que é o conteúdo e a visão de mundo representada. Por isto alguns deles são também citados nas atividades de validação.

5.1.2 Verificação Quantitativa

Para a verificação quantitativa, considerando a abordagem, proposta por Maedche, Maedche e Staab (2002), de comparar a InfoSecRM com outras ontologias, adotou-se como métrica a indicada em Ning e Shihan (2006), que é realizada com base nos indicadores:

Quantidade de classes nomeadas;

Média de propriedades do tipo objeto (relacionamentos);

Nível da ontologia quanto a hierarquias - relacionamento *is-a* (é um);

Classe com maior número de relacionamentos *is-a* da ontologia;

Foram utilizadas para este comparativo as ontologias propostas em Martimiano (2006) e Azevedo (1994), respectivamente, OntoSec e CoreSec. A OntoSec representa parte

Tabela 5.1: Média de propriedades objeto por classes nomeadas em cada ontologia

Ontologias	**CN**	**PO**	**MPO**
CoreSec	86	39	0,45
OntoSec	59	28	0,47
InfoSecRM	82	67	0,82

do domínio de segurança da informação, porém seu foco é na gestão de incidentes de segurança da informação. Já a CoreSec tem como domínio a segurança da informação, propõe uma representação com conceitos de alto nível, facilitando a sua utilização em avaliação de riscos e gestão de segurança da informação.

Com relação às classes nomeadas, observou-se que InfoSecRM apresenta 82, frente à 85 da CoreSec e à 59 da OntoSec, conforme indica a tabela 5.1.

A média de propriedades do tipo objeto por classes nomeadas, é calculada segundo a equação 5.1:

$$MPO = \frac{PO}{CN} \tag{5.1}$$

Onde MPO é a média de propriedades do tipo objeto, PO a quantidade de propriedades do tipo objeto e CN a quantidade de classes nomeada.

Com relação a este indicador, a InfoSecRM apresentou a média 0,82, a maior entre as três ontologias. A OntoSec e a CoreSec, apresentaram, respectivamente, 0,45 e 0,47. A tabela 5.1, indica a quantidade de propriedades objeto, a quantidade de classes nomeadas e a média de propriedades objeto por classe em cada ontologia.

A representação de uma hierarquia de classes de uma ontologia pode ser representada por um grafo direcionado, onde os vértices ou nós são as classes e as arestas são as relações *is-a* (é um) que ligam uma subclasse em um nível n a nó pai em um nível n-1[1]. Assim, quanto mais níveis uma ontologia possuir, mais os seus respectivos conceitos foram especializados.

[1]Por exemplo, na figura 5.4, a classe **Hardware** está no quarto nível e está relacionada à classe **PhysicalAsset**, por meio de uma relação *is-a*, que está no terceiro nível.

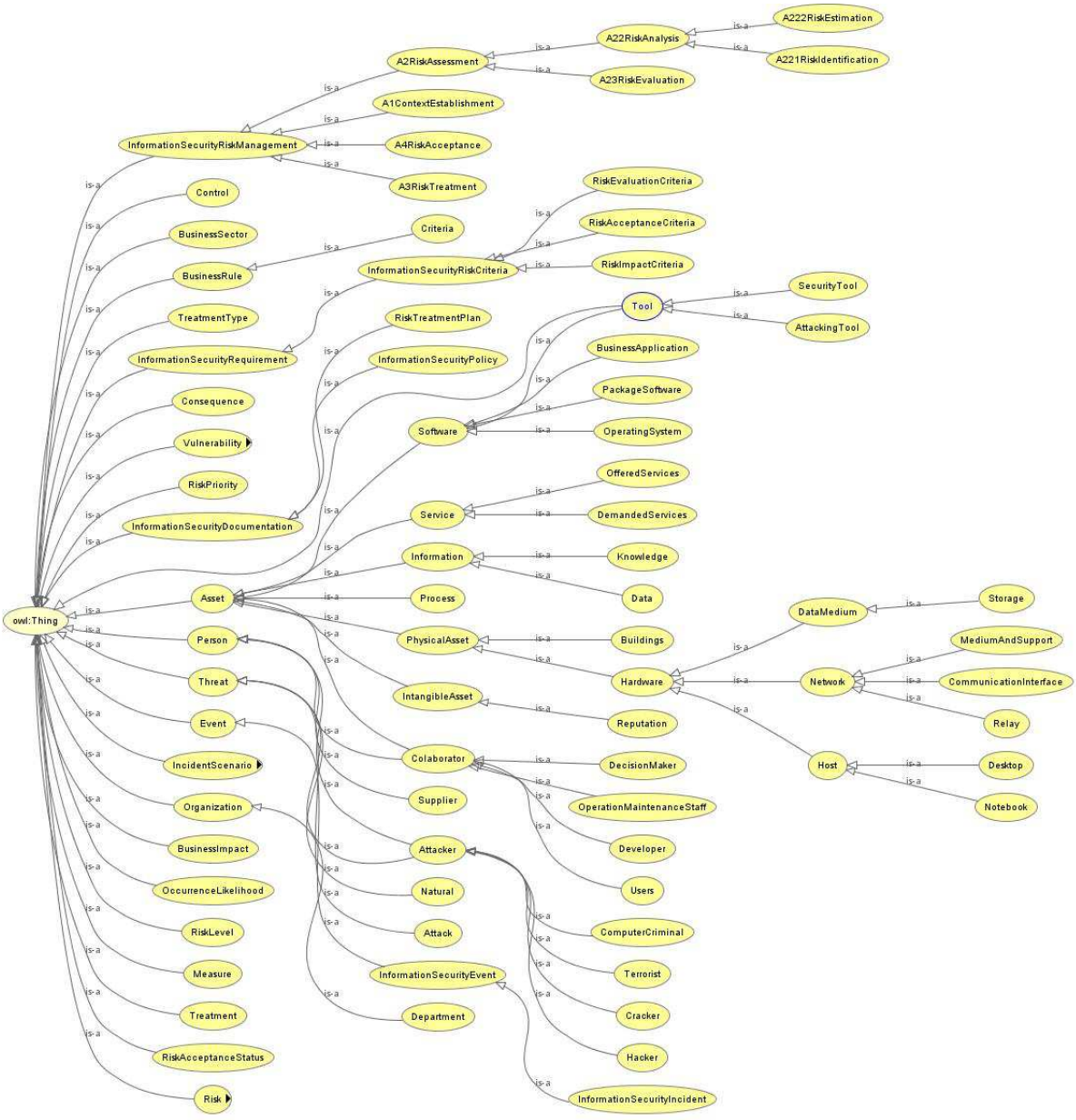

Figura 5.4: Hierarquia de classes nomeadas da ontologia InfoSecRM, gerada por meio do *plugin* OWL Viz Ellson et al. (2001)

Na figura 5.4, que indica a hierarquia de classes da InfoSecRM, podem-se observar seis níveis de classes, onde o primeiro nível, que contém apenas a classe **Thing** (classe padrão criada pelo *framework* Protégé como nó raiz em todas as ontologias), é o situado mais à esquerda e o sexto é aquele situado mais à direita. A OntoSec e a CoreSec possuem ambas cinco níveis, como ilustram as figuras 5.5 e 5.6.

Na InfoSeRM, a classe que possui maior número de relacionamentos do tipo *is-a* é a classe **Asset** (7 relacionamentos, ou seja, possui 7 subclasses diretas), enquanto que na OntoSec é a classe NonSelfReplicating (9 relacionamentos) e na CoreSec é a classe **Malware** (9 relacionamentos). Estas classes e suas hierarquias diretas são ilustradas nas figuras 5.7 5.8 e 5.9.

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

Observou-se também que a InfoSecRM apresenta maior média de propriedades do tipo objeto por classes nomeadas. Este número é um indicador de que a conceitualização proposta por esta ontologia representa bem as relações semânticas entre os conceitos do domínio representado, como pode ser observado nas propriedades que relacionam os conceitos ativo, vulnerabilidade, ameaças, consequência, incidente, cenário de incidente e riscos por exemplo.

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

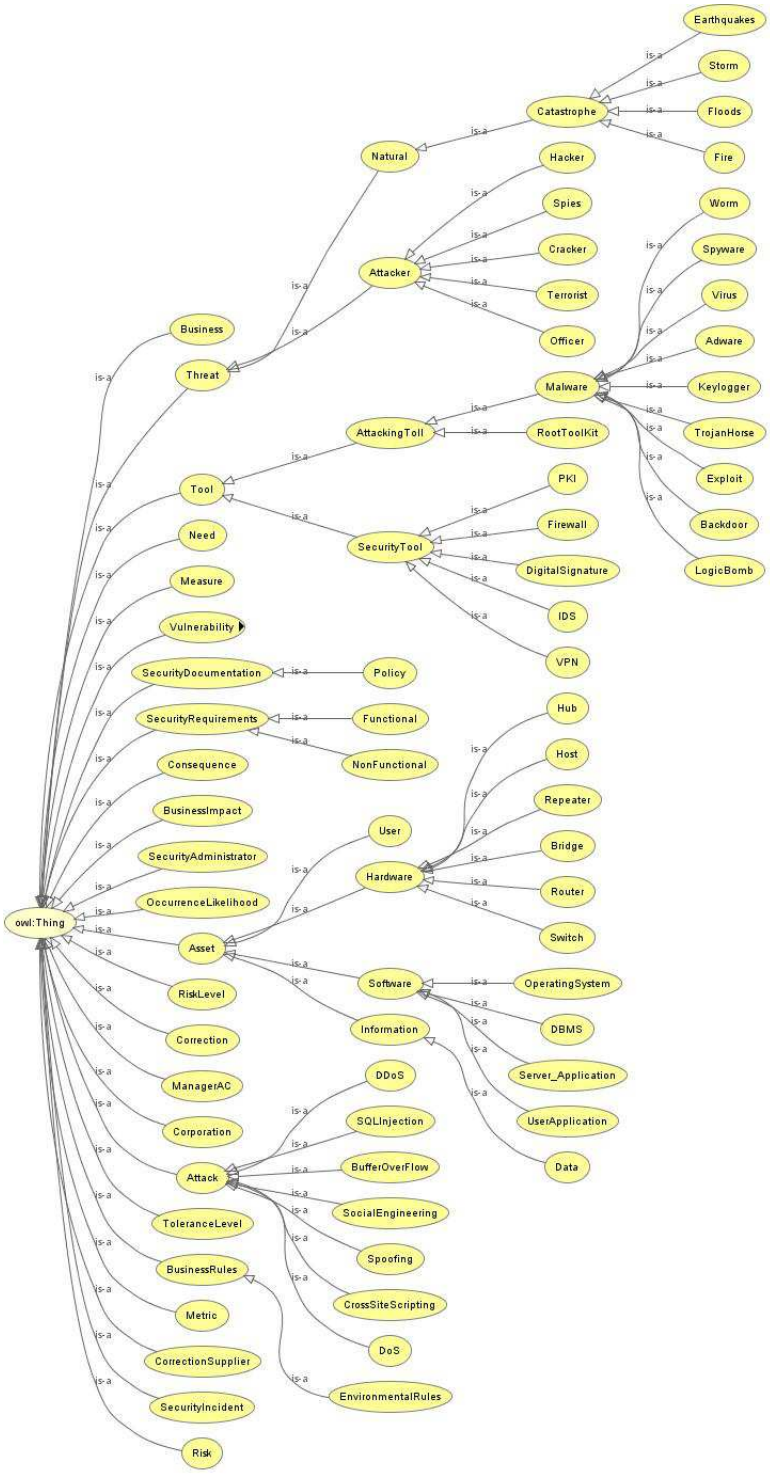

Figura 5.5: Hierarquia de classes nomeadas da ontologia CoreSec, gerada por meio do *plugin* OWL Viz Ellson et al. (2001)

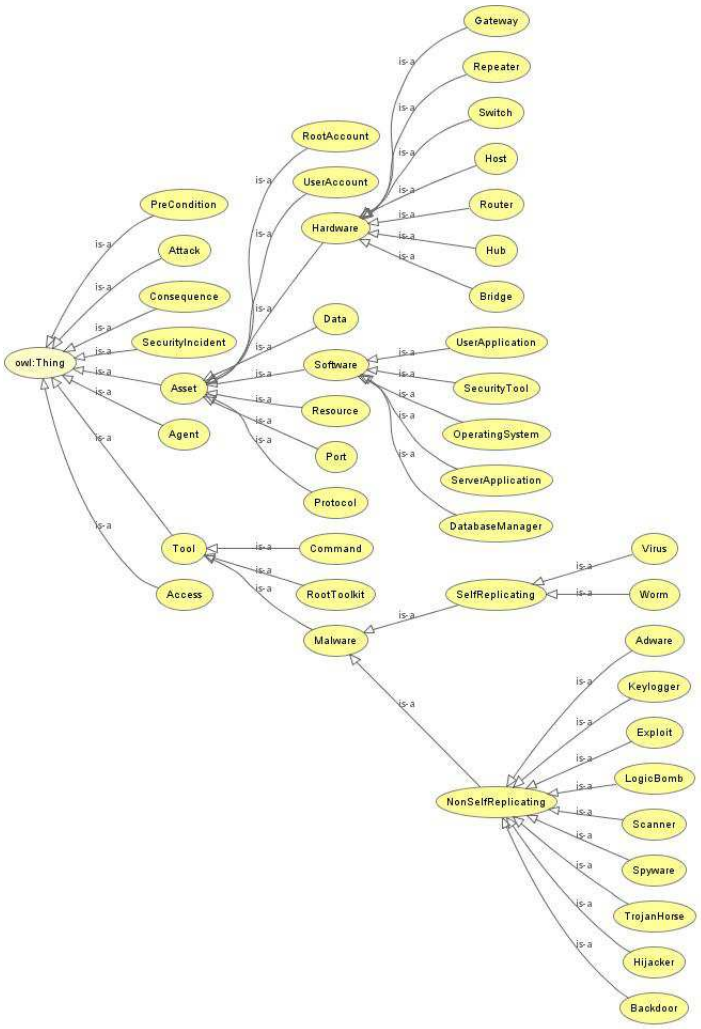

Figura 5.6: Hierarquia de classes nomeadas da ontologia OntoSec, gerada por meio do *plugin* OWL Viz Ellson et al. (2001)

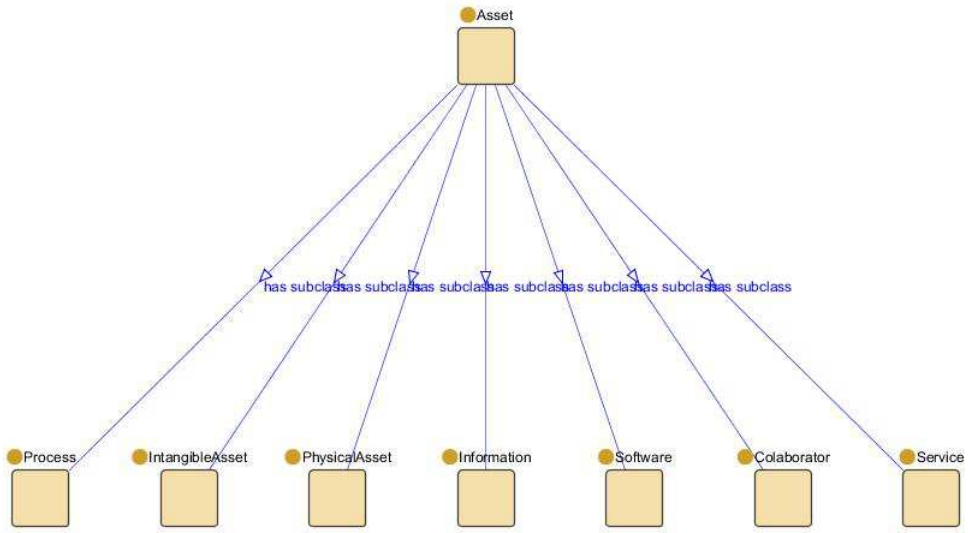

Figura 5.7: Hierarquia direta da classe Asset, gerada por meio do *plugin* Jambalaya (STOREY et al., 2002)

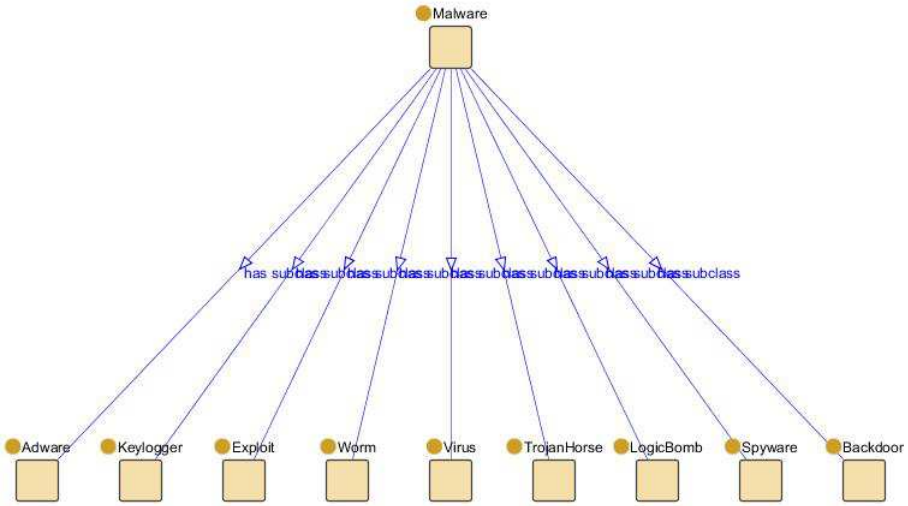

Figura 5.8: Hierarquia direta da classe Malware, gerada por meio do *plugin* Jambalaya (STOREY et al., 2002)

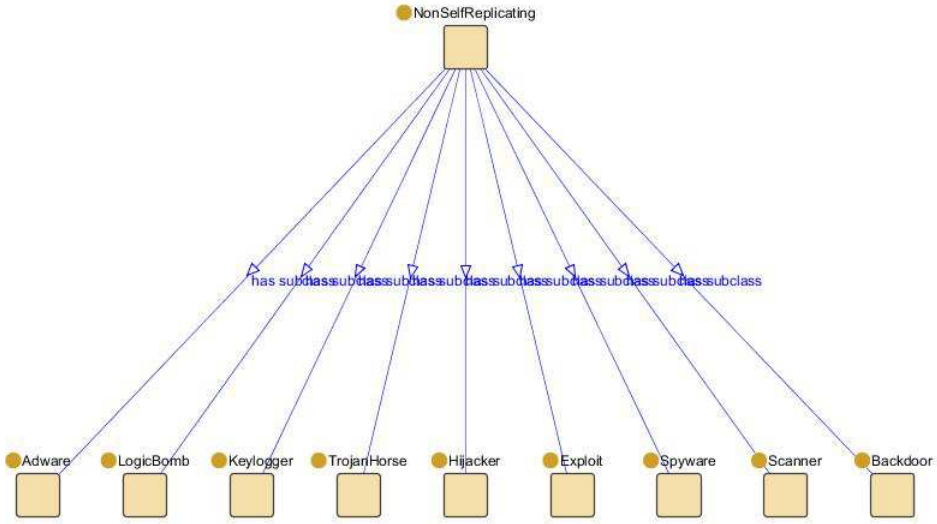

Figura 5.9: Hierarquia direta da classe NonSelfReplicating, gerada por meio do *plugin* Jambalaya (STOREY et al., 2002)

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

5.2 Validação

Para a validação foram realizadas avaliações sob duas perspectivas diferentes:

Utilização da ontologia no processo de gestão de riscos de segurança da informação de uma organização, onde suas classes e propriedades foram instanciados, e por meio destes indivíduos foram respondidas algumas das questões de competência propostas no capítulo 4;

Comparação da ontologia com documentos sobre o domínio modelado.

Cada uma dessas é descrita nas subseções seguintes:

5.2.1 Utilização da InfoSecRM em um ambiente corporativo

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

Os conceitos e relacionamentos representados na InfoSecRM foram instanciados representando as ações de processo de GRSI com as limitações descritas acima. Esta

instanciação, ou seja, a criação de indivíduos para as classes e propriedades definidas pela ontologia, deu-se por meio da utilização de formulários que podem ser editados e configurados na aba Forms do framework Protégé. Esta aba exibe, como formulários configuráveis, as propriedades objeto e de dados de cada classe, segundo às restrições e axiomas definidos para cada uma destas propriedades.

As figuras 5.10 e 5.11 por exemplo, ilustram, respectivamente, a aba Forms sendo utilizada para configurar os formulários da classe **Asset** e aba Individuals sendo utilizada para criar um indivíduo da classe **Asset** por meio dos formulários configurados. Pode-se observar que a classe **Asset** possui um formulário para cada uma das suas propriedades descritas no capítulo 4, que são *hasResponsible*, *hasValue*, *hasDescription* e *hasVulnerability*.

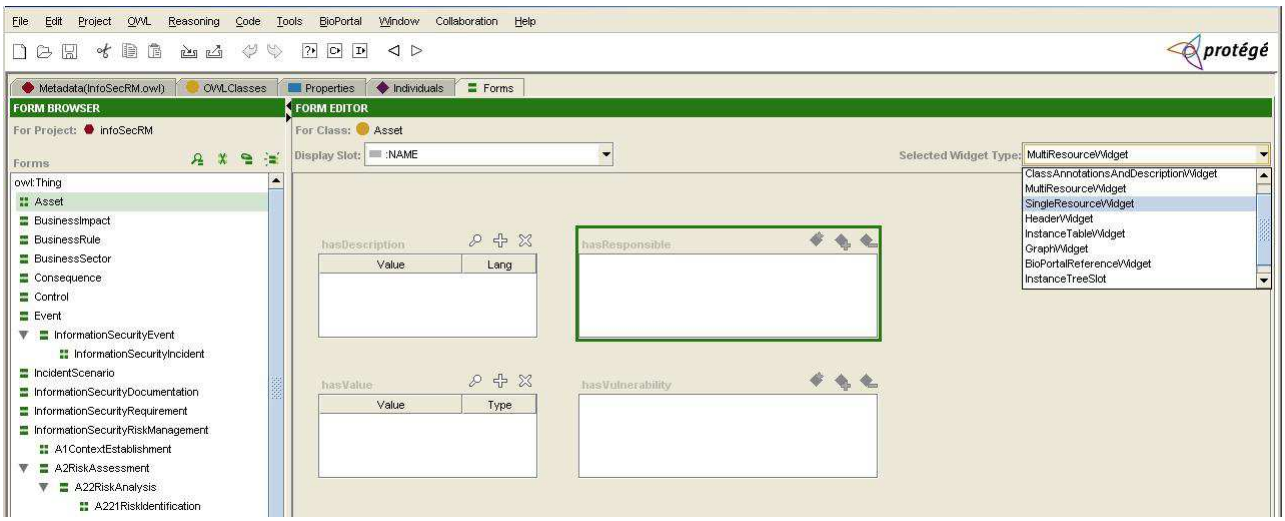

Figura 5.10: Aba Forms sendo utilizada na configuração dos formulários para a classe Asset

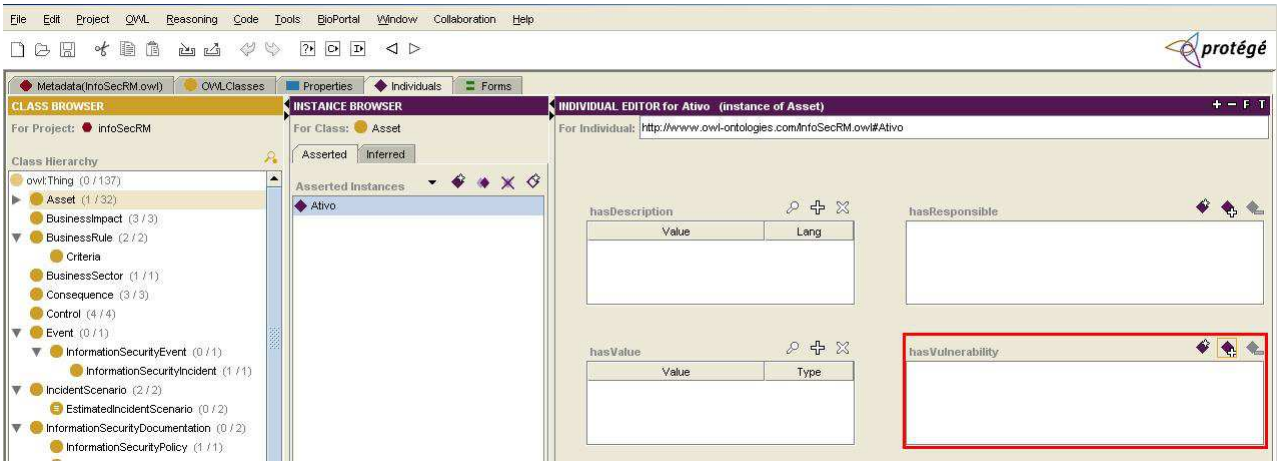

Figura 5.11: Aba Individual sendo utilizada criar um indíviduo da classe Asset por meio dos formulários configurados

Por meio das instanciações realizadas nos moldes descritos nas figuras 5.10 e 5.11, pode-

se responder às questões de competência definidas no capítulo 4 na fase de aquisição do conhecimento. Algumas das consultas realizadas por meio da linguagem SPARQL que pesquisam a ontologia por respostas para estas questões são citadas a seguir:

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

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

Quais os cenários de incidentes de segurança da informação caso se concretizem podem ter como consequência impactos na reputação da organização?

```
SELECT ?IncidentScenario
WHERE {?IncidentScenario:hasAssociatedConsequences:Reputação_Manchada}
```

Quais as vulnerabilidades associadas a um ativo?

```
SELECT ?Vulnerability
WHERE {?Vulnerability:isIn:Ativos_de_Rede}
```

Quais ameaças podem explorar uma vulnerabilidade?

```
SELECT ?Threat
WHERE {?Threat:exploresVulnerability:Quantidade_reduzida_de_licenças_disponíve
```

Quais os controles existentes/previstos para tratar um risco?

```
SELECT ?Control
WHERE {?Control:actsOn:Tratamento_de_Risco_de_vazamento_de_informações_sigilos
```

Quais riscos foram avaliados como de prioridade alta?

```
SELECT ?Risk
WHERE {?Risk:hasPriority:High_Priority}
```

Qual o contexto estabelecido para a GRSI em uma organização?

```
SELECT ?A1ContextEstablishment
WHERE {?A1ContextEstablishment:hasOrganization:Nome_Organização}
```

As respostas a questões de competência, como as citadas, permitem, não apenas verificar que os conceitos necessários à representação do domínio de GRSI foram modelados pela ontologia, como também auxiliar os usuários da InfoSecRM a buscar informações nas bases de conhecimento geradas sobre a estrutura que ela representa. Um outro recurso que auxiliou bastante nestas atividades foi a aba Query (ilustrada na figura 5.12), que é uma Application programming interface (API) do framework Protégé. Por meio dessa, podem ser realizadas buscas na ontologia, porém sem o formalismo da sintaxe da linguagem SPARQL, apenas especificando classes, propriedades e valores para estas propriedades. A primeira questão de competência, por exemplo, poderia ser pesquisada como também indicado na figura 5.12.

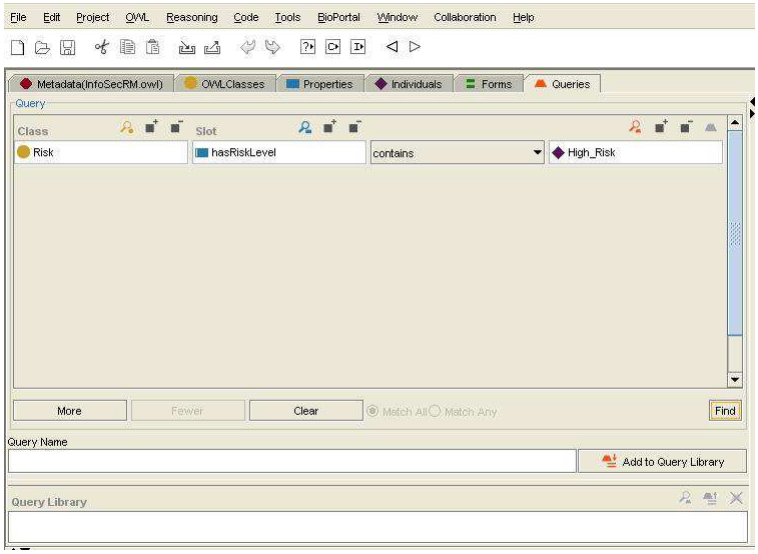

Figura 5.12: Consulta à InfoSecRM por Riscos de nível alto utilizando a aba Query

Foi possível observar que a utilização da InfoSecRm permitiu auxiliar na implementação da GRSI, ao armazenar as informações e indicar as atividades e escopo deste processo, apresentando-se como uma estrutura padronizada por meio da qual pode-se operar sobre os conceitos de segurança da informação relacionados à gestão de riscos e permitir o compartilhamento das informações relacionadas.

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

Uma sugestão dos colaboradores que utilizaram a InfoSecRM, foi que ao invés de representar apenas os responsáveis por um ativo ou risco (que na ontologia representam os responsáveis por executar uma tarefa por exemplo), quando aplicável, fossem representados os indivíduos que devem ser informados e consultados, os que são responsáveis pela execução, e aquele que é o responsável em última instância pela tarefa, ativo, risco etc, nos moldes dos papéis propostos em uma matriz RACI (*Responsible, Accoutable, Consulted* e *Informed*).

5.2.2 Comparação da ontologia com documentos sobre o domínio modelado

Para esta abordagem de validação foram utilizados os seguintes documentos:

> ABNT NBR ISO/IEC 27002 - Código de Prática para a Gestão da Segurança da informação ABNT (2005).
>
> ABNT NBR ISO/IEC 27001 - Sistemas de Gestão de Segurança da informação ABNT (2006).
>
> ABNT NBR ISO/IEC 27005 - Gestão de Riscos de Segurança da informação ABNT (2008).

Estas normas foram utilizadas como os documentos sobre o domínio representado por se tratarem, como exposto no capítulo 2, de integrantes da família de normas ISO 27000 que destina-se a auxiliar organizações a implementar e operar um sistema de gerenciamento de segurança da informação (SGSI). Como já exposto, um processo de GRSI é um fator crítico a um SGSI, pois por meio do mesmo pode-se implementar e monitorar os controles de segurança da informação de uma organização, além de promover ações que os melhorem continuamente.

Ao observar os termos e definições explicitados em ABNT (2005) e ABNT (2006), verificam-se termos recorrentes como ativo, evento de segurança da informação e incidente de segurança da informação, além de algumas atividades importantes de um processo de GRSI (o que denota a importância da GRSI em um SGSI) como análise de riscos, avaliação de riscos e tratamento de riscos. Estes conceitos básicos estão representados na ontologia desenvolvida, além de representações de propriedades e de outros

conceitos a eles relacionados. A classe **InformationSecurityIncident**, por exemplo, é representada como uma subclasse de **InformationSecurityEvent**, justamente pela definição de que um incidente de segurança da informação diz respeito a um evento de segurança da informação, ou um conjunto deles, que tenha grande probabilidade de impactar o negócio e a segurança da informação de uma organização. As atividades de gestão de riscos também estão definidas como subclasses de **InformationSecurity-RiskManagement**, indicando que são atividades de um processo de GRSI.

Além destes termos e definições, ao longo de ABNT (2005) e ABNT (2006), são discutidos objetivos de controle críticos a um SGSI tal como gestão de ativos, controles de acesso, gestão de continuidade do negócio etc, e todos estes utilizam com base para suas ações e controles a política de segurança da informação. Este documento também é um elemento importane para a GRSI e por isso está representado na ontologia (classe **InformationSecurityPolicy**, subclasse de **InformationSecurityDocumentation**), indicando por meio do relacionamento *contextualiza*, que a política de segurança da informação reúne os requisitos de segurança da informação imporantes em uma organização.

Com relação à ABNT (2008), que fornece diretrizes para o gerenciamento de riscos de segurança da informação, verifica-se que os conceitos utilizados nas atividades do processo de GRSI por ela proposto, como organização, regras de negócio, impacto, controle, cenário de incidentes de segurança da informação etc, estão representados na InfoSecRM como pode ser verificado na figura 4.1, no capítulo 4.

Ainda com relação à ABNT (2008), observa-se também que na representação das atividades de GRSI foi levado em conta a relação de entrada e saída de informações entre cada uma delas (por meio da propriedade *hasImput*). Por exemplo, a classe **A222RiskEstimation** relaciona-se à Classe **A221RiskIdentification** por meio da propriedade *hasInput*. Além disso, cada atividade é relacionada apenas aos conceitos realmente utilizados nela. Por exemplo, até à atividade de identificação de riscos, não há ainda a idéia de risco concebida, mas apenas de cenários de incidentes com ativos, vulnerabilidades, ameaças etc associados, desta forma a classe **A221RiskIdentification** não tem nenhuma propriedade que estabeleça um relacionamento entre ela e a classe **Risk**.

Ao conceito de risco são associados, tal qual proposto em ABNT (2008), um nível de risco na atividade de estimativa do riscos (classe **RiskLevel**), uma prioridade na

atividade de avaliação de riscos (Classe **RiskPriority**), um tratamento na atividade de tratamento de riscos (classe **Treatment**) e um status de aceitação de riscos na fase de aceitação de riscos (classe **RiskAcceptanceStatus**). Estas propriedades permitem à máquina de inferência indicar por quais atividades um risco já passou, gerando mais informações para os usuários da ontologia.

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

5.3 Comentários Finais

Este capítulo apresentou a avaliação da InfoSecRm. A avaliação foi dividida entre verificação e validação, que referem-se, respectivamente, à avaliação da corretude da representação e à observar se a ontologia de fato representa o domínio modelado.

Foram apresentadas as abordagens e métricas utilizados e após isso, foram descritos e analisados os resultados obtidos.

As conclusões permitidas pelo trabalho desenvolvido nesta dissertação e os trabalhos futuros identificados são apresentados no capítulo 6.

6 Conclusões e Trabalhos Futuros

O volume de informações utilizadas em um processo de gestão de riscos de segurança da informação é vasto e de fontes variadas, como dados sobre ativos, vulnerabilidades associadas, potenciais ameaças, regras de negócio etc. Não obstante, este tipo de processo de gestão tem como base vários componentes e os relacionamentos entre eles. A compreensão, por parte dos agentes envolvidos, dos conceitos e definições associados a estes componentes é essencial para a efetividade dos controles e ações associados a este contexto.

Assim foi proposta uma ontologia para gerenciamento de riscos de segurança da informação, denominada InfoSecRM, com vistas a representar os conceitos e propriedades citados e auxiliar no armazenamento das informações relacionadas em bases de conhecimento.

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

Uma conceitualização formal, desenvolvida e avaliada segundo um processo bem definido, que apresenta uma representação das informações relacionadas à gestão de riscos de segurança da informação. Por meio desta representação, promove-se a aquisição e o compartilhamento de informações e conhecimento neste domínio.

Promoção do processo de GRSI em organizações por meio da utilização InfoSecRM, que como visto pode contribuir na implementação de uma gestão de riscos e na tomada de decisões, e ser utilizada na criação e estruturação de uma base de conhecimento de riscos de segurança da informação.

Discussão de metodologias, métodos e ferramentas para o desenvolvimento e avaliação de ontologias.

Reúso de Conhecimento e informações, visto que a ontologia desenvolvida pode ser utilizada em processos de GRSI de organizações, em treinamentos de colaboradores em GRSI, para o desenvolvimento de novas ontologias (de aplicação por exemplo) e como base para aplicações.

6.1 Trabalhos Futuros

Diante das contribuições e resultados obtidos, indentificam as seguintes oportunidades de trabalhos futuros:

Desenvolver um sistema que permita auxiliar em processos de GRSI, indicando os conceitos trabalhados e as informações necessárias nos moldes do realizado neste trabalho, tendo como base a InfoSecRM. Por meio deste, fornecer uma interface ainda mais intuituiva e com uma estrutura mais robusta para usuários menos familiarizados com estes conceitos de segurança da informação e com a utilização de ontologias.

Expandir os conceitos da InfoSecRM de forma a representar também o indicado nas outras normas da família ISO 27000.

Desenvolver ontologias de aplicação, apartir da InfoSecRM, para cenários mais específicos do domínio de segurança da informação.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTS, C.; AUDREY, D. *Managing Information Security Risks: The OCTAVE Approach*. [S.l.]: Addison Wesley, 2002.

ANDERSSON, A. H. R.; HALLBERG, J. *Evaluation of the Security of Components in Distributed Information Systems*: Scientific repost. [S.l.], 2003. 63 p.

ASSOCIAçãO BRASILEIRA DE NORMAS TéCNICAS. *ABNT NBR ISO/IEC 27002 - Código de prática para a gestão de segurança da informação*. Rio de Janeiro, ago. 2005. 120 p.

ASSOCIAçãO BRASILEIRA DE NORMAS TéCNICAS. *ABNT NBR ISO/IEC 27001 - Sistemas de gestão de segurança da informação - requisitos*. Rio de Janeiro, mar. 2006. 34 p.

ASSOCIAçãO BRASILEIRA DE NORMAS TéCNICAS. *ABNT NBR ISO/IEC 27005 - Gestão de riscos de segurança da informação*. Rio de Janeiro, mar. 2008. 63 p.

AUSTRALIAN/NEW ZEALAND STANDARD. *AS/NZS 4360:2004 - RISK MANAGEMENT*. Autralia: GPO Box 5420, Sydney / New Zealand: Private Bag 2439,Wellington 6020, 2004.

AZEVEDO, R. R. et al. Coresec: Uma ontologia de domínio para auxiliar a gestão de segurança da informação. *Anais do 8th Brazilian Simposium on Information and Computer System Security (SBSeg*, 2008.

AZEVEDO, R. R. de. *CoreSec: Uma Ontologia para o Domínio de Segurança da Informação*. 122 p. Dissertação (Mestrado) — Universidade Federal de Pernambuco, Recife, 1994.

BAADER, F. et al. (Ed.). *The Description Logic Handbook: Theory, Implementation, and Applications*. [S.l.]: Cambridge University Press, 2003.

BAADER, F.; HORROCKS, I.; SATTLER, U. Description logics as ontology languages for the semantic web. In: *Festschrift in honor of Jörg Siekmann, Lecture Notes in Artificial Intelligence*. [S.l.]: Springer-Verlag, 2003. p. 228–248.

BECKETT, D. *RDF/XML Syntax Specification (Revised)*. [S.l.], February 2004. Disponível em: <http://www.w3.org/TR/rdf-syntax-grammar/>.

BERNARAS, A.; LARESGOITI, I.; CORERA, J. Building and reusing ontologies for electrical network applications. In: WAHLSTER, W. (Ed.). *Proceedings of the 12th European Conference on Artificial Intelligence (ECAI'96)*. Chichester, UK: John Wiley and Sons, 1996. p. 298–302.

BERNERS-LEE, T.; HENDLER, J.; LASSILA, O. The semantic web. *Scientific American*, v. 284, n. 5, p. 34–43, 2001.

BRASCHER, M.; CARLAN, E. Passeios no boesque da informação: Estudos sobre representação e organização da informação e do conhecimento. In: _____. Brasília: IBICT, 2010. cap. Sistemas de organização do conhecimento: antigas e novas linguagens, p. 147–176.

BREWSTER, C. et al. Data-driven ontology evaluation. In: EUROPEAN LANGUAGE RESOURCES ASSOCIATION. *Proceedings of the Language Resources and Evaluation Conference (LREC 2004)*. Lisbon, Portugal, 2004. p. 164–168.

BRUIJN, J. de. *Using Ontologies - Enabling Knowledge Sharing and Reuse on the Semantic Web*. [S.l.], 2003. Disponível em: <http://www.debruijn.net/publications/DERI-TR-2003-10-29.pdf>.

CATRO, S. de. *Ontologia*. Rio de Janeiro: Zahar, 2008.

CHIANG, T. J.; KOUH, J. S.; CHANG, R. I. Ontology-based risk control for the incident management. *IJCSNS International Journal of Computer Science and Network Security*, v. 9, n. 11, 2009.

COMISSãO DE VALORES MOBILIáRIOS. *Cartilha de Governança: Recomendações da CVM sobre governança corporativa*. [S.l.], 2002.

CORCHO, O. et al. Building legal ontologies with METHONTOLOGY and WebODE. In: BENJAMINS, R. et al. (Ed.). *Law and the Semantic Web*. Heidelberg, DE: Springer, 2005. (LNAI), p. 142–157.

DEAN, M.; SCHREIBER, G. *OWL Web Ontology Language Reference*. [S.l.], February 2004.

DENTLER, K. et al. Comparison of reasoners for large ontologies in the owl 2 el profile. *Semantic Web*, v. 2, n. 2, p. 71–87, 2011.

DONNER, M. Toward a security ontology. *IEEE Security and Privacy magazine*, v. 1, n. 3, p. 6–7, 2003.

EHRIG, M. et al. Similarity for ontologies - a comprehensive framework. *FZI Research Center for Information Technologies at the University of Karlsruhe*, 2004.

ELLSON, J. et al. Graphviz - Open Source Graph Drawing Tools. *Graph Drawing*, Vienna, Austria, p. 483–484, 2001.

FAUSTINI, R. *Política de Segurança da informação*. maio 2010. Acessado em maio de 2010. Disponível em: <http://www.faustiniconsulting.com/artigo05.htm>.

FENSEL, D. *Ontologies: Silver Bullet for Knowledge Management and Eletronic Commerce*. [S.l.]: Springer, 2000.

FENSEL, D. *Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce*. 2. ed. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003. ISBN 3540003029.

FERNANDES, A. A.; ABREU, V. F. de. *Implantando a Governança de TI - da Estratégia à Gestão de Processos e Serviços*. Rio de Janeiro: Brasport, 2006.

FLORID, I. L. Is semantic information meaningful data? *Philosophy and Phenomenological Research*, Oxford University and Universitadi Bari, v. 70, n. 2, p. 351–370, 2005.

GABINETE DE SEGURANçA INSITUCIONAL. *Gabinete de Segurança Institucional da Presidência da República. Norma Complementar GSI n 2, de 14 de outubro de 2008*. [S.l.], 2008.

GRUBER, T. R. Toward principles for the design of ontologies used for knowledge sharing. *International Journal of Human-Computer Studies*, v. 43, n. 5/6, p. 907–928, 1995.

GRÜNINGER, M.; FOX, M. Methodology for the Design and Evaluation of Ontologies. In: *IJCAI'95, Workshop on Basic Ontological Issues in Knowledge Sharing, April 13, 1995*. [S.l.: s.n.], 1995.

GUALBERTO, E. S. *Um estudo de caso sobre a Gestão de Segurança da Informação em uma organização pública*. Brasília: [s.n.], 2010.

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

GUARINO, N.; WELTY, C. Supporting ontological analysis of taxonomic relationship. *Data and Knowledge Engineering*, v. 39, n. 1, p. 51–54, 2001.

HEIJST, G. V.; SCHREIBER, A. T.; WIELINGA, B. J. Using explicit ontologies in kbs development. *Int . J . Human, Computer Studies*, v. 46, n. 2-3, p. 183–292, 1997.

HILLSON, D. When is a risk not a risk? *Project Manager Today*, v. 1, n. 3, p. 15–16, 2007.

HORRIDGE, M. et al. A Practical Guide To Building OWL Ontologies Using The Protege-OWL Plugin and CO-ODE Tools Edition 1.0. 2004. Disponível em: <http://www.co-ode.org/resources/tutorials/ProtegeOWLTutorial.pdf>.

HORRIDGE, M. et al. A Practical Guide To Building OWL Ontologies Using The Protege-OWL Plugin and CO-ODE Tools Edition 1.0. 2004. Disponível em: <http://www.co-ode.org/resources/tutorials/ProtegeOWLTutorial.pdf>.

HORROCKS, I.; PATEL-SCHNEIDER, P. F.; HARMELEN, F. V. Reviewing the design of DAML+OIL: An ontology language for the semantic web. In: DECHTER, R.; KEARNS, M.; SUTTON, R. (Ed.). *Proceedings of the Eighteenth National Conference on Artificial Intelligence*. [S.l.: s.n.], 2002. p. 792–797.

HORROCKS, I.; PATEL-SCHNEIDER, P. F.; HARMELEN, F. V. From shiq and rdf to owl: The making of a web ontology language. *Journal of Web Semantics*, v. 1, p. 2003, 2003.

INSTITUTO BRASILEIRO DE GORVENANçA CORPORATIVA. *Código de Melhores Práticas de Governança Corporativa*. São Paulo, 2010.

INSTITUTO BRASILEIRO DE GOVERNANçA CORPORATIVA. *Guia de Orientação para Gerenciamento de Riscos Corporativos*. São Paulo, SP, 2007.

INSTITUTO BRASILEIRO DE GOVERNANçA CORPORATIVA. *Governança Corporativa*. [S.l.], junho 2010. Acessado em junho de 2010. Disponível em: <http://www.ibgc.org.br>.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 13335 - Guidelines for the management of IT Security*. [S.l.], 2004.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27000 - Information Security Management Systems*: Overview and vocabulary. [S.l.], 2009.

IT GOVERNANCE INSTITUTE. *COBIT 4.1: Control Objectives / Management Guidelines / Maturity Models*. USA, 2008.

LAMEIRA, V. J. *Governança Corporativa*. Rio de Janeiro: Forense Universitária, 2001.

LAUDON, K. C.; LAUDON, J. P. *Sistemas de informações gerenciais: administrando a empresa digital*. São Paulo: Prentice Hall, 2004.

LENAT, D. B.; GUHA, R. V. Building Large Knowledge-Based Systems: Representation and Inference in the Cyc Project. Addison Wesley Publishing Company, 1990.

LOZANO-TELLO; GOMEZ-PEREZ, A. ONTOMETRIC: A method to choose the appropriate ontology. *JOURNAL OF DATABASE MANAGEMENT*, 15, n. 2, p. 1–18, APR-JUN 2004.

MACHADO, U. *Delito e Reposta, de Dostoievski a Mitnick: um olhar jurídico sobre a conduta humana em matéria de GSI*. 2010. Disponível em: <http://www.devir.adv.br>.

MAEDCHE, A.; MAEDCHE, E.; STAAB, S. Measuring similarity between ontologies. In: *in Proceedings of the European Conference on Knowledge Acquisition and Management (EKAW*. [S.l.]: Springer, 2002. p. 251–263.

MARTIMIANO, L. A. F. *Sobre a estruturação de informação de segurança computacional: o uso de ontologia*. 163 p. Tese (Doutorado) — Instituto de Ciências Matemáticas e de Computação - ICMC, Universidade de São Paulo - USP, São Carlos, 2006.

MCGUINNESS, D. L.; HARMELEN, F. van (Ed.). *OWL Web Ontology Language Overview*. [S.l.], February 2004. Disponível em: <http://www.w3.org/TR/2004/REC-owl-features-20040210/>.

NING, H.; SHIHAN, D. Structure-based ontology evaluation. In: *e-Business Engineering, 2006. ICEBE '06. IEEE International Conference on*. [S.l.: s.n.], 2006. p. 132–137.

NOY, N. F.; MCGUINNERS, D. L. Ontology development 101: A guide to create your first ontology. *Knowledge Systems Laboratory - Stanfor University*, 2001.

OBRST, L. et al. The evaluation of ontologies. In: BAKER, C. J.; CHEUNG, K.-H. (Ed.). *Revolutionizing Knowledge Discovery in the Life Sciences*. [S.l.]: Springer, 2007. cap. 7, p. 139–158.

OFFICE OF GOVERNMENT COMMERCE. *ITIL - The Official Introduction to the ITIL Service Lifecycle*. Londres, 2007.

PELTIER, T. R. *Information Security Policies and Procedures: a practitioners reference*. [S.l.]: Auerbach Publications, 2004.

PRESSMAN, R. S. *Engenharia de software*. 6. ed. São Paulo: McGraw-Hill, 2006.

PRUD'HOMMEAUX, E.; SEABORNE, A. (Ed.). *SPARQL Query Language for RDF, W3C Recommendation*. World Wide Web Consortium, 2008. Disponível em: <http://www.w3.org/TR/rdf-sparql-query/>.

RASKIN, V. et al. Ontology in information security: a useful theoretical foundation and methology tool. *Proceedings of the workshop and New Security Paradigms*, 2001.

REZENDE, D. A. *Engenharia de Software e Sistemas de Informação*. Rio de Janeiro: Brasport, 2005.

SCHUMACHER, M. Secuurity engineering with patterns - origins, theoretical and new applications. In: _____. [S.l.]: Simpreger Verlag, 2003. cap. Toward security core ontology, p. 87–96.

SHANNON, C. E. A mathematical theory of communication. *Bell system technical journal*, v. 27, 1948.

SHITSUKA, D. *Sistemas de Informação: Um Enfoque Computacional*. Rio de Janeiro: Ciência Moderna, 2005.

SILVA, D. da; SOUZA, R.; ALMEIDA, M. Ontologias e vocabulários controlados: comparação de metodologias para construção. *Ciência da Informação*, v. 37, n. 3, 2008.

SIRIN, E.; PARSIA, B. SPARQL-DL: SPARQL Query for OWL-DL. In: *In 3rd OWL Experiences and Directions Workshop (OWLED-2007*. [S.l.: s.n.], 2007.

SIRIN, E. et al. Pellet: A practical OWL-DL reasoner. *Web Semantics: Science, Services and Agents on the World Wide Web*, Elsevier Science Publishers B. V., Amsterdam, The Netherlands, The Netherlands, v. 5, n. 2, p. 51–53, jun. 2007.

SIRIN, E. et al. Pellet: A practical OWL-DL reasoner. *Web Semantics: Science, Services and Agents on the World Wide Web*, Elsevier Science Publishers B. V., Amsterdam, The Netherlands, The Netherlands, v. 5, n. 2, p. 51–53, jun. 2007.

SMITH, B. *Ontology and Information Systems*. 2001.

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

STAAB, S.; STUDER, R. (Ed.). *Handbook on Ontologies*. [S.l.]: Springer, 2004. (International Handbooks on Information Systems). ISBN 3-540-40834-7.

STOREY, M.-A. et al. Jambalaya: an interactive environment for exploring ontologies. In: *Poster at International conference on Intelligent user interfaces*. New York, NY, USA: ACM, 2002. p. 239–239.

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

Toward distributed use of large-scale ontologies. 138–148 p.

THE ASSOCIATION OF INSURANCE AND RISK MANAGERS (AIRMIC) AND NATIONAL FORUM FOR RISK MANAGEMENT IN THE PUBLIC SECTOR - (ALARM) - INSTITUTE OF RISK MANAGEMENT. *A Risk Management Standard*. Newtown Square, Pennsylvania 19073-3299 EUA, 2002.

USCHOLD, M.; GRÜNINGER, M. Ontologies: principles, methods, and applications. *Knowledge Engineering Review*, v. 11, n. 2, p. 93–155, 1996.

USCHOLD, M.; KING, M. Towards a methodology for building ontologies. In: *Workshop on Basic Ontological Issues in Knowledge Sharing, held in conjunction with IJCAI-95*. Montreal, Canada: [s.n.], 1995.

VRANDEĈIĆ, D. Ontology evaluation. In: _____. *Handbook on Ontologies (2nd edn)*. [S.l.]: Springer, 2009. (International Handbook on Information Systems), p. 293–313.

WEILL, P.; ROSS, J. W. *Governança de TI - Tecnologia da Informação*. São Paulo: M. Books, 2005.

ANEXOS

A Classes e relacionamentos da InfoSecRM

A figura A.1 representa a hierarquia de classes da ontologia InfoSecRM, seus relacionamentos *is-a*, ao passo que a figura A.2 representa os relacionamentos não hieráquicos desta ontologia.

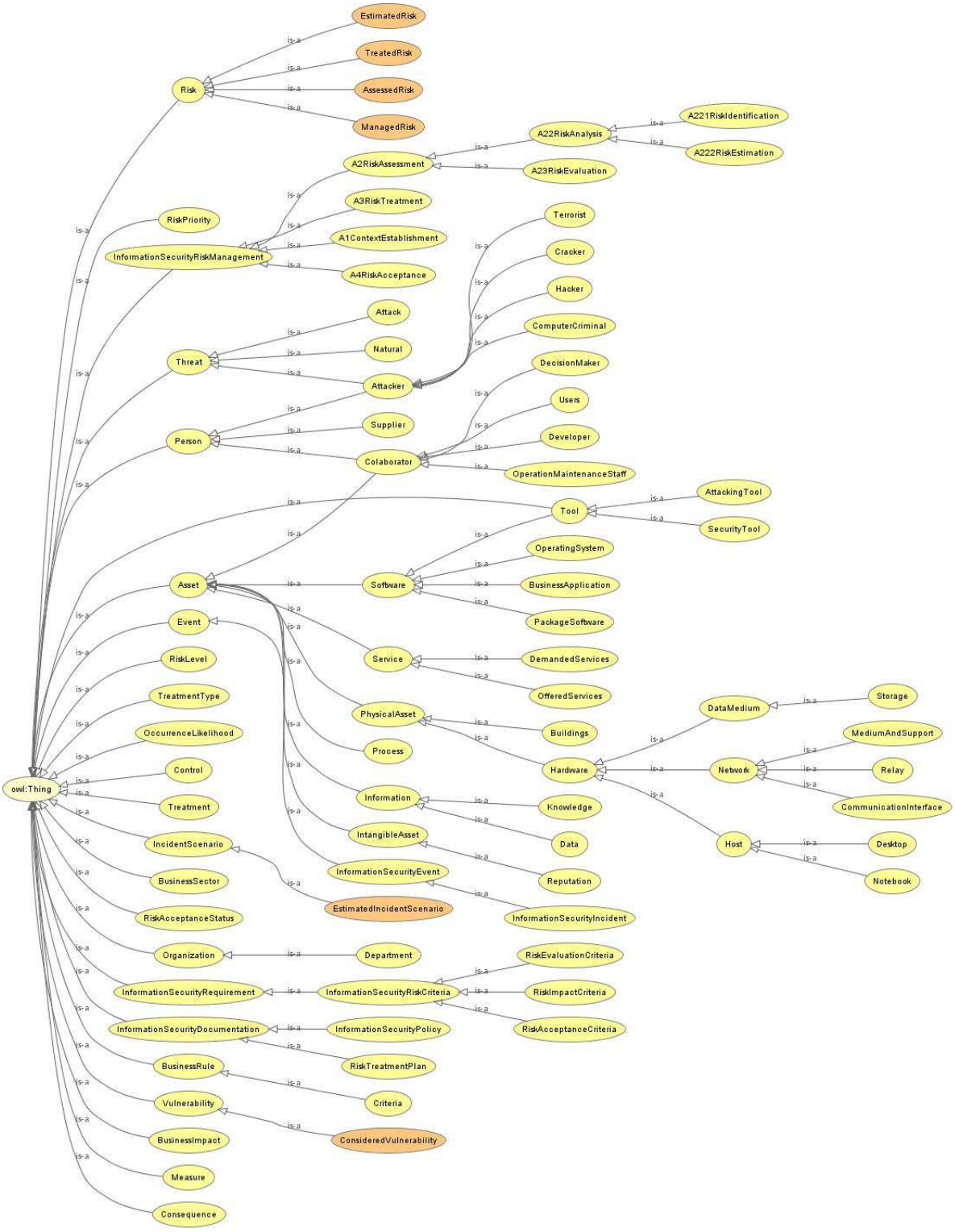

Figura A.1: Hierarquia de classes da ontologia InfoSecRM, relações *is-a*

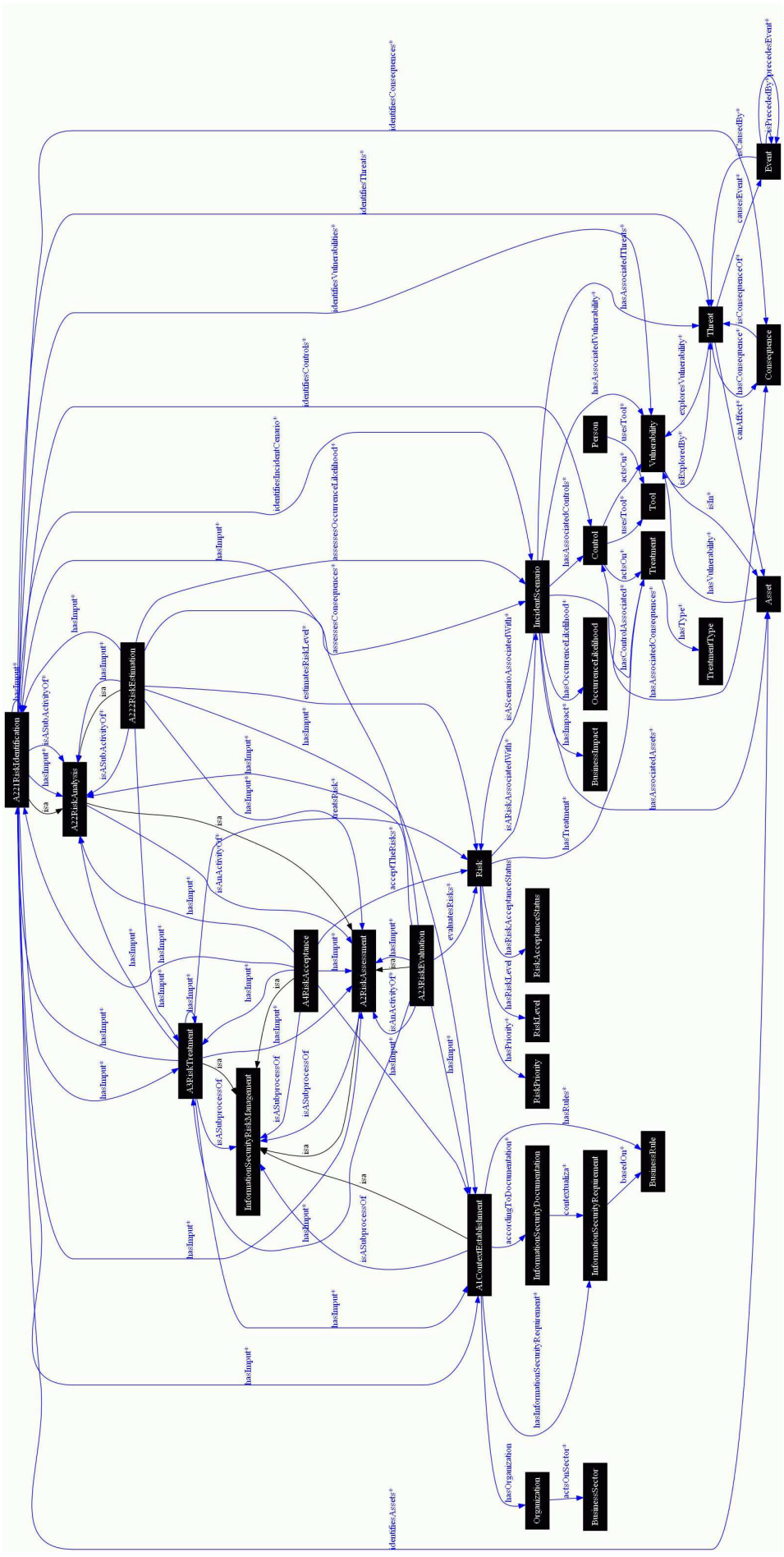

Figura A.2: Relacionamentos não hierárquicos entre as classes da InfoSecRM

B Código OWL da InfoSecRM

```
<?xml version="1.0"?>
<rdf:RDF
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:protege="http://protege.stanford.edu/plugins/owl/protege#"
    xmlns:xsp="http://www.owl-ontologies.com/2005/08/07/xsp.owl#"
    xmlns:assert="http://www.owl-ontologies.com/assert.owl#"
    xmlns:owl="http://www.w3.org/2002/07/owl#"
    xmlns:sqwrl="http://sqwrl.stanford.edu/ontologies/built-ins/3.4/sqwrl
        .owl#"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
    xmlns="http://www.owl-ontologies.com/InfoSecRM.owl#"
    xmlns:swrl="http://www.w3.org/2003/11/swrl#"
    xmlns:swrlb="http://www.w3.org/2003/11/swrlb#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
    xmlns:swrla="http://swrl.stanford.edu/ontologies/3.3/swrla.owl#"
  xml:base="http://www.owl-ontologies.com/InfoSecRM.owl">
  <owl:Ontology rdf:about=""/>
  <owl:Class rdf:ID="SecurityTool">
    <rdfs:subClassOf>
      <owl:Class rdf:ID="Tool"/>
    </rdfs:subClassOf>
  </owl:Class>
  <owl:Class rdf:ID="OperationMaintenanceStaff">
    <rdfs:subClassOf>
      <owl:Class rdf:ID="Colaborator"/>
    </rdfs:subClassOf>
  </owl:Class>
  <owl:Class rdf:ID="InformationSecurityDocumentation">
    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
    >Documentos importantes que balizam as ações e controles de segurança
        da informação, como por exemplo a política de segurança da
        informação e o plano de tratamento de riscos.</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:ID="InformationSecurityRequirement">
    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
    >Requisitos de segurança da informação apontados como importantes
        para a GRSI na organização e para os seus negócios.</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:ID="A222RiskEstimation">
    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
```

```
37      >Esta atividade objetiva desenvolver a compreensão dos riscos. A
            observação nessa etapa se baseia nas potenciais consequências de
            um determinado evento e nas suas probabilidades de acontecer.</
            rdfs:comment>
38      <rdfs:subClassOf>
39        <owl:Restriction>
40          <owl:minCardinality rdf:datatype="http://www.w3.org/2001/
                XMLSchema#int"
41          >1</owl:minCardinality>
42          <owl:onProperty>
43            <owl:ObjectProperty rdf:ID="assessesOccurrenceLikelihood"/>
44          </owl:onProperty>
45        </owl:Restriction>
46      </rdfs:subClassOf>
47      <rdfs:subClassOf>
48        <owl:Restriction>
49          <owl:onProperty>
50            <owl:ObjectProperty rdf:ID="assessesConsequences"/>
51          </owl:onProperty>
52          <owl:minCardinality rdf:datatype="http://www.w3.org/2001/
                XMLSchema#int"
53          >1</owl:minCardinality>
54        </owl:Restriction>
55      </rdfs:subClassOf>
56      <rdfs:subClassOf>
57        <owl:Class rdf:ID="A22RiskAnalysis"/>
58      </rdfs:subClassOf>
59    </owl:Class>
60    <owl:Class rdf:ID="Hardware">
61      <rdfs:subClassOf>
62        <owl:Class rdf:ID="PhysicalAsset"/>
63      </rdfs:subClassOf>
64    </owl:Class>
65    <owl:Class rdf:ID="ConsideredVulnerability">
66      <owl:equivalentClass>
67        <owl:Class>
68          <owl:intersectionOf rdf:parseType="Collection">
69            <owl:Class rdf:ID="Vulnerability"/>
70            <owl:Restriction>
71              <owl:someValuesFrom>
72                <owl:Class rdf:ID="Threat"/>
73              </owl:someValuesFrom>
74              <owl:onProperty>
75                <owl:ObjectProperty rdf:ID="isExploredBy"/>
76              </owl:onProperty>
```

```
77            </owl:Restriction>
78          </owl:intersectionOf>
79        </owl:Class>
80      </owl:equivalentClass>
81    </owl:Class>
82    <owl:Class rdf:ID="Desktop">
83      <rdfs:subClassOf>
84        <owl:Class rdf:ID="Host"/>
85      </rdfs:subClassOf>
86    </owl:Class>
87    <owl:Class rdf:ID="Department">
88      <rdfs:subClassOf>
89        <owl:Class rdf:ID="Organization"/>
90      </rdfs:subClassOf>
91    </owl:Class>
92    <owl:Class rdf:ID="TreatmentType">
93      <rdfs:subClassOf>
94        <owl:Class>
95          <owl:oneOf rdf:parseType="Collection">
96            <TreatmentType rdf:ID="Risk_Avoidance"/>
97            <TreatmentType rdf:ID="Risk_Reduction"/>
98            <TreatmentType rdf:ID="Risk_Retention"/>
99            <TreatmentType rdf:ID="Risk_Transfer"/>
100         </owl:oneOf>
101       </owl:Class>
102     </rdfs:subClassOf>
103     <rdfs:subClassOf>
104       <rdf:Description rdf:about="http://www.w3.org/2002/07/owl#Thing">
105         <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#
              string"
106         ></rdfs:comment>
107       </rdf:Description>
108     </rdfs:subClassOf>
109     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
110     >Indica o tipo de tratamento de risco. Se evita o risco, se o mitiga,
          o retem ou o terceiriza.</rdfs:comment>
111   </owl:Class>
112   <owl:Class rdf:ID="Asset">
113     <owl:disjointWith>
114       <owl:Class rdf:ID="Control"/>
115     </owl:disjointWith>
116     <rdfs:subClassOf>
117       <owl:Restriction>
118         <owl:minCardinality rdf:datatype="http://www.w3.org/2001/
              XMLSchema#int"
```

```
119         >1</owl:minCardinality>
120         <owl:onProperty>
121           <owl:ObjectProperty rdf:ID="hasVulnerability"/>
122         </owl:onProperty>
123       </owl:Restriction>
124     </rdfs:subClassOf>
125     <owl:disjointWith>
126       <owl:Class rdf:ID="Measure"/>
127     </owl:disjointWith>
128     <owl:disjointWith>
129       <owl:Class rdf:ID="Risk"/>
130     </owl:disjointWith>
131     <owl:disjointWith>
132       <owl:Class rdf:ID="Event"/>
133     </owl:disjointWith>
134     <owl:disjointWith>
135       <owl:Class rdf:ID="Attack"/>
136     </owl:disjointWith>
137     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
138     >Qualquer coisa que tenha valor para a organização.</rdfs:comment>
139     <owl:disjointWith>
140       <owl:Class rdf:about="#Vulnerability"/>
141     </owl:disjointWith>
142     <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing"/>
143     <owl:disjointWith>
144       <owl:Class rdf:about="#Threat"/>
145     </owl:disjointWith>
146   </owl:Class>
147   <owl:Class rdf:ID="AttackingTool">
148     <rdfs:subClassOf>
149       <owl:Class rdf:about="#Tool"/>
150     </rdfs:subClassOf>
151   </owl:Class>
152   <owl:Class rdf:ID="A23RiskEvaluation">
153     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
154     >O processo de avaliação de riscos consiste na comparação dos riscos
          estimados com os critérios que foram estabelecidos no processo de
          definição do contexto.</rdfs:comment>
155     <rdfs:subClassOf>
156       <owl:Class rdf:ID="A2RiskAssessment"/>
157     </rdfs:subClassOf>
158   </owl:Class>
159   <owl:Class rdf:ID="Information">
160     <owl:disjointWith>
161       <owl:Class rdf:about="#Colaborator"/>
```

```
162     </owl:disjointWith>
163     <rdfs:subClassOf rdf:resource="#Asset"/>
164   </owl:Class>
165   <owl:Class rdf:ID="ManagedRisk">
166     <owl:equivalentClass>
167       <owl:Class>
168         <owl:intersectionOf rdf:parseType="Resource">
169           <rdf:rest>
170             <rdf:List>
171               <rdf:rest>
172                 <rdf:List>
173                   <rdf:rest>
174                     <rdf:List>
175                       <rdf:first>
176                         <owl:Restriction>
177                           <owl:onProperty>
178                             <owl:ObjectProperty rdf:ID="hasTreatment"/>
179                           </owl:onProperty>
180                           <owl:someValuesFrom>
181                             <owl:Class rdf:ID="Treatment"/>
182                           </owl:someValuesFrom>
183                         </owl:Restriction>
184                       </rdf:first>
185                       <rdf:rest>
186                         <rdf:List>
187                           <rdf:rest>
188                             <rdf:List>
189                               <rdf:first>
190                                 <owl:Restriction>
191                                   <owl:onProperty>
192                                     <owl:ObjectProperty rdf:ID="
                                          isARiskAssociatedWith"/>
193                                   </owl:onProperty>
194                                   <owl:allValuesFrom>
195                                     <owl:Class rdf:ID="IncidentScenario"/
                                          >
196                                   </owl:allValuesFrom>
197                                 </owl:Restriction>
198                               </rdf:first>
199                               <rdf:rest rdf:resource="http://www.w3.org
                                    /1999/02/22-rdf-syntax-ns#nil"/>
200                             </rdf:List>
201                           </rdf:rest>
202                           <rdf:first>
203                             <owl:Restriction>
```

```
204                                    <owl:someValuesFrom>
205                                      <owl:Class rdf:ID="RiskAcceptanceStatus"/
                                             >
206                                    </owl:someValuesFrom>
207                                    <owl:onProperty>
208                                      <owl:FunctionalProperty rdf:ID="
                                             hasRiskAcceptanceStatus"/>
209                                    </owl:onProperty>
210                                  </owl:Restriction>
211                                </rdf:first>
212                              </rdf:List>
213                            </rdf:rest>
214                          </rdf:List>
215                        </rdf:rest>
216                        <rdf:first>
217                          <owl:Restriction>
218                            <owl:someValuesFrom>
219                              <owl:Class rdf:ID="RiskPriority"/>
220                            </owl:someValuesFrom>
221                            <owl:onProperty>
222                              <owl:ObjectProperty rdf:ID="hasPriority"/>
223                            </owl:onProperty>
224                          </owl:Restriction>
225                        </rdf:first>
226                      </rdf:List>
227                    </rdf:rest>
228                    <rdf:first>
229                      <owl:Restriction>
230                        <owl:onProperty>
231                          <owl:ObjectProperty rdf:ID="hasRiskLevel"/>
232                        </owl:onProperty>
233                        <owl:someValuesFrom>
234                          <owl:Class rdf:ID="RiskLevel"/>
235                        </owl:someValuesFrom>
236                      </owl:Restriction>
237                    </rdf:first>
238                  </rdf:List>
239                </rdf:rest>
240                <rdf:first>
241                  <owl:Class rdf:about="#Risk"/>
242                </rdf:first>
243              </owl:intersectionOf>
244            </owl:Class>
245          </owl:equivalentClass>
246        </owl:Class>
```

```
247   <owl:Class rdf:ID="Natural">
248     <rdfs:subClassOf>
249       <owl:Class rdf:about="#Threat"/>
250     </rdfs:subClassOf>
251   </owl:Class>
252   <owl:Class rdf:about="#RiskLevel">
253     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
254     >Define o nível de risco de um risco, com base da probabilidade de
          ocorrência e impacto de um cenário de incidente de segurança da
          informação associado.</rdfs:comment>
255     <rdfs:subClassOf>
256       <owl:Class>
257         <owl:oneOf rdf:parseType="Collection">
258           <RiskLevel rdf:ID="High_Risk">
259             <hasMeasure>
260               <Measure rdf:ID="High"/>
261             </hasMeasure>
262           </RiskLevel>
263           <RiskLevel rdf:ID="Medium_Risk">
264             <hasMeasure>
265               <Measure rdf:ID="Medium"/>
266             </hasMeasure>
267           </RiskLevel>
268           <RiskLevel rdf:ID="Low_Risk">
269             <hasMeasure>
270               <Measure rdf:ID="Low"/>
271             </hasMeasure>
272           </RiskLevel>
273         </owl:oneOf>
274       </owl:Class>
275     </rdfs:subClassOf>
276     <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing"/>
277   </owl:Class>
278   <owl:Class rdf:ID="Criteria">
279     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
280     >Critérios derivados das regras de negócio importantes que devem ser
          consideradas no processo de gestão de riscos de segurança da
          informação.</rdfs:comment>
281     <rdfs:subClassOf>
282       <owl:Class rdf:ID="BusinessRule"/>
283     </rdfs:subClassOf>
284   </owl:Class>
285   <owl:Class rdf:ID="DataMedium">
286     <rdfs:subClassOf rdf:resource="#Hardware"/>
287   </owl:Class>
```

```
288   <owl:Class rdf:ID="PackageSoftware">
289     <rdfs:subClassOf>
290       <owl:Class rdf:ID="Software"/>
291     </rdfs:subClassOf>
292   </owl:Class>
293   <owl:Class rdf:about="#Tool">
294     <owl:disjointWith>
295       <owl:Class rdf:ID="Person"/>
296     </owl:disjointWith>
297     <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing"/>
298     <owl:disjointWith>
299       <owl:Class rdf:about="#Event"/>
300     </owl:disjointWith>
301     <rdfs:subClassOf>
302       <owl:Class rdf:about="#Software"/>
303     </rdfs:subClassOf>
304     <owl:disjointWith>
305       <owl:Class rdf:about="#Risk"/>
306     </owl:disjointWith>
307     <owl:disjointWith>
308       <owl:Class rdf:about="#Control"/>
309     </owl:disjointWith>
310     <owl:disjointWith>
311       <owl:Class rdf:about="#Attack"/>
312     </owl:disjointWith>
313     <owl:disjointWith>
314       <owl:Class rdf:about="#Vulnerability"/>
315     </owl:disjointWith>
316     <owl:disjointWith>
317       <owl:Class rdf:about="#Threat"/>
318     </owl:disjointWith>
319     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
320     >Ferramentas utilizadas para defesa ou ataque em segurança da
          informação.</rdfs:comment>
321     <owl:disjointWith>
322       <owl:Class rdf:about="#Measure"/>
323     </owl:disjointWith>
324   </owl:Class>
325   <owl:Class rdf:about="#Software">
326     <owl:disjointWith>
327       <owl:Class rdf:about="#Colaborator"/>
328     </owl:disjointWith>
329     <rdfs:subClassOf rdf:resource="#Asset"/>
330   </owl:Class>
331   <owl:Class rdf:about="#Measure">
```

```
332     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
333     >Indica as possíveis medidas para probabilidade, impacto, nível de
            risco, prioridade etc.</rdfs:comment>
334     <owl:disjointWith rdf:resource="#Asset"/>
335     <owl:disjointWith>
336       <owl:Class rdf:about="#Person"/>
337     </owl:disjointWith>
338     <owl:disjointWith rdf:resource="#Tool"/>
339     <owl:disjointWith>
340       <owl:Class rdf:about="#Attack"/>
341     </owl:disjointWith>
342     <owl:disjointWith>
343       <owl:Class rdf:about="#Control"/>
344     </owl:disjointWith>
345   </owl:Class>
346   <owl:Class rdf:ID="InformationSecurityRiskCriteria">
347     <rdfs:subClassOf rdf:resource="#InformationSecurityRequirement"/>
348   </owl:Class>
349   <owl:Class rdf:ID="CommunicationInterface">
350     <rdfs:subClassOf>
351       <owl:Class rdf:ID="Network"/>
352     </rdfs:subClassOf>
353   </owl:Class>
354   <owl:Class rdf:about="#Network">
355     <rdfs:subClassOf rdf:resource="#Hardware"/>
356   </owl:Class>
357   <owl:Class rdf:ID="EstimatedRisk">
358     <owl:equivalentClass>
359       <owl:Class>
360         <owl:intersectionOf rdf:parseType="Resource">
361           <rdf:first>
362             <owl:Class rdf:about="#Risk"/>
363           </rdf:first>
364           <rdf:rest rdf:parseType="Resource">
365             <rdf:rest>
366               <rdf:List>
367                 <rdf:first>
368                   <owl:Restriction>
369                     <owl:allValuesFrom>
370                       <owl:Class rdf:about="#IncidentScenario"/>
371                     </owl:allValuesFrom>
372                     <owl:onProperty>
373                       <owl:ObjectProperty rdf:about="#
                              isARiskAssociatedWith"/>
374                     </owl:onProperty>
```

```
                    </owl:Restriction>
                  </rdf:first>
                  <rdf:rest rdf:resource="http://www.w3.org/1999/02/22-rdf-
                      syntax-ns#nil"/>
                </rdf:List>
              </rdf:rest>
              <rdf:first>
                <owl:Restriction>
                  <owl:onProperty>
                    <owl:ObjectProperty rdf:about="#hasRiskLevel"/>
                  </owl:onProperty>
                  <owl:someValuesFrom rdf:resource="#RiskLevel"/>
                </owl:Restriction>
              </rdf:first>
            </rdf:rest>
          </owl:intersectionOf>
        </owl:Class>
      </owl:equivalentClass>
    </owl:Class>
    <owl:Class rdf:about="#Colaborator">
      <rdfs:subClassOf rdf:resource="#Asset"/>
      <rdfs:subClassOf>
        <owl:Class rdf:about="#Person"/>
      </rdfs:subClassOf>
      <owl:disjointWith>
        <owl:Class rdf:ID="Service"/>
      </owl:disjointWith>
      <owl:disjointWith>
        <owl:Class rdf:ID="IntangibleAsset"/>
      </owl:disjointWith>
      <owl:disjointWith rdf:resource="#Software"/>
      <owl:disjointWith>
        <owl:Class rdf:about="#PhysicalAsset"/>
      </owl:disjointWith>
      <owl:disjointWith rdf:resource="#Information"/>
    </owl:Class>
    <owl:Class rdf:ID="RiskAcceptanceCriteria">
      <rdfs:subClassOf rdf:resource="#InformationSecurityRiskCriteria"/>
    </owl:Class>
    <owl:Class rdf:about="#Person">
      <owl:disjointWith>
        <owl:Class rdf:about="#Control"/>
      </owl:disjointWith>
      <owl:disjointWith>
        <owl:Class rdf:about="#Event"/>
```

```
419      </owl:disjointWith>
420      <owl:disjointWith>
421        <owl:Class rdf:about="#Vulnerability"/>
422      </owl:disjointWith>
423      <owl:disjointWith>
424        <owl:Class rdf:about="#Risk"/>
425      </owl:disjointWith>
426      <owl:disjointWith rdf:resource="#Measure"/>
427      <owl:disjointWith rdf:resource="#Tool"/>
428      <owl:disjointWith>
429        <owl:Class rdf:about="#Attack"/>
430      </owl:disjointWith>
431      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
432      >Pessoas envolvidas no processo de GRSI.</rdfs:comment>
433    </owl:Class>
434    <owl:Class rdf:ID="RiskTreatmentPlan">
435      <rdfs:subClassOf rdf:resource="#InformationSecurityDocumentation"/>
436    </owl:Class>
437    <owl:Class rdf:about="#Service">
438      <owl:disjointWith rdf:resource="#Colaborator"/>
439      <rdfs:subClassOf rdf:resource="#Asset"/>
440    </owl:Class>
441    <owl:Class rdf:ID="InformationSecurityPolicy">
442      <rdfs:subClassOf rdf:resource="#InformationSecurityDocumentation"/>
443      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
444      >Arranjo de princípios/procedimentos que servem de base para a gestão
             de segurança
445 da informação na mesma e que devem ser observados por todos seus
        colaboradores e
446 intervenientes.</rdfs:comment>
447    </owl:Class>
448    <owl:Class rdf:about="#Event">
449      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
450      >Acontecimentos de qualquer tipo que possam ser imporantes para a
           segurança da informação.</rdfs:comment>
451      <owl:disjointWith rdf:resource="#Person"/>
452      <owl:disjointWith rdf:resource="#Tool"/>
453      <owl:disjointWith rdf:resource="#Asset"/>
454      <owl:disjointWith>
455        <owl:Class rdf:about="#Control"/>
456      </owl:disjointWith>
457    </owl:Class>
458    <owl:Class rdf:about="#Risk">
459      <owl:disjointWith rdf:resource="#Asset"/>
460      <owl:disjointWith rdf:resource="#Person"/>
```

```
461     <owl:disjointWith rdf:resource="#Tool"/>
462     <owl:disjointWith>
463       <owl:Class rdf:about="#Attack"/>
464     </owl:disjointWith>
465     <owl:disjointWith>
466       <owl:Class rdf:about="#Control"/>
467     </owl:disjointWith>
468     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
469     >O risco de segurança da informação considera apenas a probabilidade
          de impacto negativo, assim
470 pode-se determinar risco de seguran¸ca da informação como a combinação da
       probabilidade de uma determinada ameaça explorar uma vulnerabilidade
      de um ativo (evento) com o impacto de suas potenciais consequências.</
      rdfs:comment>
471   </owl:Class>
472   <owl:Class rdf:ID="Knowledge">
473     <owl:disjointWith>
474       <owl:Class rdf:ID="Data"/>
475     </owl:disjointWith>
476     <rdfs:subClassOf rdf:resource="#Information"/>
477   </owl:Class>
478   <owl:Class rdf:ID="Terrorist">
479     <rdfs:subClassOf>
480       <owl:Class rdf:ID="Attacker"/>
481     </rdfs:subClassOf>
482   </owl:Class>
483   <owl:Class rdf:ID="InformationSecurityRiskManagement">
484     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
485     >A gestão de riscos de segurança da informação, assim como qualquer
          processo de gestão
486 de riscos, é uma gestão interativa cuja implementação tem o intuito de
      melhorar continuamente
487 o desempenho e a tomada de decisões de uma organização maximizando as
488 possibilidades de ganho, ao mesmo tempo em que minimiza as possibilidades
       de perda.</rdfs:comment>
489   </owl:Class>
490   <owl:Class rdf:ID="Relay">
491     <rdfs:subClassOf rdf:resource="#Network"/>
492   </owl:Class>
493   <owl:Class rdf:about="#A2RiskAssessment">
494     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
495     >Nessa etapa, que se divide em análise de riscos e avaliação de
          riscos, identificam-se: os
496 ativos de segurança de informação, sua valoração, as ameaças potenciais,
      os controles
```

```
497 existentes, as vulnerabilidades que podem ser exploradas, as
        consequências que podem
498 advir de uma eventual exploração de uma vulnerabilidade por uma ameaça;
        analisa-se
499 qualitativa e/ou quantitativamente as consequências, a probabilidade dos
        incidentes,
500 estima-se o nível dos riscos; e avaliam-se os riscos, com base nos
        critérios estabelecidos
501 na definição do contexto, e os ordena de acordo com as prioridades
        definidas.</rdfs:comment>
502     <rdfs:subClassOf rdf:resource="#InformationSecurityRiskManagement"/>
503   </owl:Class>
504   <owl:Class rdf:ID="InformationSecurityEvent">
505     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
506     >Ocorrência identificada de um sistema, serviço ou rede, que indica
            uma possível violação da política de segurança da informação ou
            falha de controles, ou uma situação previamente desconhecida, que
            possa ser relevante para a segurança da informação.</rdfs:comment>
507     <rdfs:subClassOf rdf:resource="#Event"/>
508   </owl:Class>
509   <owl:Class rdf:ID="ComputerCriminal">
510     <rdfs:subClassOf>
511       <owl:Class rdf:about="#Attacker"/>
512     </rdfs:subClassOf>
513   </owl:Class>
514   <owl:Class rdf:about="#RiskAcceptanceStatus">
515     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
516     >Define se o risco foi ou não aceito.</rdfs:comment>
517   </owl:Class>
518   <owl:Class rdf:ID="MediumAndSupport">
519     <rdfs:subClassOf rdf:resource="#Network"/>
520   </owl:Class>
521   <owl:Class rdf:ID="Reputation">
522     <rdfs:subClassOf>
523       <owl:Class rdf:about="#IntangibleAsset"/>
524     </rdfs:subClassOf>
525   </owl:Class>
526   <owl:Class rdf:about="#RiskPriority">
527     <rdfs:subClassOf>
528       <owl:Class>
529         <owl:oneOf rdf:parseType="Collection">
530           <RiskPriority rdf:ID="High_Priority">
531             <hasMeasure rdf:resource="#High"/>
532           </RiskPriority>
533           <RiskPriority rdf:ID="Medium_Priority">
```

```
534             <hasMeasure rdf:resource="#Medium" />
535           </RiskPriority>
536           <RiskPriority rdf:ID="Low_Priority">
537             <hasMeasure rdf:resource="#Low" />
538           </RiskPriority>
539         </owl:oneOf>
540       </owl:Class>
541     </rdfs:subClassOf>
542     <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing" />
543     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
544     >Identifica a prioridade para tratamento de um risco, de acordo com o
            nível de risco de um risco.</rdfs:comment>
545   </owl:Class>
546   <owl:Class rdf:ID="Buildings">
547     <rdfs:subClassOf>
548       <owl:Class rdf:about="#PhysicalAsset" />
549     </rdfs:subClassOf>
550   </owl:Class>
551   <owl:Class rdf:ID="DemandedServices">
552     <rdfs:subClassOf rdf:resource="#Service" />
553   </owl:Class>
554   <owl:Class rdf:about="#Data">
555     <owl:disjointWith rdf:resource="#Knowledge" />
556     <rdfs:subClassOf rdf:resource="#Information" />
557   </owl:Class>
558   <owl:Class rdf:ID="Notebook">
559     <rdfs:subClassOf>
560       <owl:Class rdf:about="#Host" />
561     </rdfs:subClassOf>
562   </owl:Class>
563   <owl:Class rdf:ID="Consequence">
564     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
565     >Consequências de um incidente de segurança da informação (
            concretização de uma ameaça explorando uma vulnerabilidade).</
            rdfs:comment>
566   </owl:Class>
567   <owl:Class rdf:about="#Control">
568     <owl:disjointWith rdf:resource="#Asset" />
569     <owl:disjointWith rdf:resource="#Person" />
570     <owl:disjointWith rdf:resource="#Tool" />
571     <owl:disjointWith>
572       <owl:Class rdf:about="#Attack" />
573     </owl:disjointWith>
574     <owl:disjointWith rdf:resource="#Event" />
575     <owl:disjointWith rdf:resource="#Risk" />
```

```
576     <owl:disjointWith rdf:resource="#Measure"/>
577     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
578     >Indicam as medidas utilizadas para sanar riscos ou vulnerabilidades.
            </rdfs:comment>
579   </owl:Class>
580   <owl:Class>
581     <owl:unionOf rdf:parseType="Collection">
582       <owl:Class rdf:about="#Asset"/>
583       <owl:Class rdf:about="#Risk"/>
584       <owl:Class rdf:about="#IncidentScenario"/>
585     </owl:unionOf>
586   </owl:Class>
587   <owl:Class rdf:about="#Organization">
588     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
589     >Organização, ambiente corporativo, escopo da GRSI.</rdfs:comment>
590     <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing"/>
591     <rdfs:subClassOf>
592       <owl:Restriction>
593         <owl:minCardinality rdf:datatype="http://www.w3.org/2001/
                XMLSchema#int"
594         >1</owl:minCardinality>
595         <owl:onProperty>
596           <owl:ObjectProperty rdf:ID="actsOnSector"/>
597         </owl:onProperty>
598       </owl:Restriction>
599     </rdfs:subClassOf>
600   </owl:Class>
601   <owl:Class rdf:ID="AssessedRisk">
602     <owl:equivalentClass>
603       <owl:Class>
604         <owl:intersectionOf rdf:parseType="Resource">
605           <rdf:first rdf:resource="#Risk"/>
606           <rdf:rest rdf:parseType="Resource">
607             <rdf:rest rdf:parseType="Resource">
608               <rdf:first>
609                 <owl:Restriction>
610                   <owl:someValuesFrom rdf:resource="#RiskLevel"/>
611                   <owl:onProperty>
612                     <owl:ObjectProperty rdf:about="#hasRiskLevel"/>
613                   </owl:onProperty>
614                 </owl:Restriction>
615               </rdf:first>
616               <rdf:rest>
617                 <rdf:List>
618                   <rdf:first>
```

```
619                     <owl:Restriction>
620                       <owl:onProperty>
621                         <owl:ObjectProperty rdf:about="#
                                isARiskAssociatedWith"/>
622                       </owl:onProperty>
623                       <owl:allValuesFrom>
624                         <owl:Class rdf:about="#IncidentScenario"/>
625                       </owl:allValuesFrom>
626                     </owl:Restriction>
627                   </rdf:first>
628                   <rdf:rest rdf:resource="http://www.w3.org/1999/02/22-
                        rdf-syntax-ns#nil"/>
629                 </rdf:List>
630               </rdf:rest>
631             </rdf:rest>
632             <rdf:first>
633               <owl:Restriction>
634                 <owl:onProperty>
635                   <owl:ObjectProperty rdf:about="#hasPriority"/>
636                 </owl:onProperty>
637                 <owl:someValuesFrom rdf:resource="#RiskPriority"/>
638               </owl:Restriction>
639             </rdf:first>
640           </rdf:rest>
641         </owl:intersectionOf>
642       </owl:Class>
643     </owl:equivalentClass>
644   </owl:Class>
645   <owl:Class rdf:ID="OperatingSystem">
646     <rdfs:subClassOf rdf:resource="#Software"/>
647   </owl:Class>
648   <owl:Class rdf:ID="A1ContextEstablishment">
649     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
650     >Quando da decisão da implementação de uma gerência de riscos, faz-se
          extremamente
651 necessário o estabelecimento de um contexto bem definido, que serão os
    parâmetros
652 básicos para que possa ser diagnosticado com excelência o escopo dos
    riscos que serão
653 considerados.</rdfs:comment>
654     <rdfs:subClassOf>
655       <owl:Restriction>
656         <owl:onProperty>
657           <owl:ObjectProperty rdf:ID="isASubprocessOf"/>
658         </owl:onProperty>
```

```
659         <owl:cardinality rdf:datatype="http://www.w3.org/2001/XMLSchema#
                int"
660         >1</owl:cardinality>
661       </owl:Restriction>
662     </rdfs:subClassOf>
663     <rdfs:subClassOf rdf:resource="#InformationSecurityRiskManagement"/>
664     <rdfs:subClassOf>
665       <owl:Restriction>
666         <owl:cardinality rdf:datatype="http://www.w3.org/2001/XMLSchema#
                int"
667         >1</owl:cardinality>
668         <owl:onProperty>
669           <owl:ObjectProperty rdf:ID="hasOrganization"/>
670         </owl:onProperty>
671       </owl:Restriction>
672     </rdfs:subClassOf>
673     <rdfs:subClassOf>
674       <owl:Restriction>
675         <owl:onProperty>
676           <owl:ObjectProperty rdf:ID="hasRules"/>
677         </owl:onProperty>
678         <owl:minCardinality rdf:datatype="http://www.w3.org/2001/
                XMLSchema#int"
679         >1</owl:minCardinality>
680       </owl:Restriction>
681     </rdfs:subClassOf>
682     <rdfs:subClassOf>
683       <owl:Restriction>
684         <owl:onProperty>
685           <owl:ObjectProperty rdf:ID="hasInformationSecurityRequirement"/
                >
686         </owl:onProperty>
687         <owl:minCardinality rdf:datatype="http://www.w3.org/2001/
                XMLSchema#int"
688         >1</owl:minCardinality>
689       </owl:Restriction>
690     </rdfs:subClassOf>
691     <rdfs:subClassOf>
692       <owl:Restriction>
693         <owl:minCardinality rdf:datatype="http://www.w3.org/2001/
                XMLSchema#int"
694         >1</owl:minCardinality>
695         <owl:onProperty>
696           <owl:ObjectProperty rdf:ID="hasResponsible"/>
697         </owl:onProperty>
```

```
698         </owl:Restriction>
699       </rdfs:subClassOf>
700     </owl:Class>
701     <owl:Class rdf:ID="Process">
702       <rdfs:subClassOf rdf:resource="#Asset"/>
703     </owl:Class>
704     <owl:Class rdf:ID="Storage">
705       <rdfs:subClassOf rdf:resource="#DataMedium"/>
706     </owl:Class>
707     <owl:Class rdf:ID="BusinessApplication">
708       <rdfs:subClassOf rdf:resource="#Software"/>
709     </owl:Class>
710     <owl:Class rdf:ID="OfferedServices">
711       <rdfs:subClassOf rdf:resource="#Service"/>
712     </owl:Class>
713     <owl:Class rdf:ID="A4RiskAcceptance">
714       <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
715       >É nessa atividade que se delimita quais riscos serão ou não aceitos
              formalmente, de acordo com os critérios para aceitação de riscos,
              descrevendo como esses serão considerados, os possíveis riscos
              residuais resultantes e as condições associadas a essas decisões.<
              /rdfs:comment>
716       <rdfs:subClassOf rdf:resource="#InformationSecurityRiskManagement"/>
717     </owl:Class>
718     <owl:Class rdf:ID="BusinessSector">
719       <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
720       >Representa o(s) negócio(s) de uma organização.</rdfs:comment>
721     </owl:Class>
722     <owl:Class rdf:ID="Cracker">
723       <rdfs:subClassOf>
724         <owl:Class rdf:about="#Attacker"/>
725       </rdfs:subClassOf>
726     </owl:Class>
727     <owl:Class rdf:ID="InformationSecurityIncident">
728       <rdfs:subClassOf rdf:resource="#InformationSecurityEvent"/>
729       <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
730       >Evento(s) de segurança da informação que tenham grande
              probabilidade de impactar o negócio e a segurança da informação de
               uma organização.</rdfs:comment>
731     </owl:Class>
732     <owl:Class rdf:ID="EstimatedIncidentScenario">
733       <owl:equivalentClass>
734         <owl:Class>
735           <owl:intersectionOf rdf:parseType="Collection">
736             <owl:Class rdf:about="#IncidentScenario"/>
```

```
737             <owl:Restriction>
738               <owl:onProperty>
739                 <owl:ObjectProperty rdf:ID="hasImpact"/>
740               </owl:onProperty>
741               <owl:someValuesFrom>
742                 <owl:Class rdf:ID="BusinessImpact"/>
743               </owl:someValuesFrom>
744             </owl:Restriction>
745             <owl:Restriction>
746               <owl:someValuesFrom>
747                 <owl:Class rdf:ID="OccurrenceLikelihood"/>
748               </owl:someValuesFrom>
749               <owl:onProperty>
750                 <owl:ObjectProperty rdf:ID="hasOccurrenceLikelihood"/>
751               </owl:onProperty>
752             </owl:Restriction>
753           </owl:intersectionOf>
754         </owl:Class>
755       </owl:equivalentClass>
756     </owl:Class>
757     <owl:Class rdf:about="#Threat">
758       <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing"/>
759       <rdfs:subClassOf>
760         <owl:Restriction>
761           <owl:someValuesFrom>
762             <owl:Class rdf:about="#Vulnerability"/>
763           </owl:someValuesFrom>
764           <owl:onProperty>
765             <owl:ObjectProperty rdf:ID="exploresVulnerability"/>
766           </owl:onProperty>
767         </owl:Restriction>
768       </rdfs:subClassOf>
769       <rdfs:subClassOf>
770         <owl:Restriction>
771           <owl:someValuesFrom rdf:resource="#Consequence"/>
772           <owl:onProperty>
773             <owl:ObjectProperty rdf:ID="hasConsequence"/>
774           </owl:onProperty>
775         </owl:Restriction>
776       </rdfs:subClassOf>
777       <owl:disjointWith rdf:resource="#Asset"/>
778       <owl:disjointWith rdf:resource="#Tool"/>
779       <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
780       >São as causas potenciais de incidentes de segurança da informação.</
              rdfs:comment>
```

```
781   </owl:Class>
782   <owl:Class rdf:ID="Users">
783     <rdfs:subClassOf rdf:resource="#Colaborator"/>
784   </owl:Class>
785   <owl:Class rdf:ID="Hacker">
786     <rdfs:subClassOf>
787       <owl:Class rdf:about="#Attacker"/>
788     </rdfs:subClassOf>
789   </owl:Class>
790   <owl:Class rdf:about="#Vulnerability">
791     <owl:disjointWith rdf:resource="#Asset"/>
792     <owl:disjointWith rdf:resource="#Person"/>
793     <owl:disjointWith rdf:resource="#Tool"/>
794     <owl:disjointWith>
795       <owl:Class rdf:about="#Attack"/>
796     </owl:disjointWith>
797     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
798     >Fragilidades inerentes ou presentes em ativos.</rdfs:comment>
799   </owl:Class>
800   <owl:Class>
801     <owl:intersectionOf rdf:parseType="Collection">
802       <owl:Restriction>
803         <owl:someValuesFrom rdf:resource="#RiskLevel"/>
804         <owl:onProperty>
805           <owl:ObjectProperty rdf:about="#hasRiskLevel"/>
806         </owl:onProperty>
807       </owl:Restriction>
808       <owl:Class rdf:about="#Risk"/>
809     </owl:intersectionOf>
810   </owl:Class>
811   <owl:Class rdf:about="#IncidentScenario">
812     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
813     >Descrições fictícias de um potencial conjunto de incidentes que uma
          organização pode estar sujeita.</rdfs:comment>
814   </owl:Class>
815   <owl:Class rdf:about="#IntangibleAsset">
816     <rdfs:subClassOf rdf:resource="#Asset"/>
817     <owl:disjointWith rdf:resource="#Colaborator"/>
818   </owl:Class>
819   <owl:Class rdf:about="#PhysicalAsset">
820     <owl:disjointWith rdf:resource="#Colaborator"/>
821     <rdfs:subClassOf rdf:resource="#Asset"/>
822   </owl:Class>
823   <owl:Class rdf:ID="Supplier">
824     <rdfs:subClassOf rdf:resource="#Person"/>
```

```
825   </owl:Class>
826   <owl:Class rdf:about="#Attacker">
827     <rdfs:subClassOf rdf:resource="#Threat"/>
828     <rdfs:subClassOf rdf:resource="#Person"/>
829   </owl:Class>
830   <owl:Class rdf:about="#BusinessImpact">
831     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
832     >Mudança adversa no nível obtido dos objetivos de negócios.</
          rdfs:comment>
833     <rdfs:subClassOf>
834       <owl:Class>
835         <owl:oneOf rdf:parseType="Collection">
836           <BusinessImpact rdf:ID="High_Impact">
837             <hasMeasure rdf:resource="#High"/>
838           </BusinessImpact>
839           <BusinessImpact rdf:ID="Medium_Impact"/>
840           <BusinessImpact rdf:ID="Low_Impact"/>
841         </owl:oneOf>
842       </owl:Class>
843     </rdfs:subClassOf>
844     <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing"/>
845   </owl:Class>
846   <owl:Class rdf:about="#Host">
847     <rdfs:subClassOf rdf:resource="#Hardware"/>
848   </owl:Class>
849   <owl:Class rdf:about="#A22RiskAnalysis">
850     <rdfs:subClassOf rdf:resource="#A2RiskAssessment"/>
851     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
852     >A análise de riscos se subdivide em identificação de riscos e
          estimativa de riscos.</rdfs:comment>
853   </owl:Class>
854   <owl:Class rdf:about="#Attack">
855     <owl:disjointWith rdf:resource="#Control"/>
856     <owl:disjointWith rdf:resource="#Risk"/>
857     <owl:disjointWith rdf:resource="#Person"/>
858     <owl:disjointWith rdf:resource="#Tool"/>
859     <owl:disjointWith rdf:resource="#Vulnerability"/>
860     <owl:disjointWith rdf:resource="#Measure"/>
861     <owl:disjointWith rdf:resource="#Asset"/>
862     <rdfs:subClassOf rdf:resource="#Threat"/>
863   </owl:Class>
864   <owl:Class rdf:ID="DecisionMaker">
865     <rdfs:subClassOf rdf:resource="#Colaborator"/>
866   </owl:Class>
867   <owl:Class rdf:about="#BusinessRule">
```

```
868     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
869     >Regras de negócio importantes que devem ser consideradas no processo
            de gestão de riscos de segurança da informação.</rdfs:comment>
870   </owl:Class>
871   <owl:Class rdf:ID="TreatedRisk">
872     <owl:equivalentClass>
873       <owl:Class>
874         <owl:intersectionOf rdf:parseType="Resource">
875           <rdf:first rdf:resource="#Risk"/>
876           <rdf:rest rdf:parseType="Resource">
877             <rdf:first>
878               <owl:Restriction>
879                 <owl:onProperty>
880                   <owl:ObjectProperty rdf:about="#hasPriority"/>
881                 </owl:onProperty>
882                 <owl:someValuesFrom rdf:resource="#RiskPriority"/>
883               </owl:Restriction>
884             </rdf:first>
885             <rdf:rest rdf:parseType="Resource">
886               <rdf:first>
887                 <owl:Restriction>
888                   <owl:onProperty>
889                     <owl:ObjectProperty rdf:about="#hasRiskLevel"/>
890                   </owl:onProperty>
891                   <owl:someValuesFrom rdf:resource="#RiskLevel"/>
892                 </owl:Restriction>
893               </rdf:first>
894               <rdf:rest rdf:parseType="Resource">
895                 <rdf:rest>
896                   <rdf:List>
897                     <rdf:first>
898                       <owl:Restriction>
899                         <owl:allValuesFrom rdf:resource="#
                                IncidentScenario"/>
900                         <owl:onProperty>
901                           <owl:ObjectProperty rdf:about="#
                                  isARiskAssociatedWith"/>
902                         </owl:onProperty>
903                       </owl:Restriction>
904                     </rdf:first>
905                     <rdf:rest rdf:resource="http://www.w3.org/1999/02/22-
                          rdf-syntax-ns#nil"/>
906                   </rdf:List>
907                 </rdf:rest>
908                 <rdf:first>
```

```
909                     <owl:Restriction>
910                       <owl:someValuesFrom>
911                         <owl:Class rdf:about="#Treatment"/>
912                       </owl:someValuesFrom>
913                       <owl:onProperty>
914                         <owl:ObjectProperty rdf:about="#hasTreatment"/>
915                       </owl:onProperty>
916                     </owl:Restriction>
917                   </rdf:first>
918                 </rdf:rest>
919               </rdf:rest>
920             </rdf:rest>
921           </owl:intersectionOf>
922         </owl:Class>
923       </owl:equivalentClass>
924     </owl:Class>
925     <owl:Class rdf:ID="RiskEvaluationCriteria">
926       <rdfs:subClassOf rdf:resource="#InformationSecurityRiskCriteria"/>
927     </owl:Class>
928     <owl:Class rdf:ID="A3RiskTreatment">
929       <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
930       >Nesta atividade, de acordo com o priorizado na atividade de
              avaliação de riscos, tratam-se os riscos por mitigação de risco,
              evitar o risco, terceirizar o risco ou reter o risco.</
              rdfs:comment>
931       <rdfs:subClassOf rdf:resource="#InformationSecurityRiskManagement"/>
932     </owl:Class>
933     <owl:Class rdf:ID="RiskImpactCriteria">
934       <rdfs:subClassOf rdf:resource="#InformationSecurityRiskCriteria"/>
935     </owl:Class>
936     <owl:Class rdf:about="#Treatment">
937       <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
938       >Ação baseada em controles para sanar um risco.</rdfs:comment>
939     </owl:Class>
940     <owl:Class rdf:about="#OccurrenceLikelihood">
941       <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
942       >Probabilidade de ocorrência de um cenário de incidentes de segurança
              da informação.</rdfs:comment>
943       <rdfs:subClassOf>
944         <owl:Class>
945           <owl:oneOf rdf:parseType="Collection">
946             <OccurrenceLikelihood rdf:ID="High_Likelihood">
947               <hasMeasure rdf:resource="#High"/>
948             </OccurrenceLikelihood>
949             <OccurrenceLikelihood rdf:ID="Medium_Likelihood">
```

```
950             <hasMeasure rdf:resource="#Medium" />
951           </OccurrenceLikelihood>
952           <OccurrenceLikelihood rdf:ID="Low_Likelihood">
953             <hasMeasure rdf:resource="#Low" />
954           </OccurrenceLikelihood>
955         </owl:oneOf>
956       </owl:Class>
957     </rdfs:subClassOf>
958     <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing" />
959   </owl:Class>
960   <owl:Class rdf:ID="A221RiskIdentification">
961     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
962     >Identificar os riscos é delinear e caracterizar os potenciais
          incidentes que podem interferir nos propósitos de uma atividade,
          sistema, processo, organização, etc, a fim de gerenciá-los.</
          rdfs:comment>
963     <rdfs:subClassOf rdf:resource="#A22RiskAnalysis" />
964   </owl:Class>
965   <owl:Class rdf:ID="Developer">
966     <rdfs:subClassOf rdf:resource="#Colaborator" />
967   </owl:Class>
968   <owl:ObjectProperty rdf:ID="identifiesIncidentCenario">
969     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
970     >Indica os cenários de incidentes identificados na fase de
          identificação de riscos.</rdfs:comment>
971     <rdfs:range rdf:resource="#IncidentScenario" />
972     <rdfs:domain rdf:resource="#A221RiskIdentification" />
973   </owl:ObjectProperty>
974   <owl:ObjectProperty rdf:ID="evaluatesRisks">
975     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
976     >Indica os riscos considerados nas atividades de avaliação de riscos.
          </rdfs:comment>
977     <rdfs:domain rdf:resource="#A23RiskEvaluation" />
978     <rdfs:range rdf:resource="#Risk" />
979   </owl:ObjectProperty>
980   <owl:ObjectProperty rdf:about="#hasTreatment">
981     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
982     >Indica o tratamento determinado para um risco.</rdfs:comment>
983     <rdfs:domain rdf:resource="#Risk" />
984     <rdfs:range rdf:resource="#Treatment" />
985   </owl:ObjectProperty>
986   <owl:ObjectProperty rdf:about="#hasInformationSecurityRequirement">
987     <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
988     >&lt;p style="margin-top: 0"&gt;
```

```
989         Indicam os requisitos utilizados no estabelecimento de contexto
                para a
990         GRSI.
991       &lt;/p&gt;</rdfs:comment>
992       <rdfs:domain rdf:resource="#A1ContextEstablishment"/>
993       <rdfs:range rdf:resource="#InformationSecurityRequirement"/>
994     </owl:ObjectProperty>
995     <owl:ObjectProperty rdf:ID="precedesInformationSecurityEvent">
996       <rdfs:domain>
997         <owl:Class>
998           <owl:unionOf rdf:parseType="Collection">
999             <owl:Class rdf:about="#Event"/>
1000            <owl:Class rdf:about="#InformationSecurityEvent"/>
1001          </owl:unionOf>
1002        </owl:Class>
1003      </rdfs:domain>
1004      <rdfs:range rdf:resource="#InformationSecurityEvent"/>
1005      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
            TransitiveProperty"/>
1006      <rdfs:subPropertyOf>
1007        <owl:ObjectProperty rdf:ID="precedesEvent"/>
1008      </rdfs:subPropertyOf>
1009    </owl:ObjectProperty>
1010    <owl:ObjectProperty rdf:ID="isPrecededBy">
1011      <owl:inverseOf>
1012        <owl:ObjectProperty rdf:about="#precedesEvent"/>
1013      </owl:inverseOf>
1014      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
            TransitiveProperty"/>
1015      <rdfs:range rdf:resource="#Event"/>
1016      <rdfs:domain rdf:resource="#Event"/>
1017      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1018      >Indica que eventos precedem um evento.</rdfs:comment>
1019    </owl:ObjectProperty>
1020    <owl:ObjectProperty rdf:ID="identifiesControls">
1021      <rdfs:range rdf:resource="#Control"/>
1022      <rdfs:domain rdf:resource="#A221RiskIdentification"/>
1023      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1024      >Indica os controles identificados na fase de identificação de riscos
            .</rdfs:comment>
1025    </owl:ObjectProperty>
1026    <owl:ObjectProperty rdf:ID="hasMeasure">
1027      <rdfs:domain>
1028        <owl:Class>
1029          <owl:unionOf rdf:parseType="Collection">
```

```
1030            <owl:Class rdf:about="#BusinessImpact"/>
1031            <owl:Class rdf:about="#RiskPriority"/>
1032            <owl:Class rdf:about="#RiskLevel"/>
1033            <owl:Class rdf:about="#OccurrenceLikelihood"/>
1034          </owl:unionOf>
1035        </owl:Class>
1036      </rdfs:domain>
1037      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1038      >Indicam as possíveis medidas associadas à impacto, prioridade, nível
            de risco e probabilidade de ocorrência.</rdfs:comment>
1039      <rdfs:range rdf:resource="#Measure"/>
1040    </owl:ObjectProperty>
1041    <owl:ObjectProperty rdf:ID="canAffect">
1042      <rdfs:range rdf:resource="#Asset"/>
1043      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1044      >Indicam quais ativos uma ameaça pode afetar.</rdfs:comment>
1045      <rdfs:domain rdf:resource="#Threat"/>
1046    </owl:ObjectProperty>
1047    <owl:ObjectProperty rdf:ID="estimatesRiskLevel">
1048      <rdfs:domain rdf:resource="#A222RiskEstimation"/>
1049      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1050      >Indica o nível de risco que é estimado levando-se em conta a
            probabilidade de ocorrência e o impacto do cenário de incidentes
            de segurança da informação associado.</rdfs:comment>
1051      <rdfs:range rdf:resource="#Risk"/>
1052    </owl:ObjectProperty>
1053    <owl:ObjectProperty rdf:about="#isExploredBy">
1054      <owl:inverseOf>
1055        <owl:ObjectProperty rdf:about="#exploresVulnerability"/>
1056      </owl:inverseOf>
1057      <rdfs:domain rdf:resource="#Vulnerability"/>
1058      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1059      >Indica quais ameaças exploram uma determinada vulnerabilidade.</
            rdfs:comment>
1060      <rdfs:range>
1061        <owl:Class>
1062          <owl:unionOf rdf:parseType="Collection">
1063            <owl:Class rdf:about="#AttackingTool"/>
1064            <owl:Class rdf:about="#Natural"/>
1065            <owl:Class rdf:about="#Attacker"/>
1066            <owl:Class rdf:about="#Attack"/>
1067            <owl:Class rdf:about="#Threat"/>
1068          </owl:unionOf>
1069        </owl:Class>
1070      </rdfs:range>
```

```
1071  </owl:ObjectProperty>
1072  <owl:ObjectProperty rdf:about="#hasOrganization">
1073    <rdfs:range rdf:resource="#Organization"/>
1074    <rdfs:domain rdf:resource="#A1ContextEstablishment"/>
1075    <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
          FunctionalProperty"/>
1076    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1077    >&lt;p style="margin-top:␣0"&gt;
1078      Indica a organiza&amp;#231;&amp;#227;o onde se dar&amp;#225; a GRSI
            , esta &amp;#233; apontada na atividade
1079      de estabelecimento do contexto.
1080    &lt;/p&gt;</rdfs:comment>
1081  </owl:ObjectProperty>
1082  <owl:ObjectProperty rdf:ID="isPerformedBy">
1083    <rdfs:domain rdf:resource="#Attack"/>
1084    <rdfs:range rdf:resource="#Attacker"/>
1085    <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
          FunctionalProperty"/>
1086    <owl:inverseOf>
1087      <owl:ObjectProperty rdf:ID="performsAttack"/>
1088    </owl:inverseOf>
1089    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1090    >Indica o atacante responsável por um ataque.</rdfs:comment>
1091  </owl:ObjectProperty>
1092  <owl:ObjectProperty rdf:ID="hasScope">
1093    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1094    >Indica o escopo da GRSI em uma organização.</rdfs:comment>
1095    <rdfs:domain rdf:resource="#A1ContextEstablishment"/>
1096    <rdfs:range>
1097      <owl:Class>
1098        <owl:unionOf rdf:parseType="Collection">
1099          <owl:Class rdf:about="#Software"/>
1100          <owl:Class rdf:about="#Hardware"/>
1101          <owl:Class rdf:about="#Department"/>
1102        </owl:unionOf>
1103      </owl:Class>
1104    </rdfs:range>
1105  </owl:ObjectProperty>
1106  <owl:ObjectProperty rdf:about="#hasPriority">
1107    <rdfs:domain rdf:resource="#Risk"/>
1108    <rdfs:range rdf:resource="#RiskPriority"/>
1109    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1110    >Indica a prioridade dada a um risco para receber tratamento,
          atribuída na atividade de avaliação de risco.</rdfs:comment>
1111  </owl:ObjectProperty>
```

```
1112  <owl:ObjectProperty rdf:ID="isUsedBy">
1113    <rdfs:range rdf:resource="#Attacker"/>
1114    <rdfs:domain rdf:resource="#AttackingTool"/>
1115    <owl:inverseOf>
1116      <owl:ObjectProperty rdf:ID="usesTool"/>
1117    </owl:inverseOf>
1118    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1119    >Indica as ferramentas utilizadas em um ataque.</rdfs:comment>
1120  </owl:ObjectProperty>
1121  <owl:ObjectProperty rdf:about="#exploresVulnerability">
1122    <owl:inverseOf rdf:resource="#isExploredBy"/>
1123    <rdfs:range rdf:resource="#Vulnerability"/>
1124    <rdfs:domain>
1125      <owl:Class>
1126        <owl:unionOf rdf:parseType="Collection">
1127          <owl:Class rdf:about="#AttackingTool"/>
1128          <owl:Class rdf:about="#Natural"/>
1129          <owl:Class rdf:about="#Attacker"/>
1130          <owl:Class rdf:about="#Attack"/>
1131          <owl:Class rdf:about="#Threat"/>
1132        </owl:unionOf>
1133      </owl:Class>
1134    </rdfs:domain>
1135    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1136    >Indicam quais vulnerabilidades podem ser exploradas por determinadas
         ameaças.</rdfs:comment>
1137  </owl:ObjectProperty>
1138  <owl:ObjectProperty rdf:ID="causesEvent">
1139    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1140    >Indica que eventos uma ameaça pode causar.</rdfs:comment>
1141    <owl:inverseOf>
1142      <owl:ObjectProperty rdf:ID="isCausedBy"/>
1143    </owl:inverseOf>
1144    <rdfs:range rdf:resource="#Event"/>
1145    <rdfs:domain rdf:resource="#Threat"/>
1146  </owl:ObjectProperty>
1147  <owl:ObjectProperty rdf:ID="isAnActivityOf">
1148    <rdfs:range rdf:resource="#A2RiskAssessment"/>
1149    <rdfs:domain>
1150      <owl:Class>
1151        <owl:unionOf rdf:parseType="Collection">
1152          <owl:Class rdf:about="#A22RiskAnalysis"/>
1153          <owl:Class rdf:about="#A23RiskEvaluation"/>
1154        </owl:unionOf>
1155      </owl:Class>
```

```
1156      </rdfs:domain>
1157      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1158      >&lt;p style="margin-top: 0"&gt;
1159        Indica que uma atividade &amp;#233; uma subatividade de outra
              atividade de GRSI.
1160      &lt;/p&gt;</rdfs:comment>
1161    </owl:ObjectProperty>
1162    <owl:ObjectProperty rdf:ID="basedOn">
1163      <rdfs:domain rdf:resource="#InformationSecurityRequirement"/>
1164      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1165      >indicam as regras de negócio em que se baseiam os requisitos de
            segurança da informação adotados.</rdfs:comment>
1166      <rdfs:range rdf:resource="#BusinessRule"/>
1167    </owl:ObjectProperty>
1168    <owl:ObjectProperty rdf:about="#hasResponsible">
1169      <rdfs:domain>
1170        <owl:Class>
1171          <owl:unionOf rdf:parseType="Collection">
1172            <owl:Class rdf:about="#Asset"/>
1173            <owl:Class rdf:about="#Risk"/>
1174            <owl:Class rdf:about="#IncidentScenario"/>
1175          </owl:unionOf>
1176        </owl:Class>
1177      </rdfs:domain>
1178      <rdfs:range>
1179        <owl:Class>
1180          <owl:unionOf rdf:parseType="Collection">
1181            <owl:Class rdf:about="#Colaborator"/>
1182            <owl:Class rdf:about="#Supplier"/>
1183          </owl:unionOf>
1184        </owl:Class>
1185      </rdfs:range>
1186      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1187      >Identifica o responsável por um risco, ativo ou cenário de incidente
            .</rdfs:comment>
1188    </owl:ObjectProperty>
1189    <owl:ObjectProperty rdf:about="#hasOccurrenceLikelihood">
1190      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1191      >Indica a probabilidade de ocorrência de um cenário de incidentes.</
            rdfs:comment>
1192      <rdfs:domain rdf:resource="#IncidentScenario"/>
1193      <rdfs:range rdf:resource="#OccurrenceLikelihood"/>
1194    </owl:ObjectProperty>
1195    <owl:ObjectProperty rdf:ID="hasAssociatedAssets">
1196      <rdfs:range rdf:resource="#Asset"/>
```

```
1197      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1198      >Indica os ativos que estão relacionados a um cenário de incidentes
              de segurança da informação.</rdfs:comment>
1199      <rdfs:domain rdf:resource="#IncidentScenario"/>
1200    </owl:ObjectProperty>
1201    <owl:ObjectProperty rdf:about="#precedesEvent">
1202      <owl:inverseOf rdf:resource="#isPrecededBy"/>
1203      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1204      >Indica que evento é precedido por um evento.</rdfs:comment>
1205      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
              TransitiveProperty"/>
1206      <rdfs:range rdf:resource="#Event"/>
1207      <rdfs:domain rdf:resource="#Event"/>
1208    </owl:ObjectProperty>
1209    <owl:ObjectProperty rdf:ID="definesTheRiskTreatmentPlan">
1210      <rdfs:domain rdf:resource="#A3RiskTreatment"/>
1211      <rdfs:range rdf:resource="#RiskTreatmentPlan"/>
1212      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1213      >Indica qual o plano de tratamento de riscos adotado nas atividades
              de tratamento de risco.</rdfs:comment>
1214    </owl:ObjectProperty>
1215    <owl:ObjectProperty rdf:about="#hasVulnerability">
1216      <rdfs:domain rdf:resource="#Asset"/>
1217      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1218      >Indica as vulnerabilidades associadas a um ativo.</rdfs:comment>
1219      <rdfs:range rdf:resource="#Vulnerability"/>
1220      <owl:inverseOf>
1221        <owl:ObjectProperty rdf:ID="isIn"/>
1222      </owl:inverseOf>
1223    </owl:ObjectProperty>
1224    <owl:ObjectProperty rdf:about="#actsOnSector">
1225      <rdfs:range rdf:resource="#BusinessSector"/>
1226      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1227      >Indica o Setor/negócio em que a organização atua.</rdfs:comment>
1228      <rdfs:domain rdf:resource="#Organization"/>
1229    </owl:ObjectProperty>
1230    <owl:ObjectProperty rdf:ID="isAScenarioAssociatedWith">
1231      <rdfs:domain rdf:resource="#IncidentScenario"/>
1232      <rdfs:range rdf:resource="#Risk"/>
1233      <owl:inverseOf>
1234        <owl:ObjectProperty rdf:about="#isARiskAssociatedWith"/>
1235      </owl:inverseOf>
1236      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1237      >Indica a qual risco um cenário está associado.</rdfs:comment>
1238    </owl:ObjectProperty>
```

```
1239  <owl:ObjectProperty rdf:about="#isIn">
1240    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1241    >Indica em quais ativos uma vulnerabilidade está presente.</
          rdfs:comment>
1242    <rdfs:domain rdf:resource="#Vulnerability"/>
1243    <owl:inverseOf rdf:resource="#hasVulnerability"/>
1244    <rdfs:range rdf:resource="#Asset"/>
1245  </owl:ObjectProperty>
1246  <owl:ObjectProperty rdf:ID="hasImput">
1247    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1248    >&lt;p style="margin-top: 0"&gt;
1249      Indica a rela&amp;#231;&amp;#227;o que existe entre as atividades
            de um processo de GRSI
1250      de entrada e sa&amp;#237;da de informa&amp;#231;&amp;#245;es.
1251    &lt;/p&gt;</rdfs:comment>
1252    <rdfs:range>
1253      <owl:Class>
1254        <owl:unionOf rdf:parseType="Collection">
1255          <owl:Class rdf:about="#A1ContextEstablishment"/>
1256          <owl:Class rdf:about="#A221RiskIdentification"/>
1257          <owl:Class rdf:about="#A22RiskAnalysis"/>
1258          <owl:Class rdf:about="#A2RiskAssessment"/>
1259          <owl:Class rdf:about="#A3RiskTreatment"/>
1260        </owl:unionOf>
1261      </owl:Class>
1262    </rdfs:range>
1263    <rdfs:domain>
1264      <owl:Class>
1265        <owl:unionOf rdf:parseType="Collection">
1266          <owl:Class rdf:about="#A221RiskIdentification"/>
1267          <owl:Class rdf:about="#A222RiskEstimation"/>
1268          <owl:Class rdf:about="#A23RiskEvaluation"/>
1269          <owl:Class rdf:about="#A3RiskTreatment"/>
1270          <owl:Class rdf:about="#A4RiskAcceptance"/>
1271        </owl:unionOf>
1272      </owl:Class>
1273    </rdfs:domain>
1274  </owl:ObjectProperty>
1275  <owl:ObjectProperty rdf:about="#assessesOccurrenceLikelihood">
1276    <rdfs:domain rdf:resource="#A222RiskEstimation"/>
1277    <rdfs:range rdf:resource="#IncidentScenario"/>
1278    <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1279    >Indica a avaliação de consequências dos cenários de incidentes de
          segurança da informação lhe associando uma medida de probabilidade
           de ocorrência.</rdfs:comment>
```

```
1280    </owl:ObjectProperty>
1281    <owl:ObjectProperty rdf:ID="hasAssociatedControls">
1282      <rdfs:domain rdf:resource="#IncidentScenario"/>
1283      <rdfs:range rdf:resource="#Control"/>
1284      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1285      >Indica os controles que estão relacionados a um cenário de
            incidentes de segurança da informação.</rdfs:comment>
1286    </owl:ObjectProperty>
1287    <owl:ObjectProperty rdf:ID="treatsRisk">
1288      <rdfs:range rdf:resource="#Risk"/>
1289      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1290      >Indica quais riscos são tratados na atividade de tratamento de risco
            .</rdfs:comment>
1291      <rdfs:domain rdf:resource="#A3RiskTreatment"/>
1292    </owl:ObjectProperty>
1293    <owl:ObjectProperty rdf:about="#hasRules">
1294      <rdfs:range rdf:resource="#BusinessRule"/>
1295      <rdfs:domain rdf:resource="#A1ContextEstablishment"/>
1296      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1297      >Indica as regras de negócio consideradas no estabelecimento de
            contexto da GRSI.</rdfs:comment>
1298    </owl:ObjectProperty>
1299    <owl:ObjectProperty rdf:ID="hasMonitoringAndAnalysisBy">
1300      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1301      >Indica quem é o responsável por monitorar e analisar continuamente
            uma atividade, requisito ou processo.</rdfs:comment>
1302      <rdfs:range rdf:resource="#Colaborator"/>
1303      <rdfs:domain>
1304        <owl:Class>
1305          <owl:unionOf rdf:parseType="Collection">
1306            <owl:Class rdf:about="#InformationSecurityRequirement"/>
1307            <owl:Class rdf:about="#InformationSecurityRiskManagement"/>
1308          </owl:unionOf>
1309        </owl:Class>
1310      </rdfs:domain>
1311    </owl:ObjectProperty>
1312    <owl:ObjectProperty rdf:ID="identifiesThreats">
1313      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1314      >Indica as ameaças de incidentes identificados na fase de
            identificação de riscos.</rdfs:comment>
1315      <rdfs:range rdf:resource="#Threat"/>
1316      <rdfs:domain rdf:resource="#A221RiskIdentification"/>
1317    </owl:ObjectProperty>
1318    <owl:ObjectProperty rdf:ID="hasScenario">
1319      <owl:inverseOf>
```

```
1320        <owl:ObjectProperty rdf:ID="isScenarioOf"/>
1321      </owl:inverseOf>
1322      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1323      >Indica o cenário de um incidente em específico.</rdfs:comment>
1324      <rdfs:range rdf:resource="#IncidentScenario"/>
1325      <rdfs:domain rdf:resource="#InformationSecurityIncident"/>
1326    </owl:ObjectProperty>
1327    <owl:ObjectProperty rdf:about="#isCausedBy">
1328      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1329      >Indica quais ameaças causaram um incidente.</rdfs:comment>
1330      <owl:inverseOf rdf:resource="#causesEvent"/>
1331      <rdfs:range rdf:resource="#Threat"/>
1332      <rdfs:domain rdf:resource="#Event"/>
1333    </owl:ObjectProperty>
1334    <owl:ObjectProperty rdf:ID="hasCriteria">
1335      <rdfs:range rdf:resource="#InformationSecurityRiskCriteria"/>
1336      <rdfs:domain rdf:resource="#A1ContextEstablishment"/>
1337      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1338      >Indica os critérios de riscos de segurança da informação utilizados
            para estabelecer o contexto da GRSI.</rdfs:comment>
1339    </owl:ObjectProperty>
1340    <owl:ObjectProperty rdf:ID="precedesInformationSecurityIncident">
1341      <rdfs:domain>
1342        <owl:Class>
1343          <owl:unionOf rdf:parseType="Collection">
1344            <owl:Class rdf:about="#InformationSecurityEvent"/>
1345            <owl:Class rdf:about="#InformationSecurityIncident"/>
1346          </owl:unionOf>
1347        </owl:Class>
1348      </rdfs:domain>
1349      <rdfs:subPropertyOf rdf:resource="#precedesInformationSecurityEvent"/
            >
1350      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
            TransitiveProperty"/>
1351      <rdfs:range rdf:resource="#InformationSecurityIncident"/>
1352    </owl:ObjectProperty>
1353    <owl:ObjectProperty rdf:about="#hasConsequence">
1354      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1355      >Indica as consequências de uma determinada ameaça.</rdfs:comment>
1356      <rdfs:domain rdf:resource="#Threat"/>
1357      <rdfs:range rdf:resource="#Consequence"/>
1358    </owl:ObjectProperty>
1359    <owl:ObjectProperty rdf:ID="actsOn">
1360      <rdfs:range>
1361        <owl:Class>
```

```
1362          <owl:unionOf rdf:parseType="Collection">
1363            <owl:Class rdf:about="#Vulnerability"/>
1364            <owl:Class rdf:about="#Treatment"/>
1365          </owl:unionOf>
1366        </owl:Class>
1367      </rdfs:range>
1368      <rdfs:domain rdf:resource="#Control"/>
1369      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1370      >Indica sob qual vulnerabilidade ou em qual tratamento um controle
             agirá.</rdfs:comment>
1371    </owl:ObjectProperty>
1372    <owl:ObjectProperty rdf:ID="identifiesAssets">
1373      <rdfs:range rdf:resource="#Asset"/>
1374      <rdfs:domain rdf:resource="#A221RiskIdentification"/>
1375      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1376      >Indica os ativos identificados na fase de identificação de riscos.</
             rdfs:comment>
1377    </owl:ObjectProperty>
1378    <owl:ObjectProperty rdf:ID="accordingToDocumentation">
1379      <rdfs:domain rdf:resource="#A1ContextEstablishment"/>
1380      <rdfs:range rdf:resource="#InformationSecurityDocumentation"/>
1381      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1382      >Indica sobre qual documentação estabelecer-se-á o contexto para a
             GRSI.</rdfs:comment>
1383    </owl:ObjectProperty>
1384    <owl:ObjectProperty rdf:ID="contextualiza">
1385      <rdfs:domain rdf:resource="#InformationSecurityDocumentation"/>
1386      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1387      >As documentações de segurança da informação, principalmente uma
             política de segurança da informação, contextualizam os requisitos
             de segurança da informação adotados.</rdfs:comment>
1388      <rdfs:range rdf:resource="#InformationSecurityRequirement"/>
1389    </owl:ObjectProperty>
1390    <owl:ObjectProperty rdf:ID="providedIn">
1391      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1392      >Indica em que plano de tratamentos um tratamento está inserido.</
             rdfs:comment>
1393      <rdfs:range rdf:resource="#RiskTreatmentPlan"/>
1394      <rdfs:domain rdf:resource="#Treatment"/>
1395    </owl:ObjectProperty>
1396    <owl:ObjectProperty rdf:about="#isScenarioOf">
1397      <owl:inverseOf rdf:resource="#hasScenario"/>
1398      <rdfs:domain rdf:resource="#IncidentScenario"/>
1399      <rdfs:range rdf:resource="#InformationSecurityIncident"/>
1400      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
```

```
1401      >Indica de quais incidentes um cenário é escopo.</rdfs:comment>
1402    </owl:ObjectProperty>
1403    <owl:ObjectProperty rdf:about="#isARiskAssociatedWith">
1404      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1405      >Indica a qual cenário de incidentes um risco está associado.</
            rdfs:comment>
1406      <rdfs:domain rdf:resource="#Risk"/>
1407      <owl:inverseOf rdf:resource="#isAScenarioAssociatedWith"/>
1408      <rdfs:range rdf:resource="#IncidentScenario"/>
1409    </owl:ObjectProperty>
1410    <owl:ObjectProperty rdf:about="#isASubprocessOf">
1411      <rdfs:domain>
1412        <owl:Class>
1413          <owl:unionOf rdf:parseType="Collection">
1414            <owl:Class rdf:about="#A1ContextEstablishment"/>
1415            <owl:Class rdf:about="#A2RiskAssessment"/>
1416            <owl:Class rdf:about="#A4RiskAcceptance"/>
1417            <owl:Class rdf:about="#A3RiskTreatment"/>
1418          </owl:unionOf>
1419        </owl:Class>
1420      </rdfs:domain>
1421      <rdfs:range rdf:resource="#InformationSecurityRiskManagement"/>
1422      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1423      >Indica a relação entre as atividades e um processo de GRSI.</
            rdfs:comment>
1424      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
            FunctionalProperty"/>
1425    </owl:ObjectProperty>
1426    <owl:ObjectProperty rdf:ID="acceptTheRisks">
1427      <rdfs:range rdf:resource="#Risk"/>
1428      <rdfs:domain rdf:resource="#A4RiskAcceptance"/>
1429      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1430      >Indica os riscos aceitos na atividade de aceitação dos riscos.</
            rdfs:comment>
1431    </owl:ObjectProperty>
1432    <owl:ObjectProperty rdf:ID="hasStakeholder">
1433      <rdfs:domain rdf:resource="#A1ContextEstablishment"/>
1434      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1435      >Indicam os intervenientes que terão participação na GRSI.</
            rdfs:comment>
1436      <rdfs:range>
1437        <owl:Class>
1438          <owl:unionOf rdf:parseType="Collection">
1439            <owl:Class rdf:about="#Supplier"/>
1440            <owl:Class rdf:about="#Colaborator"/>
```

```
1441          </owl:unionOf>
1442        </owl:Class>
1443      </rdfs:range>
1444    </owl:ObjectProperty>
1445    <owl:ObjectProperty rdf:about="#hasRiskLevel">
1446      <rdfs:domain rdf:resource="#Risk"/>
1447      <rdfs:range rdf:resource="#RiskLevel"/>
1448      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
            FunctionalProperty"/>
1449      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1450      >Indica o nível de risco associado a um risco.</rdfs:comment>
1451    </owl:ObjectProperty>
1452    <owl:ObjectProperty rdf:ID="identifiesConsequences">
1453      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1454      >Indica as consequências identificadas na fase de identificação de
            riscos.</rdfs:comment>
1455      <rdfs:domain rdf:resource="#A221RiskIdentification"/>
1456      <rdfs:range rdf:resource="#Consequence"/>
1457    </owl:ObjectProperty>
1458    <owl:ObjectProperty rdf:about="#performsAttack">
1459      <rdfs:range rdf:resource="#Attack"/>
1460      <rdfs:domain rdf:resource="#Attacker"/>
1461      <owl:inverseOf rdf:resource="#isPerformedBy"/>
1462      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
            InverseFunctionalProperty"/>
1463      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1464      >Indica que ataque é realizado por um atacante.</rdfs:comment>
1465    </owl:ObjectProperty>
1466    <owl:ObjectProperty rdf:ID="hasAssociatedThreats">
1467      <rdfs:domain rdf:resource="#IncidentScenario"/>
1468      <rdfs:range rdf:resource="#Threat"/>
1469      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1470      >Indica as ameaças que estão relacionadas a um cenário de incidentes
            de segurança da informação.</rdfs:comment>
1471    </owl:ObjectProperty>
1472    <owl:ObjectProperty rdf:about="#usesTool">
1473      <owl:inverseOf rdf:resource="#isUsedBy"/>
1474      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1475      >Indica ferramentas utilizadas por colaboradores ou em controles.</
            rdfs:comment>
1476      <rdfs:domain>
1477        <owl:Class>
1478          <owl:unionOf rdf:parseType="Collection">
1479            <owl:Class rdf:about="#Person"/>
1480            <owl:Class rdf:about="#Control"/>
```

```
1481          </owl:unionOf>
1482        </owl:Class>
1483      </rdfs:domain>
1484      <rdfs:range rdf:resource="#Tool"/>
1485    </owl:ObjectProperty>
1486    <owl:ObjectProperty rdf:about="#hasImpact">
1487      <rdfs:range rdf:resource="#BusinessImpact"/>
1488      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1489      >Indica o impacto atribuído a um cenário de incidentes.</rdfs:comment
          >
1490      <rdfs:domain rdf:resource="#IncidentScenario"/>
1491    </owl:ObjectProperty>
1492    <owl:ObjectProperty rdf:ID="identifiesVulnerabilities">
1493      <rdfs:domain rdf:resource="#A221RiskIdentification"/>
1494      <rdfs:range rdf:resource="#Vulnerability"/>
1495      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1496      >Indica as vulnerabilidades de incidentes identificados na fase de
          identificação de riscos.</rdfs:comment>
1497    </owl:ObjectProperty>
1498    <owl:ObjectProperty rdf:about="#assessesConsequences">
1499      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1500      >Indica a avaliação de consequências dos cenários de incidentes de
          segurança da informação lhe associando uma medida de impacto.</
          rdfs:comment>
1501      <rdfs:domain rdf:resource="#A222RiskEstimation"/>
1502      <rdfs:range rdf:resource="#IncidentScenario"/>
1503    </owl:ObjectProperty>
1504    <owl:ObjectProperty rdf:ID="isADivisionOf">
1505      <rdfs:range rdf:resource="#Organization"/>
1506      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#
          FunctionalProperty"/>
1507      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1508      >Indicam a relação entre um departamento ou área e uma organização.</
          rdfs:comment>
1509      <rdfs:domain rdf:resource="#Department"/>
1510    </owl:ObjectProperty>
1511    <owl:ObjectProperty rdf:ID="hasAssociatedConsequences">
1512      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1513      >Indica as consequências que estão relacionadas a um cenário de
          incidentes de segurança da informação.</rdfs:comment>
1514      <rdfs:domain rdf:resource="#IncidentScenario"/>
1515      <rdfs:range rdf:resource="#Consequence"/>
1516    </owl:ObjectProperty>
1517    <owl:ObjectProperty rdf:ID="usesAttackingTool">
1518      <rdfs:subPropertyOf rdf:resource="#usesTool"/>
```

```
1519      <rdfs:range rdf:resource="#AttackingTool"/>
1520      <rdfs:domain rdf:resource="#Attacker"/>
1521    </owl:ObjectProperty>
1522    <owl:ObjectProperty rdf:ID="hasType">
1523      <rdfs:range rdf:resource="#TreatmentType"/>
1524      <rdfs:domain rdf:resource="#Treatment"/>
1525      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1526      >Indica o tipo do tratamento se evita o risco, se o mitiga, se o
            transfere ou se o retem.</rdfs:comment>
1527    </owl:ObjectProperty>
1528    <owl:ObjectProperty rdf:ID="hasAssociatedVulnerability">
1529      <rdfs:range rdf:resource="#Vulnerability"/>
1530      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1531      >Indica as ameaças que estão relacionadas a um cenário de incidentes
            de segurança da informação.</rdfs:comment>
1532      <rdfs:domain rdf:resource="#IncidentScenario"/>
1533    </owl:ObjectProperty>
1534    <owl:ObjectProperty rdf:ID="isASubActivityOf">
1535      <rdfs:domain>
1536        <owl:Class>
1537          <owl:unionOf rdf:parseType="Collection">
1538            <owl:Class rdf:about="#A221RiskIdentification"/>
1539            <owl:Class rdf:about="#A222RiskEstimation"/>
1540          </owl:unionOf>
1541        </owl:Class>
1542      </rdfs:domain>
1543      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1544      >Indica a relação entre uma atividade e suas tarefas.</rdfs:comment>
1545      <rdfs:range rdf:resource="#A22RiskAnalysis"/>
1546    </owl:ObjectProperty>
1547    <owl:ObjectProperty rdf:ID="hasControlAssociated">
1548      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1549      >Identifica controles que estão sendo utilizados em um tratamento de
            um risco.</rdfs:comment>
1550      <rdfs:range rdf:resource="#Control"/>
1551      <rdfs:domain rdf:resource="#Treatment"/>
1552    </owl:ObjectProperty>
1553    <owl:ObjectProperty rdf:ID="isConsequenceOf">
1554      <rdfs:domain rdf:resource="#Consequence"/>
1555      <rdfs:range rdf:resource="#Threat"/>
1556      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1557      >Identificam quais ameaças tem uma determinada consequência.</
            rdfs:comment>
1558    </owl:ObjectProperty>
1559    <owl:DatatypeProperty rdf:ID="hasOrigin">
```

```
1560      <rdfs:range>
1561        <owl:DataRange>
1562          <owl:oneOf rdf:parseType="Resource">
1563            <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                  string"
1564            >Deliberate</rdf:first>
1565            <rdf:rest rdf:parseType="Resource">
1566              <rdf:rest rdf:parseType="Resource">
1567                <rdf:rest rdf:resource="http://www.w3.org/1999/02/22-rdf-
                      syntax-ns#nil"/>
1568                <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                      string"
1569                >Environmental</rdf:first>
1570              </rdf:rest>
1571              <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                    string"
1572              >Accidental</rdf:first>
1573            </rdf:rest>
1574          </owl:oneOf>
1575        </owl:DataRange>
1576      </rdfs:range>
1577      <rdfs:domain rdf:resource="#Threat"/>
1578    </owl:DatatypeProperty>
1579    <owl:DatatypeProperty rdf:ID="hasValue">
1580      <rdfs:range>
1581        <owl:DataRange>
1582          <owl:oneOf rdf:parseType="Resource">
1583            <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                  string"
1584            >Very Small</rdf:first>
1585            <rdf:rest rdf:parseType="Resource">
1586              <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                    string"
1587              >Small</rdf:first>
1588              <rdf:rest rdf:parseType="Resource">
1589                <rdf:rest rdf:parseType="Resource">
1590                  <rdf:rest rdf:parseType="Resource">
1591                    <rdf:rest rdf:parseType="Resource">
1592                      <rdf:first rdf:datatype="http://www.w3.org/2001/
                            XMLSchema#string"
1593                      >Insignificant</rdf:first>
1594                      <rdf:rest rdf:parseType="Resource">
1595                        <rdf:first rdf:datatype="http://www.w3.org/2001/
                              XMLSchema#string"
1596                        >Critical</rdf:first>
```

```
1597                        <rdf:rest rdf:resource="http://www.w3.org
                                /1999/02/22-rdf-syntax-ns#nil"/>
1598                      </rdf:rest>
1599                    </rdf:rest>
1600                    <rdf:first rdf:datatype="http://www.w3.org/2001/
                            XMLSchema#string"
1601                    >Very High</rdf:first>
1602                  </rdf:rest>
1603                  <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema
                        #string"
1604                  >High</rdf:first>
1605                </rdf:rest>
1606                <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                        string"
1607                >Medium</rdf:first>
1608              </rdf:rest>
1609            </rdf:rest>
1610          </owl:oneOf>
1611        </owl:DataRange>
1612      </rdfs:range>
1613      <rdfs:domain rdf:resource="#Asset"/>
1614    </owl:DatatypeProperty>
1615    <owl:DatatypeProperty rdf:ID="impactsOn">
1616      <rdfs:range>
1617        <owl:DataRange>
1618          <owl:oneOf rdf:parseType="Resource">
1619            <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                      string"
1620            >Availability</rdf:first>
1621            <rdf:rest rdf:parseType="Resource">
1622              <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                        string"
1623              >Integrity</rdf:first>
1624              <rdf:rest rdf:parseType="Resource">
1625                <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                          string"
1626                >Confidentiality</rdf:first>
1627                <rdf:rest rdf:parseType="Resource">
1628                  <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema
                            #string"
1629                  >Authenticity</rdf:first>
1630                  <rdf:rest rdf:parseType="Resource">
1631                    <rdf:first rdf:datatype="http://www.w3.org/2001/
                              XMLSchema#string"
1632                    >Privacy</rdf:first>
```

```
1633                    <rdf:rest rdf:parseType="Resource">
1634                      <rdf:rest rdf:parseType="Resource">
1635                        <rdf:first rdf:datatype="http://www.w3.org/2001/
                              XMLSchema#string"
1636                        >ROI</rdf:first>
1637                        <rdf:rest rdf:parseType="Resource">
1638                          <rdf:rest rdf:parseType="Resource">
1639                            <rdf:rest rdf:resource="http://www.w3.org
                                  /1999/02/22-rdf-syntax-ns#nil"/>
1640                            <rdf:first rdf:datatype="http://www.w3.org
                                  /2001/XMLSchema#string"
1641                            >Business Oportunity</rdf:first>
1642                          </rdf:rest>
1643                          <rdf:first rdf:datatype="http://www.w3.org/2001/
                                XMLSchema#string"
1644                          >Business Continuity</rdf:first>
1645                        </rdf:rest>
1646                      </rdf:rest>
1647                      <rdf:first rdf:datatype="http://www.w3.org/2001/
                            XMLSchema#string"
1648                      >Business Objetives</rdf:first>
1649                    </rdf:rest>
1650                  </rdf:rest>
1651                </rdf:rest>
1652              </rdf:rest>
1653            </rdf:rest>
1654          </owl:oneOf>
1655        </owl:DataRange>
1656      </rdfs:range>
1657      <rdfs:domain rdf:resource="#Consequence"/>
1658    </owl:DatatypeProperty>
1659    <owl:DatatypeProperty rdf:ID="hasDate">
1660      <rdfs:range rdf:resource="http://www.w3.org/2001/XMLSchema#date"/>
1661      <rdfs:domain rdf:resource="#Event"/>
1662    </owl:DatatypeProperty>
1663    <owl:DatatypeProperty rdf:ID="hasAcceptanceDescription">
1664      <rdfs:domain rdf:resource="#RiskAcceptanceStatus"/>
1665      <rdfs:range rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
1666    </owl:DatatypeProperty>
1667    <owl:DatatypeProperty rdf:ID="hasAttackLocation">
1668      <rdfs:domain rdf:resource="#Attack"/>
1669      <rdfs:range>
1670        <owl:DataRange>
1671          <owl:oneOf rdf:parseType="Resource">
```

```
1672            <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                    string"
1673            >Local</rdf:first>
1674            <rdf:rest rdf:parseType="Resource">
1675              <rdf:rest rdf:resource="http://www.w3.org/1999/02/22-rdf-
                      syntax-ns#nil"/>
1676              <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                      string"
1677              >Remote</rdf:first>
1678            </rdf:rest>
1679          </owl:oneOf>
1680        </owl:DataRange>
1681      </rdfs:range>
1682    </owl:DatatypeProperty>
1683    <owl:DatatypeProperty rdf:ID="hasImplementationStatus">
1684      <rdfs:domain rdf:resource="#Control"/>
1685      <rdfs:range>
1686        <owl:DataRange>
1687          <owl:oneOf rdf:parseType="Resource">
1688            <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                    string"
1689            >implemented</rdf:first>
1690            <rdf:rest rdf:parseType="Resource">
1691              <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                      string"
1692              >partially implemented</rdf:first>
1693              <rdf:rest rdf:parseType="Resource">
1694                <rdf:rest rdf:resource="http://www.w3.org/1999/02/22-rdf-
                        syntax-ns#nil"/>
1695                <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                        string"
1696                >not implemented</rdf:first>
1697              </rdf:rest>
1698            </rdf:rest>
1699          </owl:oneOf>
1700        </owl:DataRange>
1701      </rdfs:range>
1702    </owl:DatatypeProperty>
1703    <owl:DatatypeProperty rdf:ID="hasAcceptanceStatus">
1704      <rdfs:range>
1705        <owl:DataRange>
1706          <owl:oneOf rdf:parseType="Resource">
1707            <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                    string"
1708            >accepted</rdf:first>
```

```
1709            <rdf:rest rdf:parseType="Resource">
1710              <rdf:rest rdf:resource="http://www.w3.org/1999/02/22-rdf-
                      syntax-ns#nil"/>
1711              <rdf:first rdf:datatype="http://www.w3.org/2001/XMLSchema#
                      string"
1712              >not accepted</rdf:first>
1713            </rdf:rest>
1714          </owl:oneOf>
1715        </owl:DataRange>
1716      </rdfs:range>
1717      <rdfs:domain rdf:resource="#RiskAcceptanceStatus"/>
1718    </owl:DatatypeProperty>
1719    <owl:DatatypeProperty rdf:ID="hasDescription">
1720      <rdfs:domain>
1721        <owl:Class>
1722          <owl:unionOf rdf:parseType="Collection">
1723            <owl:Class rdf:about="#Asset"/>
1724            <owl:Class rdf:about="#Threat"/>
1725            <owl:Class rdf:about="#Control"/>
1726            <owl:Class rdf:about="#Vulnerability"/>
1727            <owl:Class rdf:about="#Consequence"/>
1728            <owl:Class rdf:about="#Event"/>
1729            <owl:Class rdf:about="#BusinessSector"/>
1730            <owl:Class rdf:about="#Treatment"/>
1731            <owl:Class rdf:about="#IncidentScenario"/>
1732            <owl:Class rdf:about="#BusinessImpact"/>
1733            <owl:Class rdf:about="#InformationSecurityRiskManagement"/>
1734            <owl:Class rdf:about="#RiskPriority"/>
1735            <owl:Class rdf:about="#RiskLevel"/>
1736            <owl:Class rdf:about="#Organization"/>
1737            <owl:Class rdf:about="#OccurrenceLikelihood"/>
1738            <owl:Class rdf:about="#Person"/>
1739            <owl:Class rdf:about="#TreatmentType"/>
1740            <owl:Class rdf:about="#Risk"/>
1741            <owl:Class rdf:about="#BusinessRule"/>
1742            <owl:Class rdf:about="#InformationSecurityRequirement"/>
1743            <owl:Class rdf:about="#Tool"/>
1744            <owl:Class rdf:about="#Measure"/>
1745            <owl:Class rdf:about="#InformationSecurityDocumentation"/>
1746          </owl:unionOf>
1747        </owl:Class>
1748      </rdfs:domain>
1749      <rdfs:range rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
1750    </owl:DatatypeProperty>
1751    <owl:FunctionalProperty rdf:about="#hasRiskAcceptanceStatus">
```

```
1752      <rdfs:comment rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
1753      >Indica o status de aceitação de um risco, se aceito ou não aceito.</
              rdfs:comment>
1754      <rdfs:range rdf:resource="#RiskAcceptanceStatus"/>
1755      <rdfs:domain rdf:resource="#Risk"/>
1756      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#ObjectProperty"
              />
1757    </owl:FunctionalProperty>
1758    <RiskAcceptanceStatus rdf:ID="AcceptedRisk">
1759      <hasAcceptanceDescription rdf:datatype="http://www.w3.org/2001/
              XMLSchema#string"
1760      >Risco Aceito pela organização</hasAcceptanceDescription>
1761      <hasAcceptanceStatus rdf:datatype="http://www.w3.org/2001/XMLSchema#
              string"
1762      >accepted</hasAcceptanceStatus>
1763    </RiskAcceptanceStatus>
1764    <A222RiskEstimation rdf:ID="A222RiskEstimation_2"/>
1765    <RiskAcceptanceStatus rdf:ID="NoAcceptedRisk">
1766      <hasAcceptanceDescription rdf:datatype="http://www.w3.org/2001/
              XMLSchema#string"
1767      ></hasAcceptanceDescription>
1768      <hasAcceptanceStatus rdf:datatype="http://www.w3.org/2001/XMLSchema#
              string"
1769      >not accepted</hasAcceptanceStatus>
1770    </RiskAcceptanceStatus>
1771  </rdf:RDF>
```